

ONYX Antivirus & Firewall Guidelines

Contents

Introduction	2
Antivirus Settings.....	2
Licensing	3
Printer and Profile Downloads	4
Network Communications.....	4
Firewall Settings.....	5
Appendix.....	6
Extended Port Information List.....	6
Testing with PortQry	8
Setting Folder Permissions.....	8

Introduction

ONYX does not endorse any specific antivirus software or recommend using our software without security protection running; however, most firewalls and antivirus programs must be configured, with exceptions for ONYX applications and printer ports, to ensure proper operation and optimal performance. This documentation will refer to C:\ONYXDirectory\ as the location where Onyx is installed. Your installation directory name may vary depending on the product name and version of Onyx you have.

Antivirus Settings

- None of the executable files within the ONYX directories should be blocked by antivirus software.
 - Change the antivirus settings to add exceptions for individual program files or the entire installation directory.
 - Typical antivirus settings allow programs to be called “low-risk” or “safe” processes.
 - The most important programs are:
 - RIP-Queue – C:\ONYXDirectory\server\postershop.exe
 - Media Manager – C:\ONYXDirectory\MediaManager\bin\MediaManager.exe
 - Job Editor – C:\ONYXDirectory\Preflight\preflightLauncher.exe
 - RIP processing EXE files should also have no restrictions:
 - Thrive: appeui.exe, appenormalizer.exe
 - Onyx contains its own Java. This Java folder should not have restrictions:
 - Onyx Java: C:\ONYXDirectory\Vendor\
- Folders that ONYX uses should have antivirus scanning/monitoring disabled
 - All folders in the ONYX installation (C:\ONYXDirectory and all subdirectories)
 - Printer-specific “work” folders may need to be added as a separate exception if the work folder for a printer has been configured to be outside of the main installation path (C:\ONYXDirectory\ in our example)

Licensing

- License-related files and servers must also be allowed with no restrictions:
 - C:\ProgramData\SafeNet Sentinel\Sentinel RMS Development Kit\System
 - C:\Windows\SysWOW64\servdat.slm (needed for network licenses on the server)
 - C:\ProgramData\Onyx\NetLicense
 - C:\Program Files (x86)\Common Files\Aladdin Shared\HASP
 - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Onyx License Manager\
 - Hardware Key Specific
 - C:\Documents and Settings\All Users\Application Data\SafeNet Sentinel\Sentinel RMS Development Kit\System

**Not all of the above folders will exist, depending on the type of license being used (physical key vs. soft license).*

- **Ports** (TCP and UDP) 1947 and 5093 need to be open
- **Onyx License Verification Server** <https://api-prod-ogfx.azure-api.net/licensing/connection/test>
 - You should receive the following message if communication is successful with the server:

```
{
  "statusCode": 1,
  "message": "Valid connection found"
}
```

- Security settings need to be set so that all users are allowed to Read and Write to the C:\ProgramData\SafeNet Sentinel Folder (for additional instructions, see [setting folder permissions](#) in the Appendix below)

Printer and Profile Downloads

- The Printer & Profile Downloads Manager (PPDM) needs to be able to communicate with the following server. <http://efd.onyxgfx.com> through port 80.
 - The elements of the driver download are contained in zip files. Some networks or domains may block this file format.
 - Some zip files may contain executable files from the printer manufacturer that run during the printer installation. Some networks or domains may block zip files that contain executable files.
 - To test, go to the following URL. The results should be the download of an approximate 297 KB file named “Agfa_Anapurna_H3200i_LED.NoMedia”. If no download is initiated, something in the security policy or settings may be blocked and must be adjusted.
 - http://efd.onyxgfx.com/Media?download=MedialessPrnInsts/Agfa_Anapurna_H3200i_LED.NoMedia&version=Onyx24&prninst=Agfa_Anapurna_H3200i_LED

Network Communications

- Network communication must not be blocked by antivirus or firewall on the following ports.
 - Critical port to check
 - TCP/IP needs to be allowed on ports 80, 515, 1947, 5093, 8889, 9100, 27017, and 10000
 - Device-specific ports
 - For HP printers, ports 8085, 8086, and 8090 need to be allowed.
 - For Epson printers, port 30561 needs to be allowed.
 - For Mimaki printers, ports 8002, 11110, and 11111 need to be allowed.
 - For Zund Cutters, port 51000 needs to be allowed

Firewall Settings

To verify if your Network Firewall permits ONYX programs to communicate through it, open your Start menu and search for "Allow an app through Windows Firewall." The necessary firewall settings should be enabled to let ONYX RIP-Queue communicate over the network. The type of network your computers connect to and your network configuration will determine which profiles must be allowed through the firewall.

These permissions are required to allow the licensing software to communicate with the server through the firewall.

Allowed apps and features:

Name	Domain	Private	Public
<input checked="" type="checkbox"/> Sentinel License Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Sentinel RMS License Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

These permissions are required to allow the ONYX Thrive RIP-Queue stations to communicate with each other.

Allowed apps and features:

Name	Domain	Private	Public
<input checked="" type="checkbox"/> ONYX Rip-Queue Executable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ONYX Rip-Queue Executable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> ONYX Rip-Queue Executable	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> OpenJDK Platform binary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> OpenJDK Platform binary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> OpenJDK Platform binary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This permission is required if you are trying to set up workstations for Job Editor, Print Forwarding, etc.

Allowed apps and features:

Name	Domain	Private	Public	Group Policy
<input checked="" type="checkbox"/> Bonjour Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No

Appendix

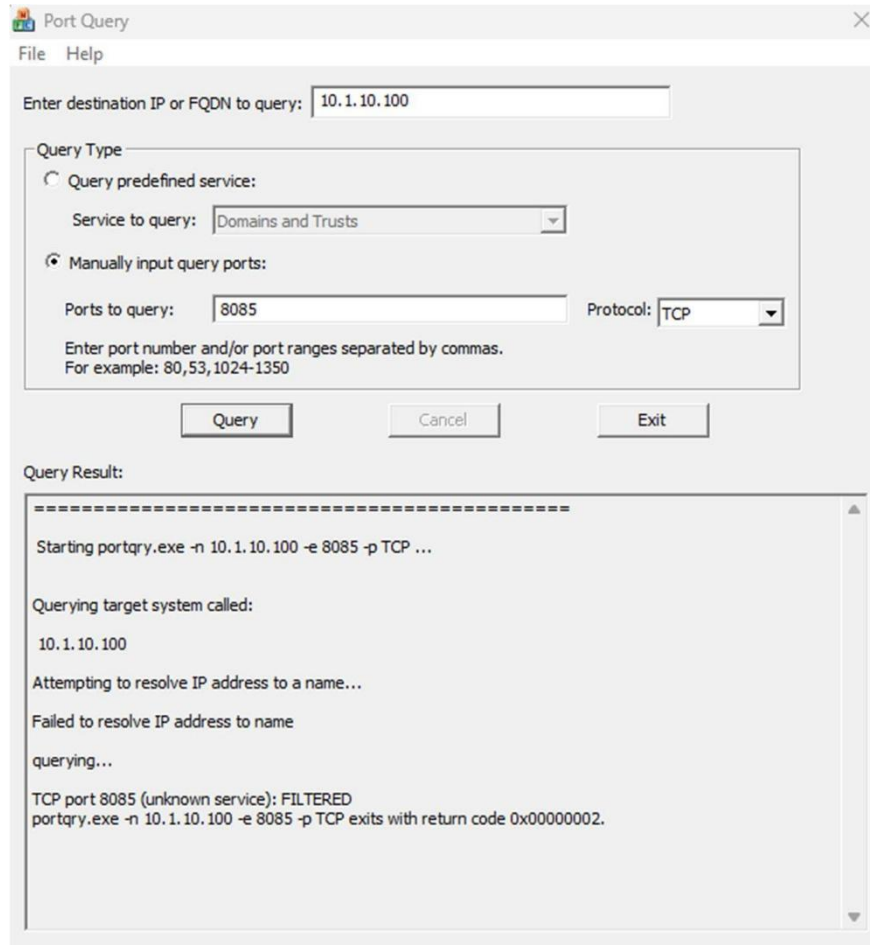
Extended Port Information List

Port	Product	Purpose	Additional Info
80	Dashboard, P&PDM, Production Manager / PDP	Default for Production Manager / PDP	When using the API products. This port must match the Production Manager port set in RIP-Queue
443	Dashboard V3, Production Manager / PDP	Default for Production Manager / PDP	When using the API products. This port must match the Production Manager port set in RIP-Queue
515	Any product connecting to Canon ColorWave printers	Some devices use this default LDP printing protocol.	The Canon ColorWave printers may still use this.
1947	All products	Sentinel Licensing	License-related communication
5093	The machine that hosts the network license manager	Network License port for TCP/UDP	May need to be unblocked on the computer running the network license.
5432	Data Access (Postgresql)	Postgres (during Data Access upgrades from version 2.x Databases only)	
8000	RIP-Queue Server	Used for API access	
8443	Data Access (formerly HUB Controller)	API Server to send and receive data	Setting found in the Data Access application (HUB Controller)
8444	Data Access Notify Port		Setting found in the Data Access application (HUB Controller)
8889	Any product connecting to a JETi printer	A generic port that any device or app can use.	Used by the JETi printers
9100	All products	Common print data connection	Used by almost all modern printers for communication.
10000	All products	The default UPD port is used to broadcast station information.	

27000 - 29999	RIP, Thrive, Go	MongoDB	
50000 - 69999	MongoDB/RMS License	MongoDB range for individual async connections and RMS license connections	Software License range: 50000 - 59999; Hardware license range: 50000 – 69999
63702	Align	Submitting print jobs to Thrive	To send and receive data from the Azure server.
8085, 8086, 8080, 8090	Any product connecting to HP printer(s)	HP Printers	
30561	Any product connecting to Epson printer(s)	Epson Printers	
8002, 11110, 11111	Any product connecting to Mimaki printer(s)	Mimaki Printers	
51000	Any product connecting to Zund cutter(s)	Zund Cutters	

Testing with PortQry

Microsoft offers a free PortQry tool for verifying whether ports are open, blocked, or filtered. It can be downloaded here. <https://www.microsoft.com/en-us/download/details.aspx?id=24009>



Setting Folder Permissions

- Right-click on the following folder:
 - C:\ProgramData\SafeNet Sentinel
- Click *Properties* in the pop-up menu
- Click the *Security* tab
- In "Group or user names", click *Users*
- In "Permissions for Users", if not all items are set to "Allow"
 - Click *Advanced* to open the Advanced Security Settings for SafeNet Sentinel
 - In "Permission entries", click *Users*
 - Click *Edit*
 - Enable all permissions
 - Click the *OK* button to accept the permissions
 - Select the "Replace all child object permission entries..." checkbox
 - Click the *OK* button to close the Advanced settings dialog