MFPsecure/Scan Whitepaper

Version 0.7

March 2020

1. Version Control

Version	Author	Date	Changes
0.1	Calvin Orley	21st July 2019	First Draft
0.2	Calvin Orley	24th August 2019	Adding HA options
0.3	Calvin Orley	27th August 2019	Feedback changes
0.4	Calvin Orley	29th October 2019	Added changes throughout
0.5	Calvin Orley	13th November 2019	Changed Overview
0.6	Calvin Orley	8th January 2020	Various Updates

Contents

1. Version Control 3
2. Introduction 5
3. MFPsecure/Scan Overview 6
4. MFPsecure/Scan Installation 8
5. MFPSecure/Scan Server Sizing 9
5.1. How many scan devices are in scope? 9
5.2. How many scan jobs per day / week / month? 10
5.3. Sample Processing times for Server Specification recommendations 11
6. Infrastructure Design 13
6.1. Scenario One – Single VPSX 13
6.2. Scenario Two – One VPSX, Multiple MFPsecure Servers 14
6.2.1. Option A 14
6.2.2. Option B 15
7. High Availability 16
7.1. VMware High Availability 16
7.2. Network Load Balancer 17
7.3. F5 Load Balancer setup 19
7.4. Microsoft Clustering 20
8. Embedded Print Device Compatibility 21
9. Ports / Protocols for MFPsecure/Scan 22
10. Network bandwidth and usage 25
11. MFPsecure/Scan Antivirus exclusions 26
12. Troubleshooting MFPsecure/Scan 27
13. Appendix A MFPSecure/Scan Internal Architecture 29
14. Appendix B – Port Flow 30

Written By Calvin Orley

2. Introduction

This white paper provides the technical brief of the MFPsecure/Scan component that is part of the VPSX product family.

3. MFPsecure/Scan Overview

Documents play a critical role in many business processes. Today, organizations need the ability to protect these key information assets while making them easier to share and manage. Secure scanning software helps companies transform physical document workflows into digital ones.

LRS has a powerful suite of document capture components to help you tailor your infrastructure for the digital workplace. MFPsecure/Scan software can run on compatible touchscreen enabled MFPs from most leading print hardware manufacturers. From the interface built into your multifunction devices, users can scan documents and send them to a file folder, portal, cloud repository, email address, FTP server, and other destinations as well as leverage built-in Optical Character Recognition (OCR) capabilities.

The solution offers single sign-on via proximity cards, PIN codes, and other authentication methods. Innovative features offer faster, more flexible OCR capabilities, advanced barcode recognition, auto-mated faxing, as well as integration with Microsoft Exchange, SharePoint, and leading Cloud storage platforms.

Figure 1 High Level Overview

How does MFPsecure/Scan software work?

Login to the MFPsecure/Scan solution at your scan device and access personalized profiles that allow for one-touch automated multi-layer scan and distribution processes.

MFPsecure/Scan software manages the communication between the scan device and your server, database and business solutions. You can use existing information to name, categorize and file scanned documents or add important data from manual input, barcodes or zonal text analysis.

Multiple features help to tailor the document scanning capabilities to the needs of your business and make sure you end up with optimized scanned documents that are enriched with relevant data and filed in exactly the right location within seconds.

Scan and convert documents

MFPsecure/Scan makes it easy to turn scanned documents into searchable PDF or editable Microsoft Office formats. Intelligent and intuitive optical character recognition software facilitates the integration of scanned files into document management workflows. Scanned images can also be cleaned to remove common blemishes like hole punch marks and coffee stains.

Connect to the cloud

Scan documents to your favourite cloud solutions. With MFPsecure/Scan cloud connectors to Google Drive Professional, OneDrive and Box, allowing the digital document workflow to be a cloud based file management system.

Browse network folders

Search the authenticated network folder structure right from the scan-device screen. MFPsecure/Scan profiles can be customized to give each user their preferred experience. It can even create new digital network folders if they don't already exist. The MFPsecure/Scan solution is an easy to use document archiving system that will instantly create a corporate document repository.

Easy to configure

MFPsecure/Scan software is simple to install and configure, and scanning processes are easy to create and manage via the central server-based administration application.

User Profiles

Quickly create profiles for users or devices to personalize their experience. You can restrict the system to only allow access to desired functions based on individual authentication at the scan device.

Who should use MFPsecure/Scan software?

Scanning and processing documents is a important task for organizations of any industry and size. The MFPsecure/Scan solution provides companies with the ability to optimize scan and capture processes for their organization and the employees. MFPsecure/Scan software offers a simple, scalable, user friendly experience whilst maintaining the document security in the scanning processes.

All in all, …

MFPsecure/Scan intelligent document scanning software offers a comprehensive set of best-in-class, intelligent document scanning features with robust security functions and a simple user-friendly design. MFPsecure/Scan will transform your single or mixed fleet of input devices into a highly integrated environment for managing document scanning and workflows.

4. MFPsecure/Scan Installation

MFPsecure/Scan is installed as part of the MFPsecure installation. The components installed are integrated with the existing application installation along with a Secure Scan application which is available under the programs listing. This cannot be separated from the MFPsecure application.

All components are installed under the folder C:\Program Files\LRS\MFP Secure\Secure Scan.

There are 3 services that run once installed;

DrivveImage

DrivveImagePrinterService

Drivvemanagement

5. MFPSecure/Scan Server Sizing

MFPsecure/Print and Scan are now integrated and any sizing requirements need to take into account both sets of software to determine load.

In most scenarios, a single VPSX with MFPsecure/Print and MFPsecure/Scan infrastructure will be sufficient. However, you may need to consider handling scanning on a dedicated MFPsecure/Print & Scan server should there be requirements for medium to heavy OCR processing, as this uses CPU during the processing workflow.

Below are two scenarios to help with providing sizing specifications

There are two metrics that you can work against.

- How many scan devices are in scope (consideration of the Web Server)?
- How many scan jobs per day / week / month (Consideration of the Windows service)?

5.1. How many scan devices are in scope?

This gives a GENERAL idea of the type of server specifications required over a number of scan devices in scope.

Scan Devices	Recommended free resources for scanning
1 - 25	4 GB RAM & 2 CPU
26 – 100	8 GB RAM & 4 CPU
101 – 250	16 GB RAM & 6 CPU
251 +	16GB+ RAM & 8+ CPU

Figure 2 Scan device in scope table

5.2. How many scan jobs per day / week / month?

If the customer is aware of the amount of volume that is used for scanning, this section gives the specification metrics available depending on the number of jobs. This assumes average usage and not peak usage. Any spikes in usage will still have the potential for issues with lack of resources.

Region		**Example One**	**Example Two**	**Example Three**
Throughput		Up to 190.000 pages/month	Up to 53.000 pages/month	Up to 19.000 pages/month
Number of servers		2	1	1
Hardware requirements per server	CPU (i7)	2 x 8 Core CPU i7 2.8MHz	1 x 8 Core CPU i7 2.8MHz	1 x 8 Core CPU i7 2.8MHz
	Memory	32 GB RAM	16 GB RAM	8 GB RAM
	Disk Space	HA NAS with 1 TB Disk space as shared storage	HA NAS with 500 GB Disk space as shared storage	HA NAS with 500 GB Disk space as shared storage
	Network connectivity	1 Network Interface Card with TCP/IP and UDP supported, minimum 1Gbps recommended	1 Network Interface Card with TCP/IP and UDP supported, minimum 1Gbps recommended	1 Network Interface Card with TCP/IP and UDP supported, minimum 1Gbps recommended

Figure 3 Pages per month scope table

5.3. Sample Processing times for Server Specification recommendations

When determining the specifications of the Secure Scan server it's important to consider the TYPE of scan jobs that the server will be asked to process. By first testing the processing time of a sample job on your server you can extrapolate that to a higher volume. Scan job processing is highly CPU intensive, so you should decide how many CPUs you should allocate to a VM (or build in a physical server) before putting the application into production.

Internal load balancing and multi-threading

Secure Scan supports multi-threading, so it will internally process multiple jobs at once based off the number of CPUs that have been assigned to it. You can configure this setting in the Tools > Options Advanced window of the admin app. You can also set a priority by scan profile, so more urgent workflows like scan-to-fax are processed first.

As multiple jobs are scanned in they are moved to the hotfolder, then work\tmp and are queued there until an available CPU becomes available. They are then moved into the work\service folder, where they are processed and then deleted. This means that a large number of scans will not crash the application, but they may take longer to be processed and delivered.

Sample Workflow Processing Times

	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz - 4GB RAM	
	5-pg B&W	**15-pg color (200dpi)**
Image processing (despeckle, deskew, auto-rotate) PDF JPG2000 compression	9s	40s
Image processing (despeckle, deskew, auto-rotate), searchable PDF conversion, IRIS iHQC medium compression	12s	40s
Image processing (despeckle, deskew, auto-rotate), searchable PDF conversion, IRIS iHQC HIGH compression	15s	52s

Sample Workflow Processing Times

	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz - 4GB RAM	
	5-pg B&W	**15-pg color (200dpi)**
Image processing (despeckle, deskew, auto-rotate), searchable PDF conversion, IRIS iHQC medium compression, barcode recognition	14s	51s

6. Infrastructure Design

MFPsecure is available to be implemented under various design scenarios integrated with a number of High Availability technologies.. Included below are three scenarios. This is not an exhaustive scenario list. Each will also provide the High Availability options for each scenario.

a) Single server with VPSX, MFPsecure/Print and Scan on the same server.

b) VPSX on a single server with MFPsecure/Print and Scan on a separate server. This can be expanded to two, three, four servers.

c) VPSX, MFPsecure/Print and Scan on a two node Microsoft cluster.

6.1. Scenario One – Single VPSX

This option comprises of all components being available on the same server. This is recommended for

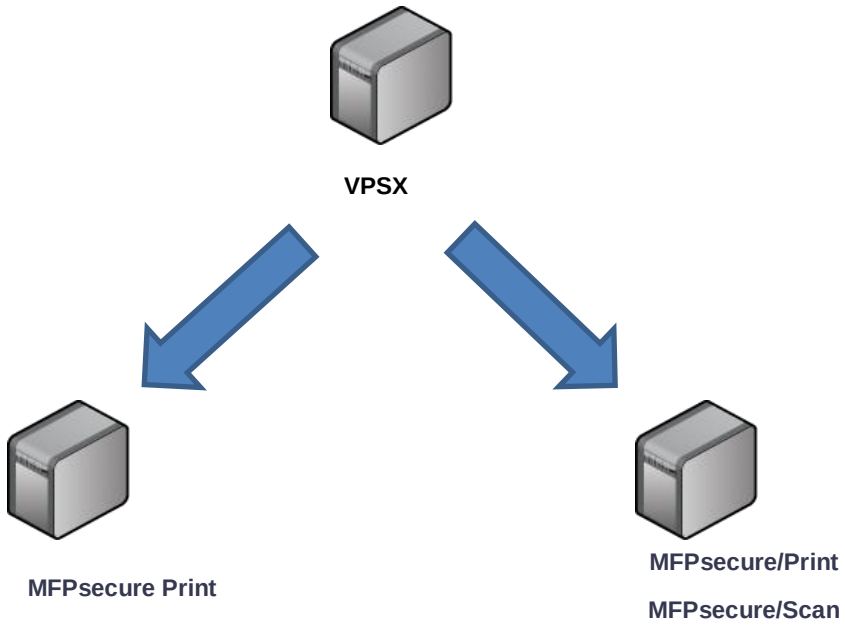
- Small implementations
- Implementations with no HA requirements
- Implementations with VMware HA requirements using server image level High Availability with Vmotion or manual snapshot backups.

6.2. Scenario Two – One VPSX, Multiple MFPsecure Servers

In this scenario there are a couple of options on how you can have MFPsecure working

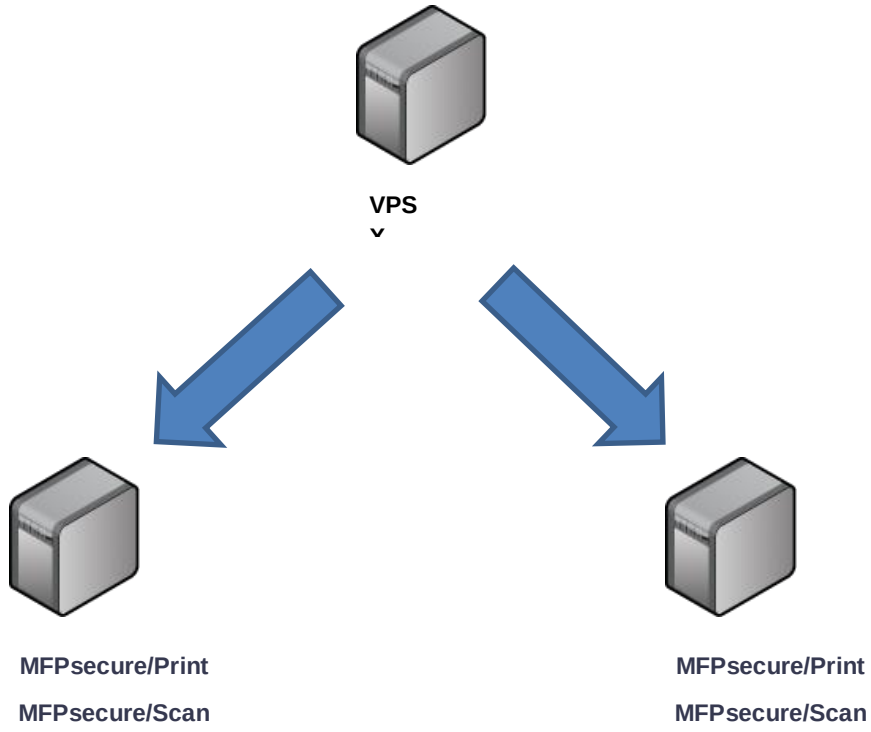
6.2.1. Option A

You have many embedded devices required for MFPsecure/Print and the requirement for scan is small, So we have two MFPsecure/Print servers but only scan running on one of the servers. The only High Availability options available are through VMware HA.



6.2.2. Option B

This scenario is for where there are substantial print and scan requirements. MFPsecure/Print and MFPsecure/Scan is installed on both servers and you can use High Availability options such as Network Load Balancer to provide either active / active or active / passive configurations for High Availability. You could also use Microsoft Clustering if this is a customer requirement. All details on High Availability options are in the next section.



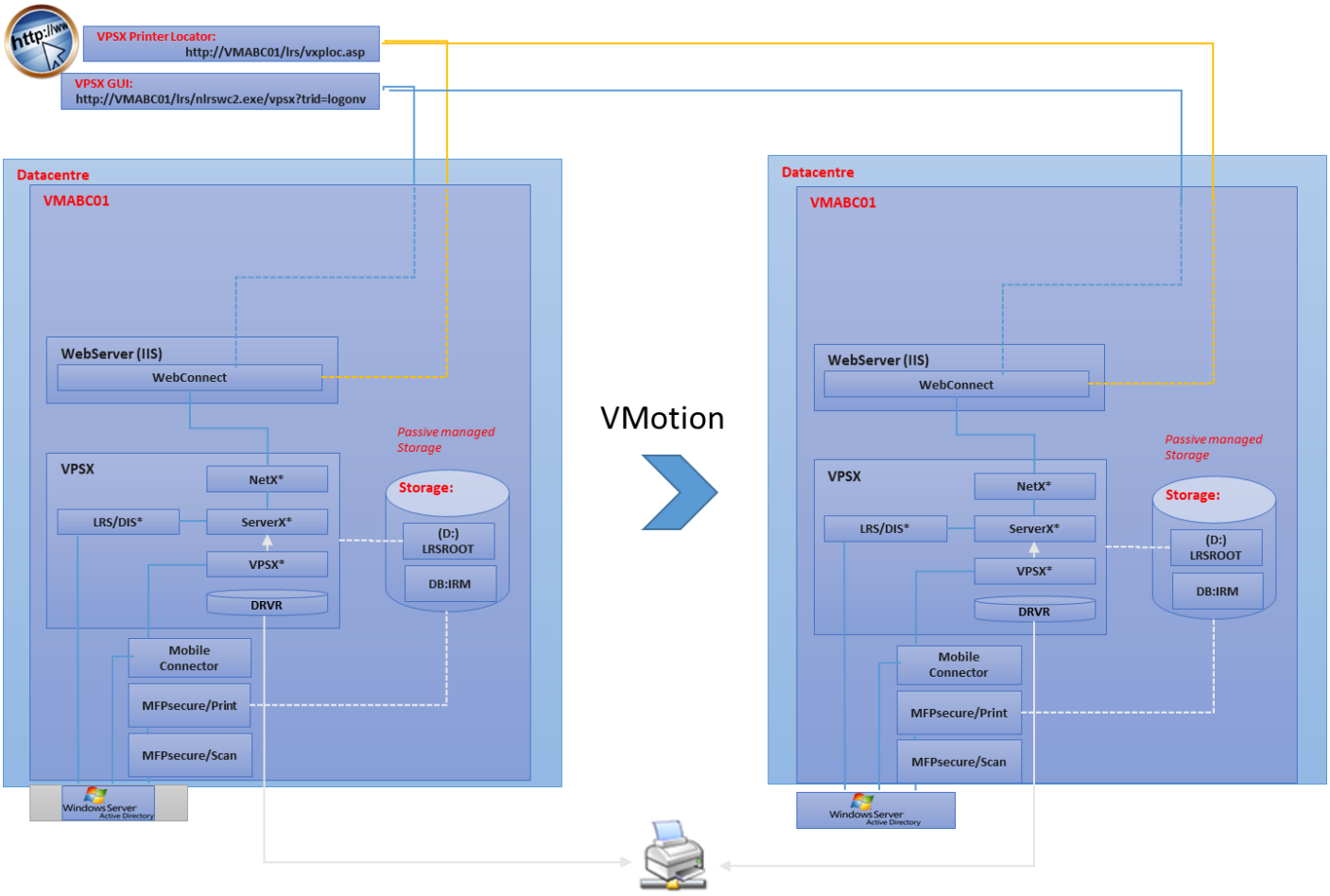
7. High Availability

In the previous section we discussed the infrastructure design options. This section will support with the High Availability options for each infrastructure design option.

7.1. VMware High Availability

VMware High Availability is a common used utility to ensure the image that the server is built on is online as much as possible. Any VMware host failure can use the VMotion application to switch over to another local or stretched host.

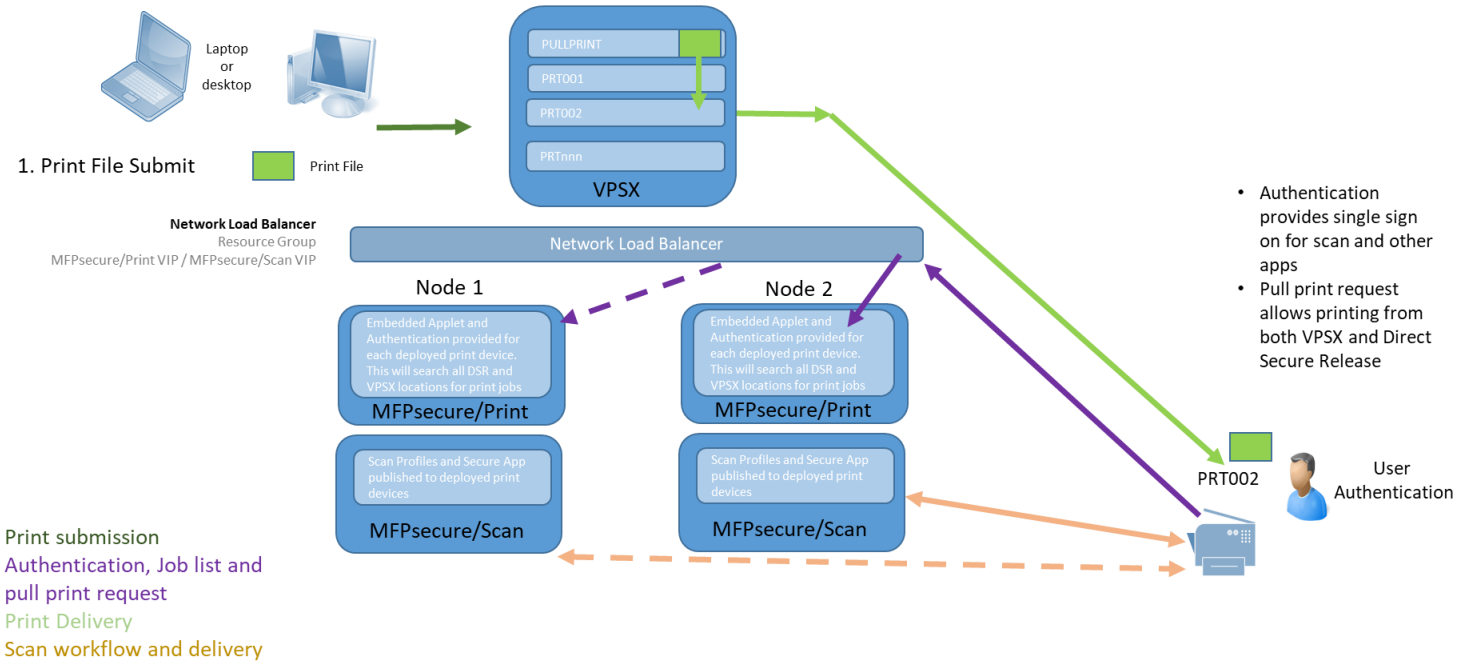
Below is an example how VPSX and MFPsecure can be implemented in a VMware High Availability configuration.



7.2. Network Load Balancer

We are seeing more often requirements for the LRS products working behind a load balancer. There are many vendors but the most common are F5 and NetScaler by Citrix.

MFPsecure/Scan has been tested and confirmed to work on F5. Specifically, a special configuration is needed on the load balancer so that the user session information is passed from the Load Balancer to the Nodes. This ensures that single sign-on and licensing works properly.



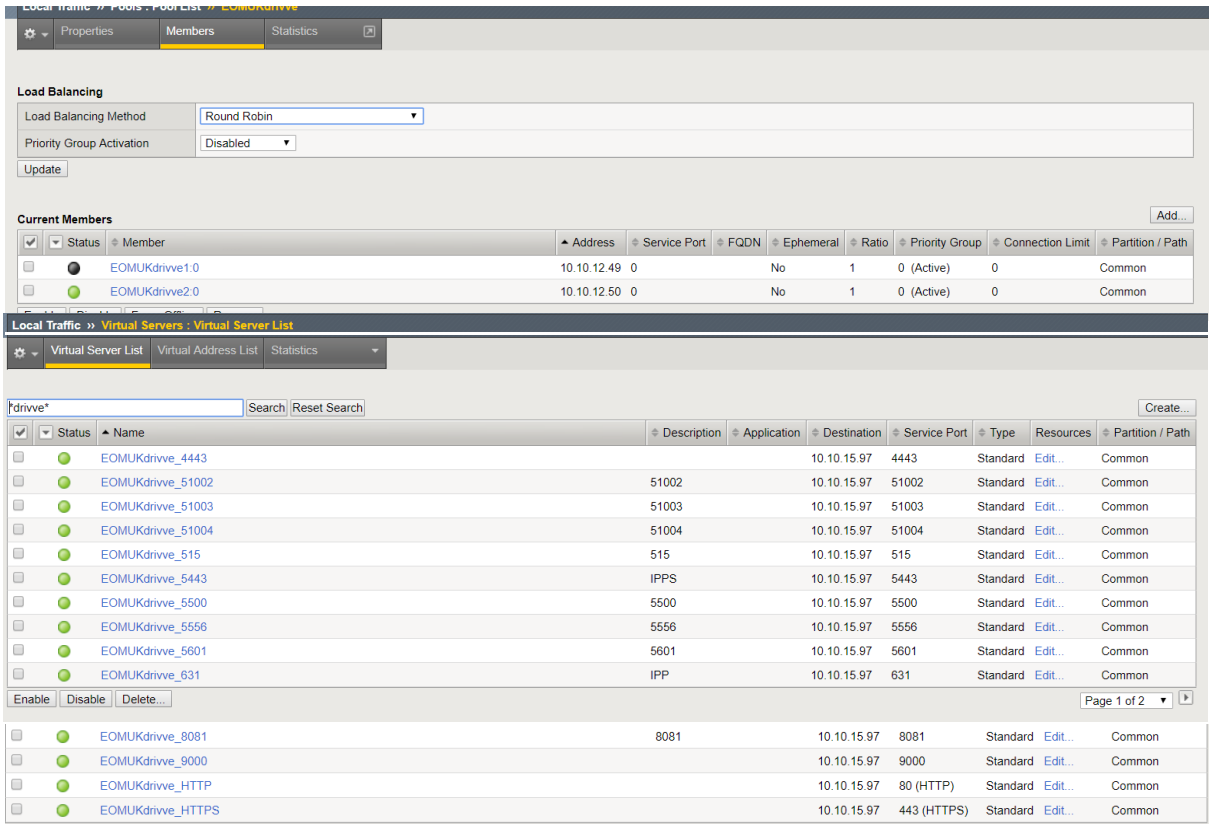
SSO Cache of credentials will not be available in a Load Balancer as the Key Store for each server is used for the encryption.

F5 Load Balancer setup

To Summarise, you need;

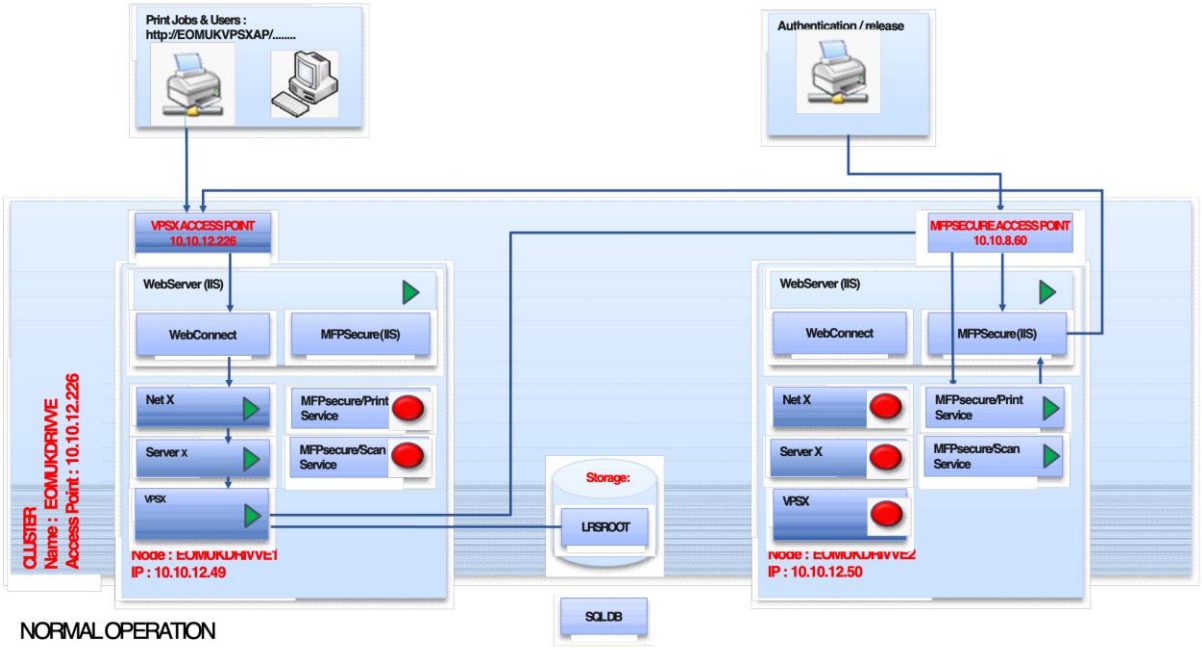
- A VIP Hostname (in the this example EOMUKMFPsecure/Scan.EOMHB.Shared
- 2 Nodes (EOMUKMFPsecure/Scan1 & EOMUKMFPsecure/Scan2)
- A Server Pool
- Virtual Servers (ports to monitor)

Figure 9 F5 Nodes



7.4. Microsoft Clustering

Many customers have requirements to use cluster technologies for High Availability. Below is a view of the cluster setup required in an active / passive configuration. The diagram shows the MFPsecure components running on Node 2 along with the VPSX components on Node 1. Should any failure occur, each node can handle all cluster resources on one node.



8. Embedded Print Device Compatibility

MFPsecure/Scan has worked with all the major vendors to ensure compatibility. In the first release of MFPsecure/Scan there are some limitations on the vendors supported. They are Xerox, HP, Ricoh and Konica Minolta.

There is an in depth compatibility list available can be found at **[PORTAL LOCATION]**

9. Ports / Protocols for MFPsecure/Scan

The following list shows all ports applicable to the MFPsecure/Scan application.

Component	Protocol	Port	Description
FTP Poll	TCP	21	Plain FTP
FTP Poll	TCP	990	Implicit FTP over SSL
FTP Poll	TCP	21	Explicit FTP over SSL
LDAP/AD	UDP	88	Kerberos
LDAP/AD	Both TCP/UDP	135	Client to DC Comm
LDAP/AD	UDP	389	LDAP query from Client to DC
LDAP/AD	Both TCP/UDP	53	DNS query from Client to DC
Notification Options	TCP	25	SMTP Port
Notification Options	TCP	465	ESMTP Port (SSL)
Notification Options	TCP	587	ESMTP Port (STARTTLS)
Send to FTP	TCP	21	FTP Port
Send to Mail Recipient	TCP	25	SMTP Port
Send to Mail Recipient	TCP	465	ESMTP Port (SSL)

Component	Protocol	Port	Description
Send to SFTP	TCP	22	SFTP Port
HP OXPd	TCP	9000/4443, 7627	Device to Server – HTML UI
HP OXPd	TCP	7627	Server to Device – OXPd web service
Toshiba EWB and EBX	TCP	9000/4443	Device to Server – HTML UI
Toshiba EWB and EBX, OKI	TCP	50083, 9090, 443	Server to Device – WSDL SOAP Web Service
Toshiba EWB and EBX, OKI	SNMP	161	Server to Device – device management and validation
Kyocera	TCP	9000/4443	Device to Server – HTML UI
Kyocera	SNMP	161	Server to Device – device management and validation
Kyocera	TCP	9090, 443	Server to Device – WSDL SOAP Web Service
Kyocera	TCP	8080	Server to device – JAMP Servlet
Xerox	TCP	9000/4443	Device to Server – HTML UI
Xerox	SNMP	161	Server to Device – device management and validation
Xerox	TCP	80/443	Server to Device - device manager
Sharp OSA	TCP	9000/4443	Device to Server – HTML UI

Component	Protocol	Port	Description
Sharp OSA	TCP	80/443	Server to Device
Sharp OSA	SNMP	161	Server to Device – device management and validation
Samsung XOA	TCP	9000/4443, 161	Server to Device
Samsung XOA	SNMP	161	Server to Device – device management and validation
Samsung XOA	TCP	9090	Server to Device – WSDL SOAP Web Service
Lexmark	TCP	9000/4443, 161	Server to Device
Lexmark	SNMP	161	Server to Device – device management and validation
Lexmark	TCP	9090	Server to Device – WSDL SOAP Web Service
Konica	TCP	9000/4443	Server to Device – html UI
Konica	TCP	50666	Device to server – notification listener
Konica	TCP	50001/50003	Server to Device – OpenAPI
Konica	SNMP	161	Server to Device – device management and validation

Figure 13 Port Listing Table

10. Network bandwidth and usage

The amount of traffic between the MFPsecure/Scan server and the device can vary greatly depending on the specific job settings and the make/model of device that is communicating with the server. For instance, if the MFD is configured to send an uncompressed color TIFF rather than a compressed B&W PDF, the network traffic will be significantly higher.

The following section shows a sample of the average file sizes coming from the device in kilobytes.

	Dots Per Inch		
	Low	Medium	High
Mono	30 to 200 KB	100 to 500 KB	500 to 1500 KB
Greyscale	100 to 500 KB	300 to 1000 KB	1000 to 5000 KB
Colour	300 to 1000 KB	600 to 2000 KB	2000 to 7000 KB

11. MFPsecure/Scan Antivirus exclusions

Having an active antivirus software running while installing and running MFPsecure/Scan may lead to potential issues (including but not limited to performance hits while scanning). It is recommended to exclude the MFPsecure/Scan work, input and destination folders from anti-virus scanning, backup solutions and other software that lock files and directories.

Exclude the following file locations from anti-virus scanning and backup (if possible). If the file location is changed manually, make sure to adjust the file path accordingly.

Work and Input folders:

The work and input folders are subfolders in the installation path of the software:

- C:\Program Files\LRS\MFPsecure\Securescan

Troubleshooting AVS issues

In some cases it may be necessary to completely disable the AVS application on the server and work backwards. This was we can be sure that we have not gotten a false negative and have not gone far enough with the exclusions. For instance, with some applications you may need to exclude the SERVICE or the entire application folder.

12. Troubleshooting MFPsecure/Scan

There are debug logs available to view should you encounter any issues within MFPsecure/Scan.

To enable Debug mode, Go to Tools > Options > Advanced. Check the box next to Enable Debug Log, Press OK. When this is enabled the logging will be more verbose and the service will create a unique folder for each scan job so that the logs stay independent of other jobs.

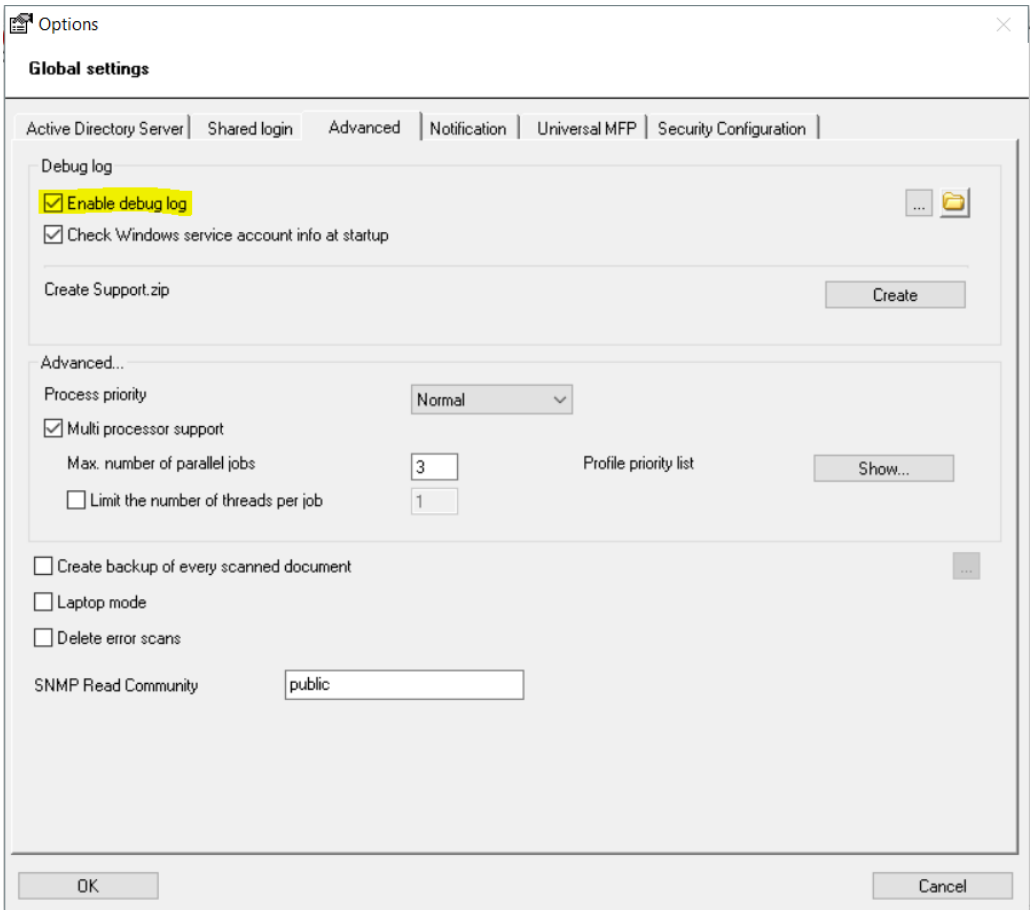


Figure 14 Enable Debug Logs

The logs for both the Windows service and the WS are available in the file location C:\Program Files\LRS\MFPsecure\securescan\Log.

To view the WS and Web logs there is a tool available to view and search rather than look through text files. This log viewer is located in C:\Program Files\LRS\MFPsecure\securescan\Tools

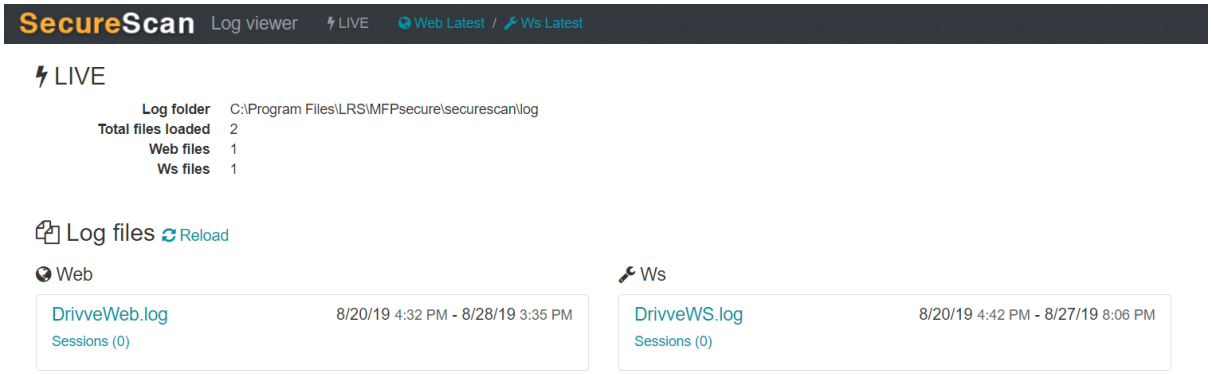


Figure 15 MFPsecure/Scan Log viewer

Should LRS support request the logs, you can use the Create Support.zip utility which is located in Tools > Options > Advanced. Choose 'Create' and the zip file will be created in the Log\zip files directory. This file includes settings and all logs.

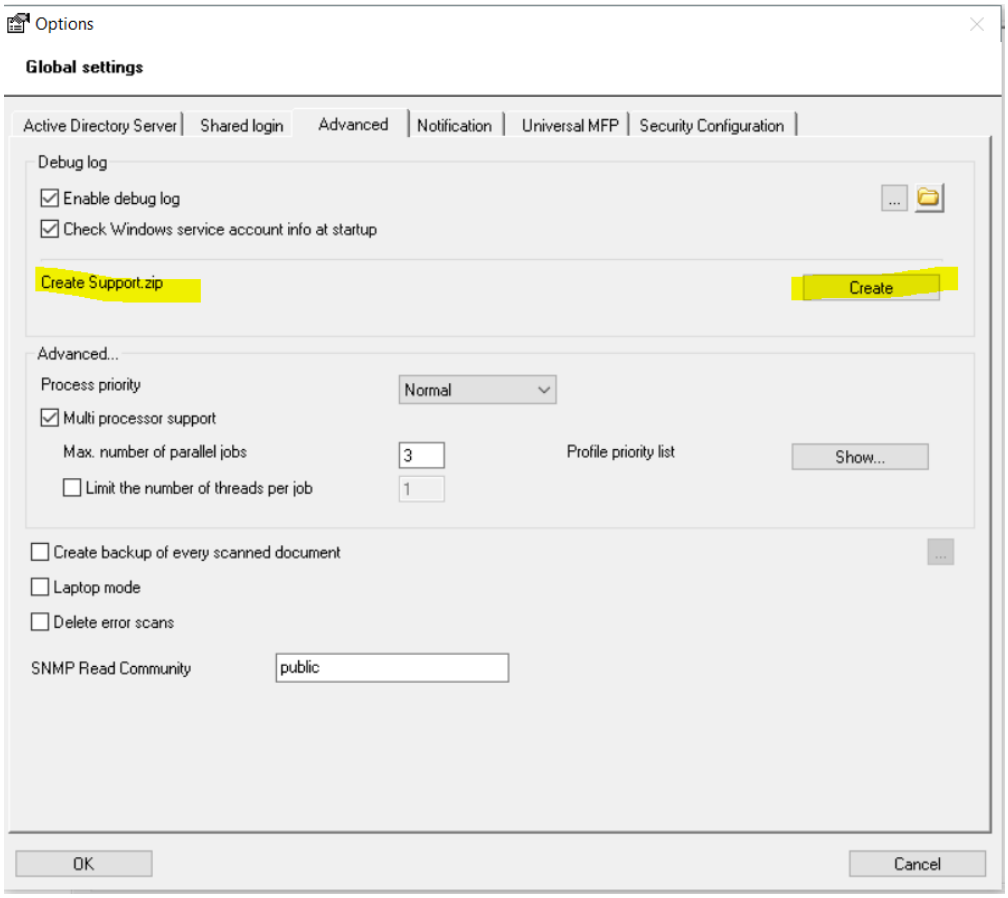
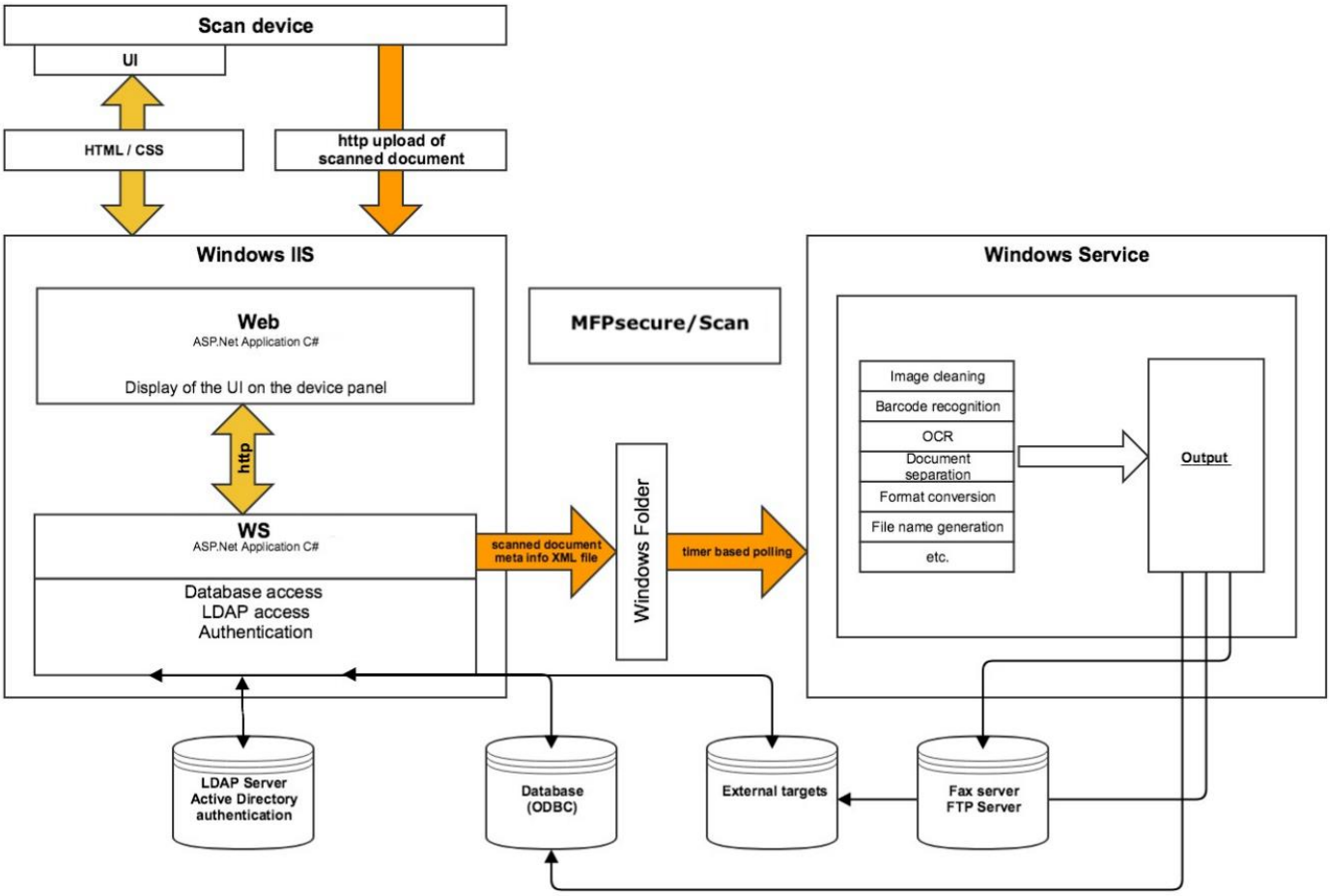
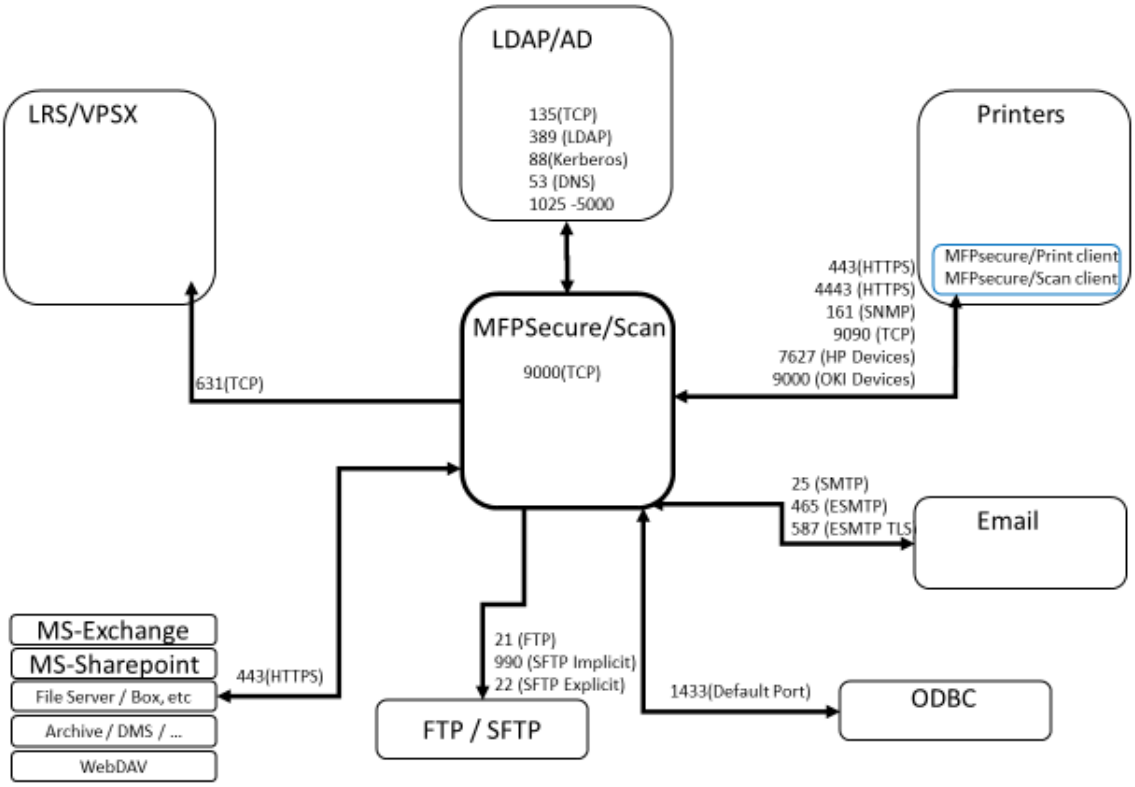


Figure 16 Create Support Logs

13. Appendix A MFPSecure/Scan Internal Architecture

The drawing below shows the architecture and workflow for scan.



14. Appendix B – Port Flow