

# LT Auditor+ Scanner – User Manual

1. Introduction .....	3
2. Application Overview.....	3
2.1. LT Auditor+ Scanner Manager.....	3
2.2. Scanner Agent Module .....	3
2.3. Scanner Reporting Module.....	3
3. Prerequisites .....	3
3.1. LT Auditor+ Scanner Manager.....	3
3.2. Scanner Agent Module .....	4
Windows Agent.....	4
Linux Agent.....	4
3.3. Reporting .....	4
3.4 Process Flow.....	4
3.5 LT Auditor+ Manager Installation.....	6
Step 1: Download and Unblock the Installation Package.....	6
Step 2: Extract the Installation Files .....	6
Step 4: Install the Scanner Manager .....	7
Step 5: Verify Installation.....	7
Step 6: Verify and Configure File Share.....	8
3.7 Setting Up LT Auditor+ Scanner Reports .....	9
Licensing Requirements.....	10
Steps to Set Up Power BI Reports .....	10
Setting Up Paginated Reports (Power BI Premium Per User).....	10
3.8 LT Auditor+ Scanner Agent Installation.....	12
Automated Installation Script .....	12
Manual Installation Steps .....	12
Installing the Agent on Windows Systems .....	13
3.8 Creating Scan Jobs .....	14
3.9 Reporting .....	17
Interactive Dashboard Overview .....	17
Export and Sharing Options.....	19
4.0 Troubleshooting - Logs .....	19

APPENDIX A – Power BI Gateway and Dashboard Setup.....	20
Install and Register Power BI Gateway .....	20
Configure SQL Server Connection on the Gateway .....	20
Upload Dashboard and Configure Semantic Model .....	20
Update Parameters and Map to Gateway Data Source .....	20
Configure Refresh Schedule .....	20
Share Reports and Manage Access .....	21
Note on Workspace Type for PPU Users.....	21

## 1. Introduction

This manual provides a comprehensive guide to installing, configuring, and using the LT Auditor+ Scanner, a module within the LT Auditor+ Suite, designed to identify and report PII (Personally Identifiable Information) and PHI (Protected Health Information) in documents across Windows and Linux systems.

## 2. Application Overview

The LT Auditor+ Scanner operates as a distributed system comprising three key components:

### 2.1. LT Auditor+ Scanner Manager

- Purpose: Central configuration and orchestration of scan jobs
- Platform: Must be installed on the Windows Server that hosts the LT Auditor+ Manager
- Functionality:
  - Manage scan job definitions
  - Assign scan jobs to agent nodes
  - Receive scan results for reporting

### 2.2. Scanner Agent Module

- Purpose: Performs actual scanning of files for PII/PHI
- Platform:
  - Windows Agents: Installed on Windows file servers
  - Linux Agents: Installed on Linux machines (e.g., SLES, Debian, Ubuntu)
- Functionality:
  - Polls for new job assignments
  - Scans local file systems or mounted shares
  - Returns structured results to the scanner

### 2.3. Scanner Reporting Module

- Purpose: Visualization and reporting of scan results
- Tool: Microsoft Power BI
- Functionality:
  - Prebuilt Power BI dashboards and reports
  - Reports uploaded to Power BI Service
  - Requires Power BI Pro or Premium licensing for access and sharing

## 3. Prerequisites

### 3.1. LT Auditor+ Scanner Manager

- Windows Server OS (> Windows Server >= 2019)
- LT Auditor+ Manager (Build 22 or later) installed

- .NET 8.0 Runtime
- Internet access (for Power BI and updates)
- Power BI Gateway (if using on-prem data sources)
- A user account (local or domain) with read/write access to the share created during installation
- Windows Authenticated access to the database

### 3.2. Scanner Agent Module

#### Windows Agent

- .NET Framework 4.7.2 or later
- Read access to folders to be scanned
- Network access to the scanner server

#### Linux Agent

- Python 3.10+
- OpenSSL Libraries
- Mounted share or local access to files
- Outbound connectivity to scanner server (HTTP/S or TCP)

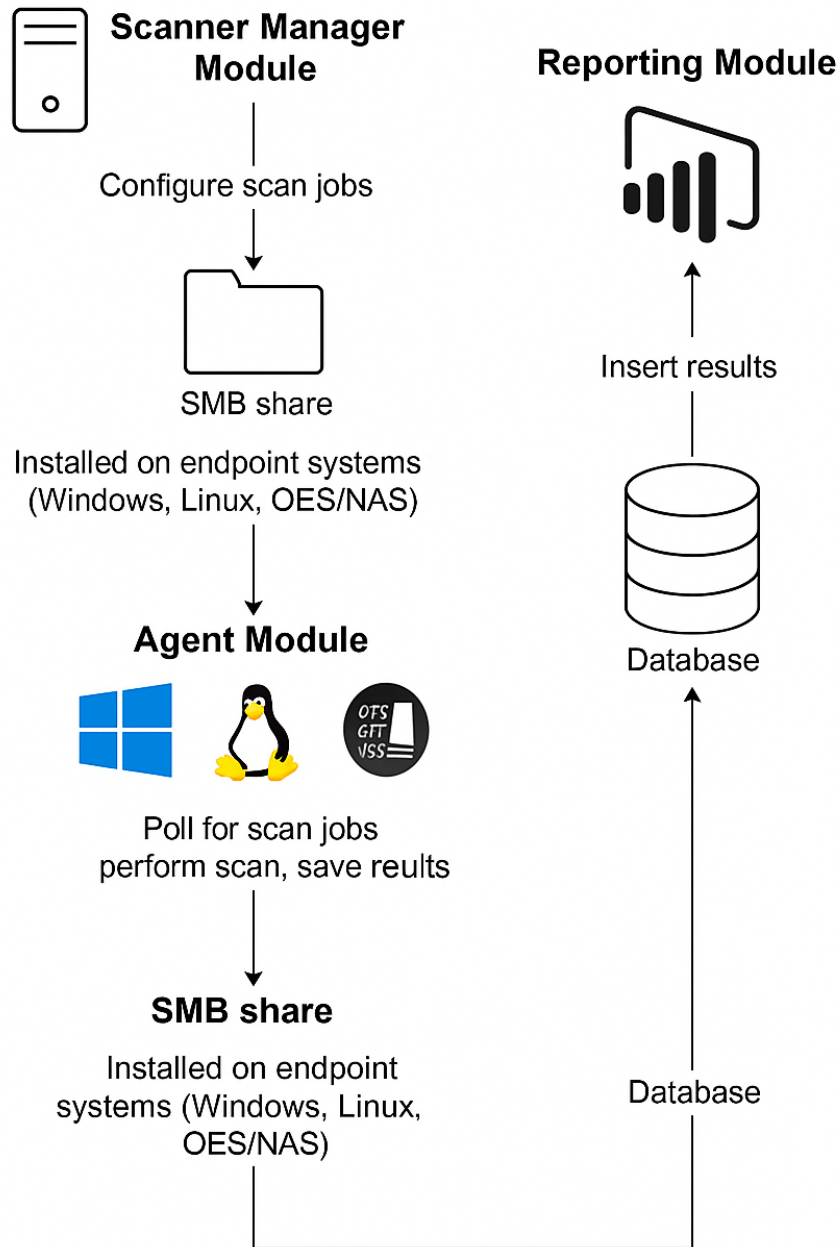
### 3.3. Reporting

- Power BI Desktop for report customization
- Power BI Service account
- Power BI Gateway installed and configured on the Scanner server (if needed)

### 3.4 Process Flow

The following schematic outlines the process flow of the application

## LT Auditor+ Scanner – Process Flow

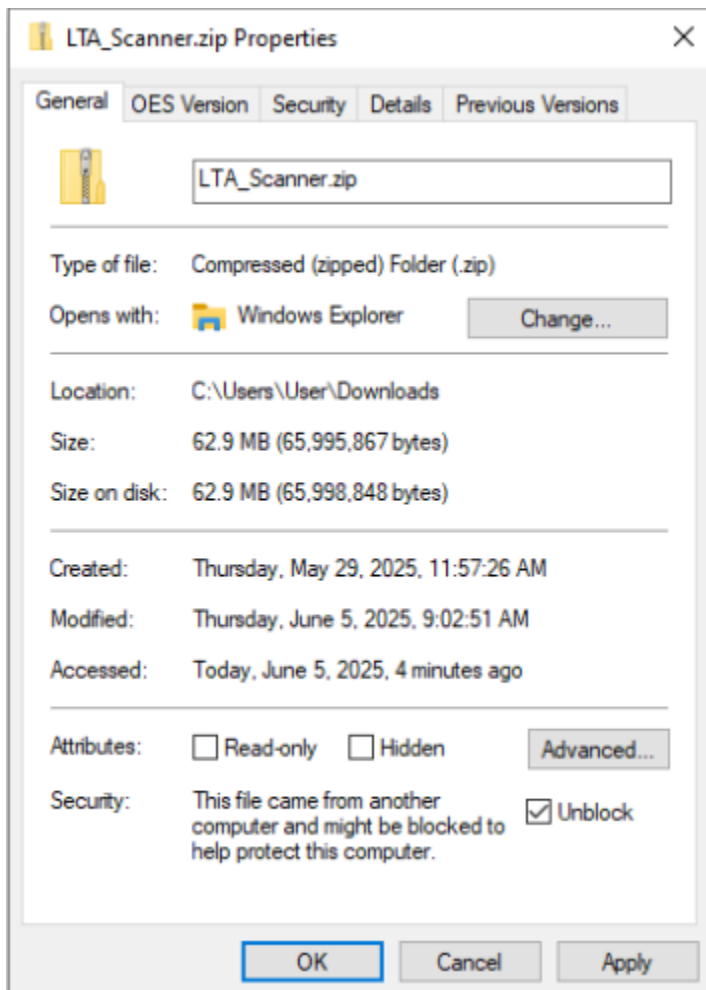


### 3.5 LT Auditor+ Manager Installation

To install the LT Auditor+ Scanner Manager, follow the steps outlined below.

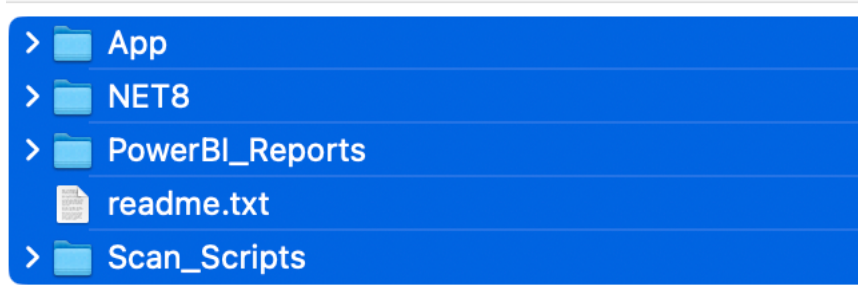
#### Step 1: Download and Unblock the Installation Package

1. Download the installation archive from the following location:  
[https://downloads.ltauditor.com/ltascanner/LTA\\_Scanner.zip](https://downloads.ltauditor.com/ltascanner/LTA_Scanner.zip)
2. Before extracting, right-click the downloaded .zip file, select Properties, and check the "Unblock" option if it is present. Then click Apply and OK.



#### Step 2: Extract the Installation Files

1. Extract the ZIP file to a folder of your choice.
2. The extracted directory will include the following structure:



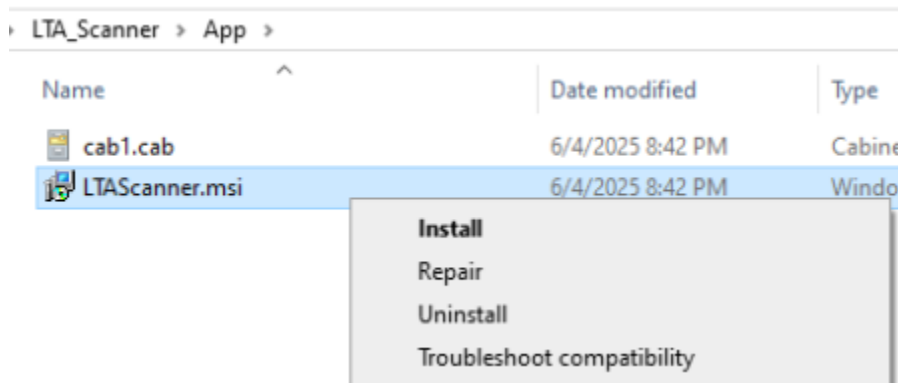
### Step 3: Pre-Installation Checklist

Before proceeding with the installation, ensure the following prerequisites are met:

- LT Auditor+ Manager is already installed on the server.
- NET 8 Runtime is installed. If not, run the installer located in the NET8 folder:  
windowsdesktop-runtime-8.0.16-win-x64.exe

### Step 4: Install the Scanner Manager

1. Navigate to the App directory.
2. Right-click on LTA\_Scanner.msi and select Install.



Upon successful installation, the application will reside in the following directory:

\\Program Files\Blue Lance, Inc\LT Auditor+\Security Management Farmwork\LTAScanner


A Windows service named LT Auditor+ Sensitive Data Scanner will also be registered. This service must be able to connect to the LT Auditor+ database.

### Step 5: Verify Installation

To confirm successful installation and database connectivity:



- Open the log file located at:  
\\Program Files\Blue Lance, Inc\LT Auditor+\Security Management Farmwork\LTAScanner\logs\
- Locate the latest srv-log-<date>.log file.
- Scroll to the bottom of the log and verify that a successful connection message is displayed.

Local Disk (C:) > Program Files > Blue Lance, Inc > LT Auditor+ > Security Management Framework > LTAScanner > Logs			
Name	Date modified	Type	Size
 srv-log-20250605.log	6/5/2025 9:34 AM	Text Document	8 KB





2025-06-06 08:18:35 [Information] Successfully connected to database

### Step 6: Verify and Configure File Share

The installation process automatically creates a shared folder named:

<HOSTMACHINE>\_scanner in:

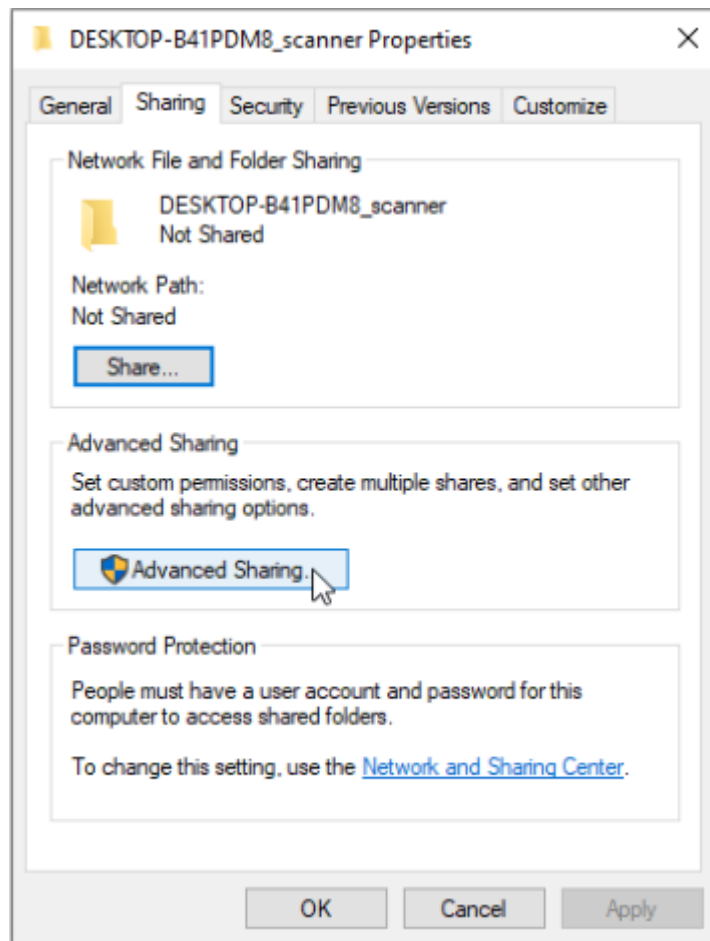
\\Program Files\Blue Lance, Inc\LT Auditor+\Security Management Farmwork\LTAScanner

s > Blue Lance, Inc > LT Auditor+ > Security Management Framework > LTAScanner			
Name	Date modified	Type	Size
 bin	6/5/2025 9:23 AM	File folder	
 DESKTOP-B41PDM8_scanner	6/5/2025 8:18 AM	File folder	
 Jobs	6/5/2025 9:12 AM	File folder	
 Logs	6/5/2025 9:39 AM	File folder	

This shared folder must be accessible by agent machines. Assign read and write permissions to a local or domain user account that will be used by the agents to transfer job and result files.

To configure permissions:

- Right-click the folder and select Properties.
- Go to the Sharing tab and click Advanced Sharing.
- Enable sharing and click Permissions to assign read/write access to the required user.



- Next, switch to the Security tab and ensure that the same user has NTFS-level read and write permissions.

### 3.7 Setting Up LT Auditor+ Scanner Reports

LT Auditor+ Scanner utilizes Microsoft Power BI Service for reporting sensitive data scan results. To use this functionality, appropriate Microsoft 365 and Power BI licenses are required.

### Licensing Requirements

- A Microsoft 365 account and an associated Power BI license are required.
- At a minimum, a Power BI Pro license is necessary to view and interact with dashboards.
- Users with a Power BI Premium Per User (PPU) license can access Paginated Reports for enhanced reporting.
- Please verify your license status with your Microsoft 365 Administrator.
- Any user who needs to access reports must be assigned the appropriate Power BI license by Microsoft.

### Steps to Set Up Power BI Reports

1. Power BI Gateway Setup – If your organization does not already have a gateway, refer to Appendix A below to install and configure the Power BI Gateway.
2. Configure SQL Database Connection - Configure a SQL Server data source on the Power BI Gateway pointing to the LT Auditor+ database.
3. Upload the Dashboard File - In Power BI Service, either create or navigate to your desired Workspace and upload the dashboard file 'LT Auditor+ Sensitive Data Scans.pbix' from the PowerBI\_Reports\Dashboards folder.
4. Configure the Semantic Model - After uploading, open the semantic model settings and configure the following
  - a. Parameters:
    - i. SQL Server Name
    - ii. Database Name: Default is LTAProductionDB
    - iii. Prior Days: Default is 30
    - iv. Gateway Connection - Map the model to the configured SQL data source.
    - v. Scheduled Refresh:
      - Enable data refresh
      - Set the schedule to refresh every 4 hours or as required

### Setting Up Paginated Reports (Power BI Premium Per User)

1. Run PowerShell Setup Script
  - a. Open PowerShell with Administrator privileges.
  - b. Execute 'InstallPowerBIReports.ps1' located in the PowerBI\_Reports folder.
  - c. Provide Required Inputs:
    - i. SQL Server name.
    - ii. Database name.
    - iii. Authentication type (Windows or SQL).
    - iv. The script will test the connection and, if successful:

- Create the required stored procedure,
  - Update the file 'LT Auditor+ Sensitive Data Reports.rdl' with the connection details.
2. Upload Paginated Report - Upload the updated .rdl file to the same Power BI workspace used for the dashboardext4

## 3.8 LT Auditor+ Scanner Agent Installation

### Automated Installation Script

The provided automated script has been tested on Debian, Ubuntu, and SUSE-based Linux distributions. For other Linux distributions, a manual installation is recommended.

1. Download the installation package from  
[https://downloads.ltauditor.com/ltascanner/LTA\\_Scanner.zip](https://downloads.ltauditor.com/ltascanner/LTA_Scanner.zip).
2. Extract the archive and navigate to the 'Scan\_Scripts' directory in a terminal.
3. Run the following command to make the scripts executable:  

```
sudo chmod +x *.sh
```
4. Start the installation using:  

```
sudo ./install.sh
```
5. Follow the prompts to enter the SMB share username, domain, and full UNC path (e.g., [\\192.168.1.10\share](#)). This share was set up in Step 6 in Section 3.5 above.
6. The script will verify the Python version (must be 3.10 or higher) and prompt to upgrade if necessary.
7. The script will also install required dependencies (e.g., pip, venv) and the Python libraries.
8. You will be prompted to enter the password for the SMB user; it will be securely encrypted.
9. Upon completion, the service will be registered and started. Confirm it is running with:  

```
sudo systemctl status lta-scanner.service
```

### Manual Installation Steps

1. Download and extract the agent package from:  
[https://downloads.ltauditor.com/ltascanner/LTA\\_Scanner.zip](https://downloads.ltauditor.com/ltascanner/LTA_Scanner.zip)
2. Ensure Python 3.10 or later installed python3 version.
3. Install required tools (pip, venv) and Python libraries:  

```
python3 -m pip install -r requirements.txt.
```
4. Create the following directory structure:
  - a. /opt/bluelance/scanner/logs
  - b. /opt/bluelance/scanner/certs
  - c. /opt/bluelance/scanner/mnt.
5. Copy all Python scripts and daemon\_setup.sh to /opt/bluelance/scanner.
6. (Optional) Set up a Python virtual environment:
  - a. 

```
python3 -m venv PII;
```
  - b. 

```
source PII/bin/activate;
```
  - c. 

```
python3 -m pip install -r requirements.txt;
```
7. Run setup.py and provide the password when prompted (stored encrypted).
8. Update the interpreter path in daemon\_setup.sh if needed (line 6).
9. Run the daemon setup script:

```
sudo ./daemon_setup.sh
```

10. Upon completion, the service will be registered and started. Confirm it is running with:

```
sudo systemctl status lta-scanner.service
```

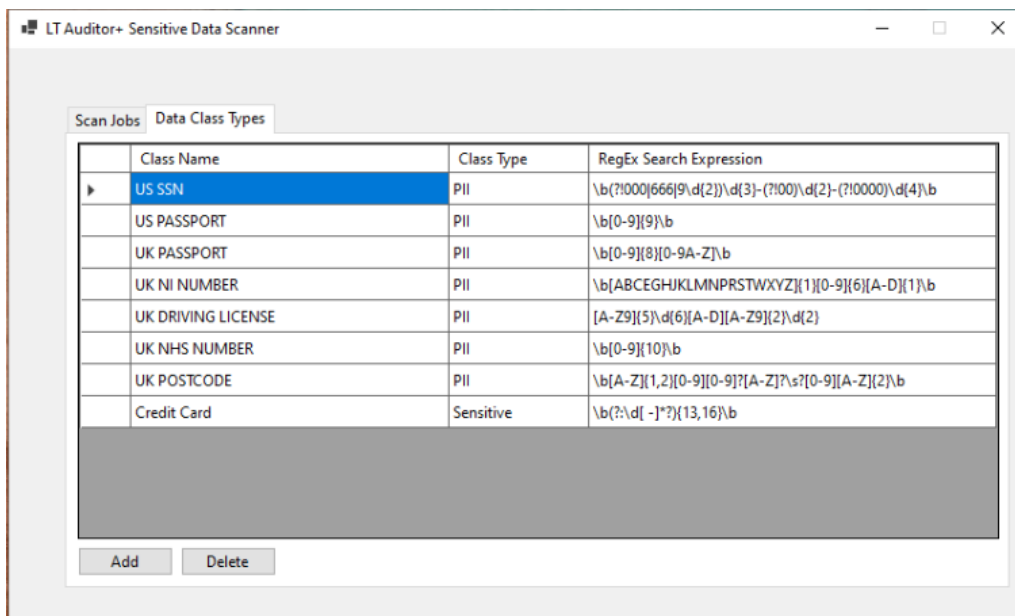
## Installing the Agent on Windows Systems

1. Download the installation ZIP from:  
[https://downloads.ltauditor.com/lta-scanner/LTA\\_Scanner.zip](https://downloads.ltauditor.com/lta-scanner/LTA_Scanner.zip)
2. Right-click the ZIP file, select 'Properties', and check 'Unblock' before extracting.
3. Extract the contents and open Command Prompt or PowerShell.
4. Navigate to the 'Scan\_Scripts' directory.
5. Ensure Python 3.10 or above is installed and accessible.
6. Install required Python libraries:  

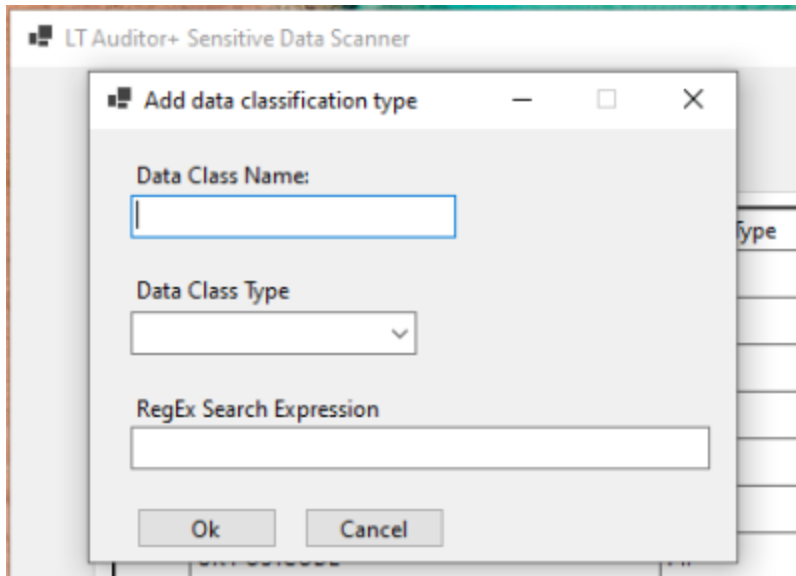
```
python -m pip install -r requirements.txt
```
7. Configure agent parameters and SMB credentials.
8. Launch the agent manually or register it as a Windows service.

## 3.7 Creating Data Class Types

LT Auditor+ Sensitive Data Scanner has several default data class types.



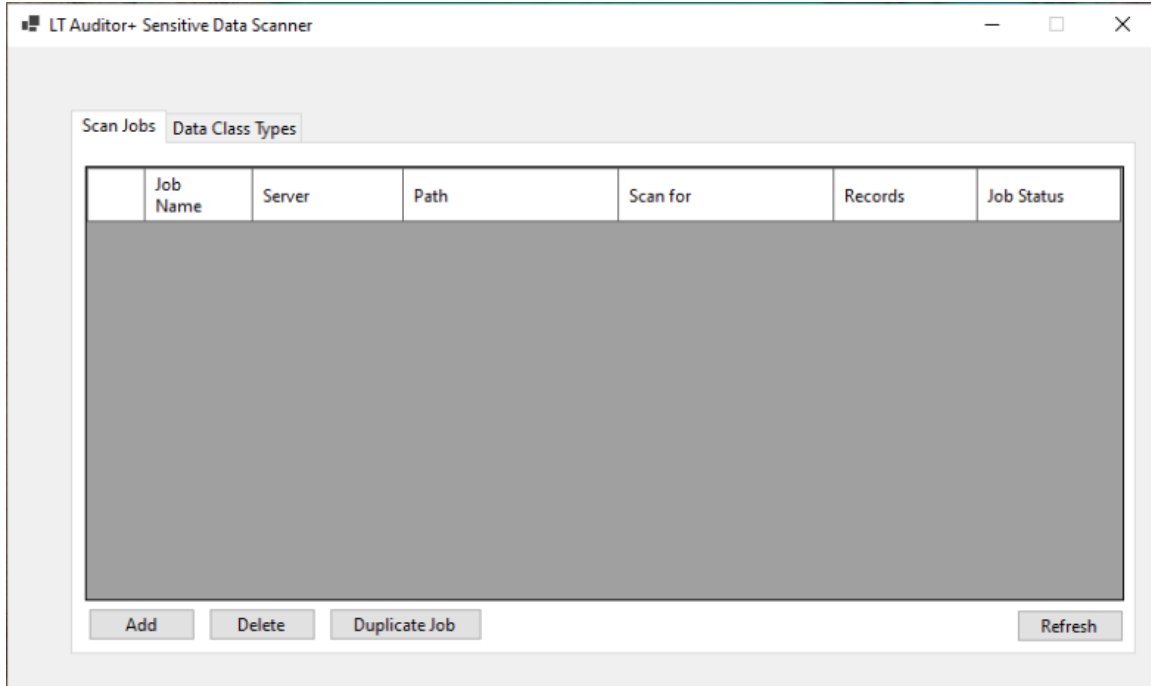
To create your own data class type, click the add button.

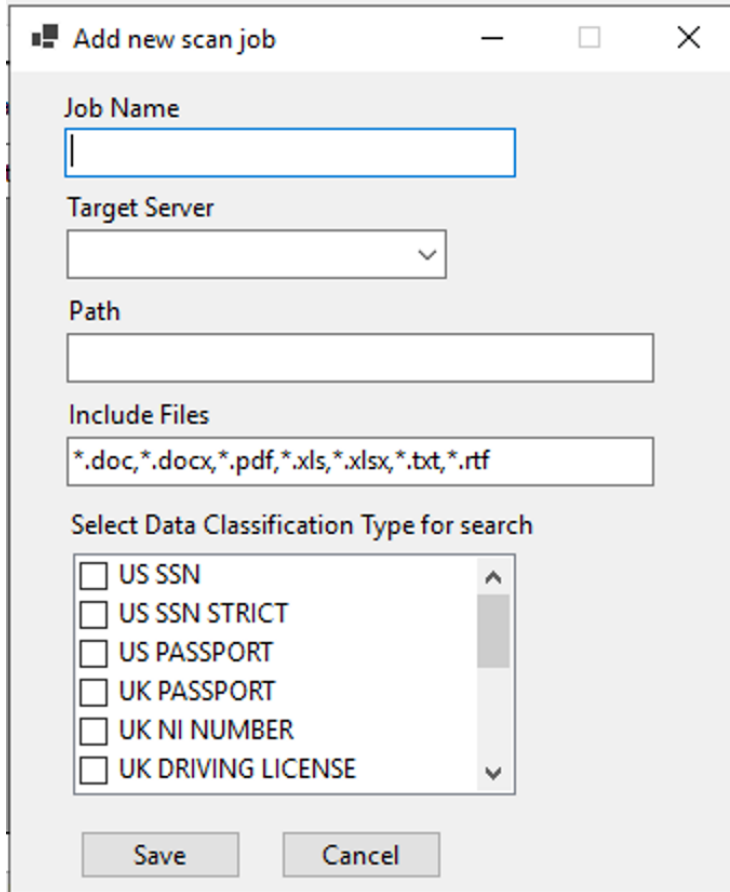


Enter a Name, A class type, and the Regex search pattern. Then hit Ok. This will add your data class type to the list.

### 3.8 Creating Scan Jobs

To create a scan job hit the 'Add' button from the LT Auditor+ Sensitive Data Scanner program.





**Add new scan job**

Job Name

Target Server

Path

Include Files

Select Data Classification Type for search

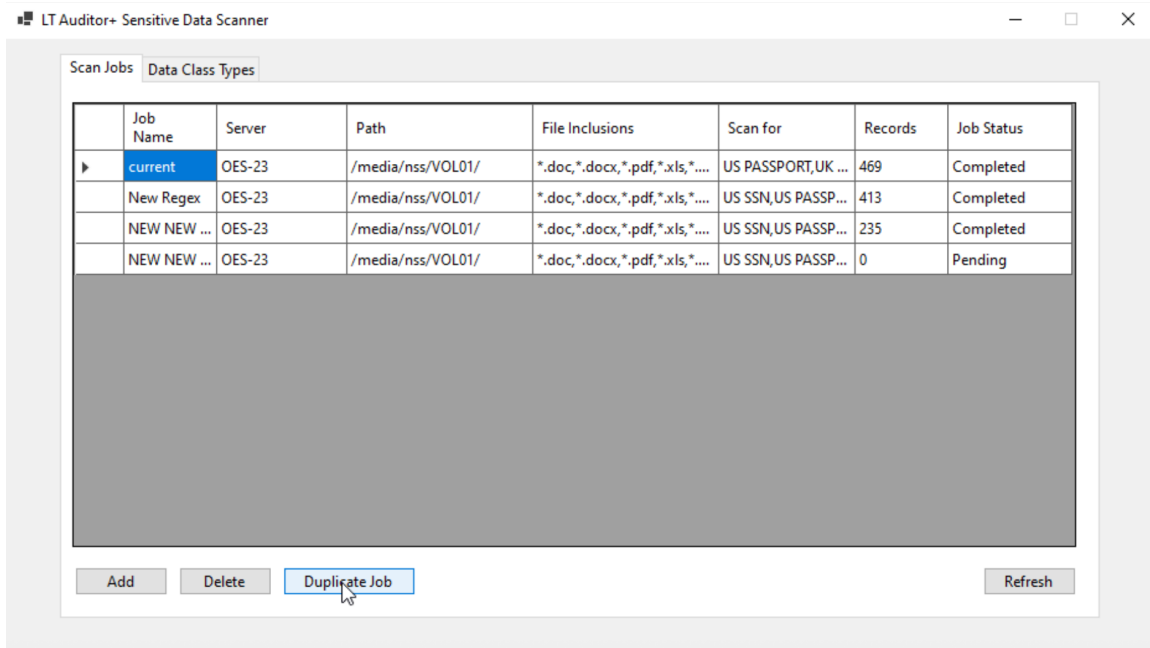
- ☐ US SSN
- ☐ US SSN STRICT
- ☐ US PASSPORT
- ☐ UK PASSPORT
- ☐ UK NI NUMBER
- ☐ UK DRIVING LICENSE

Save Cancel

Enter a Name for the Job, select a Server from the drop-down menu, enter the directory to scan, types of files to scan and then select the Data Classifications you would like to scan for. To scan all files, enter \*.\* in the **Include Files** field. To include files without extensions, use the keyword [noext]. For example, to scan for PDF files, Word documents, and files with no extensions, enter: \*.pdf, \*.docx, [noext]

After hitting the save button, the program will add the job to the Job list, and the Agent will start the scan shortly after.





After the scan is done, the Agent will output a CSV file that will be inserted into the Database, and the Job list will update. You may have to press the 'Refresh' button to see the updated Job list.

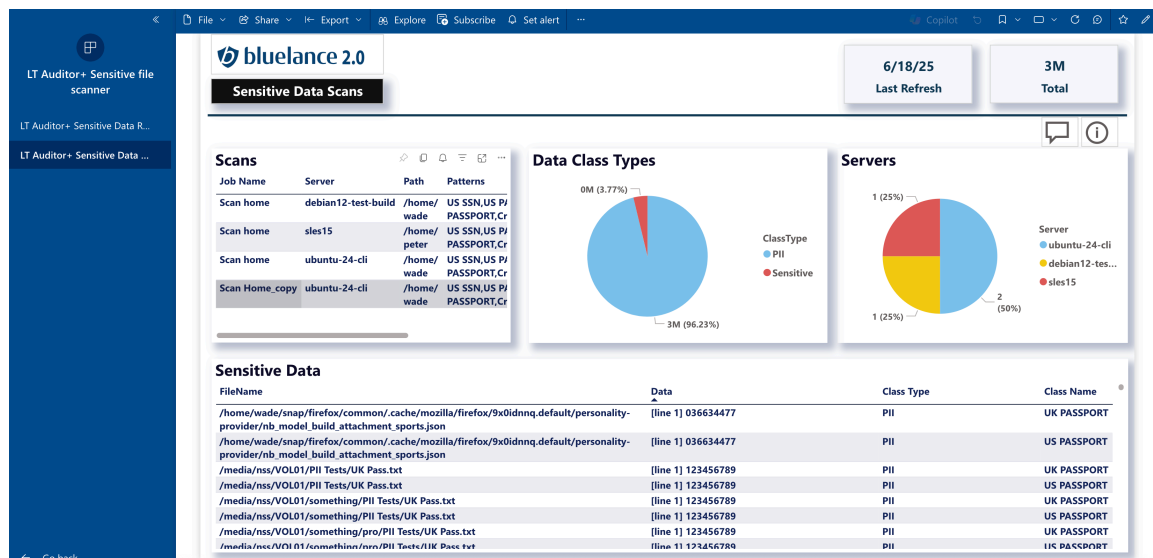
If the Job list is already populated, you can create a job with the 'Duplicate Job' Button. To Duplicate a job select it, then press the 'Duplicate Job' Button.

This will create a new job with the same server, path, and Data Classifications.

### 3.9 Reporting

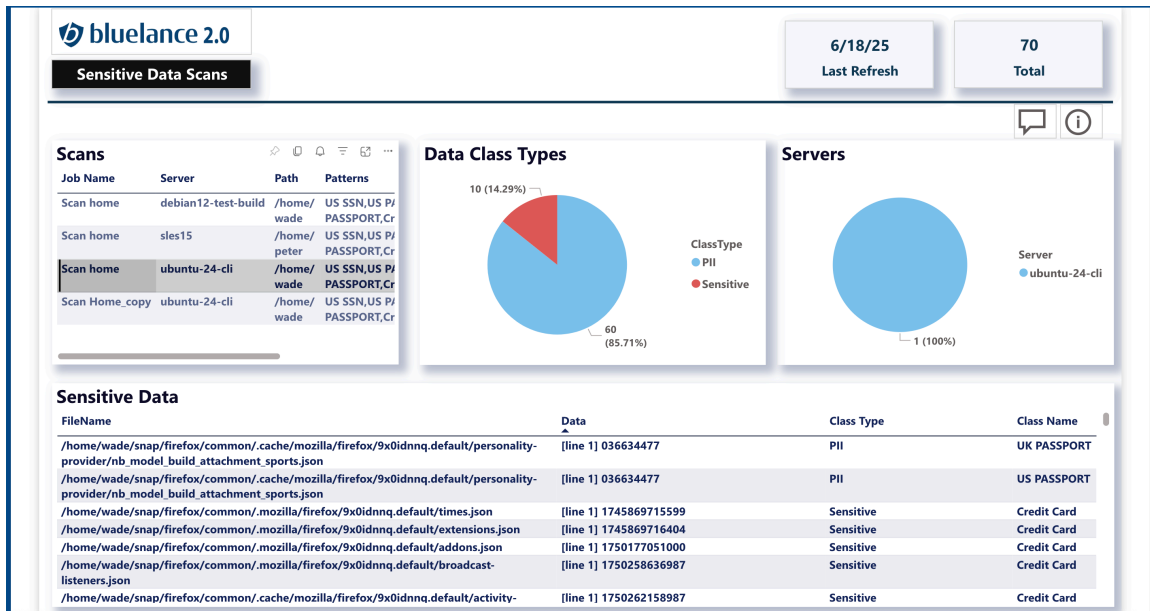
Once the Power BI reports have been installed and configured, users can access and view them via the Microsoft Power BI Service. Typically, a Power BI App will be created within a workspace to streamline report access.

The App typically includes one or more interactive dashboards, including the LT Auditor+ Sensitive Data Dashboard, which presents a high-level summary of scan activity and detailed findings.



### Interactive Dashboard Overview

The main dashboard provides a summary of all scans performed. Users can click on a specific scan entry to drill down into its details, such as detected PII/PHI patterns, file paths, and other metadata.



The results are displayed in a grid format showing all sensitive data identified during the scan. To filter results, click anywhere inside the grid and then select the 'Filter' option from the top-right menu. This enables dynamic querying based on specific attributes (e.g., data type, path, file name).

**Filters** »

Search

Filters on this visual ...

Class Name  
is (All)

Class Type  
is (All)

Data  
is (All)

FileName  
is (All)

## Export and Sharing Options

Filtered or full scan result sets can be exported directly from the dashboard to CSV or PDF formats using the export feature in the Power BI toolbar.

Additionally, the dashboard can be embedded into Microsoft Teams channels for collaborative access. Users with appropriate permissions can also share the dashboard or app with other users within the organization.

## 4.0 Troubleshooting - Logs

There are logs for both the Auditor+ Manager and the Agent. The log location for the Auditor+ Manager is within this folder:

```
C:\Program Files\Blue Lance, inc\LT Auditor+\Security Management  
Farmwork\LTAScanner\logs
```

The log location for the Agent for Linux is:

```
/opt/bluelance/scanner/logs
```

These logs are very important for troubleshooting issues.

## APPENDIX A – Power BI Gateway and Dashboard Setup

The following sections detail how to set up the Power BI Gateway and create a database connection to view reports.

### Install and Register Power BI Gateway

1. Download the Power BI Gateway installer from:  
<https://powerbi.microsoft.com/en-us/gateway/>
2. Run the installer and select 'On-premises data gateway (recommended)'.
3. Sign in with your Power BI service account to register the gateway.
4. Complete the configuration by assigning the gateway to your organization.

### Configure SQL Server Connection on the Gateway

1. Sign in to Power BI Service at <https://app.powerbi.com>.
2. Navigate to 'Settings' > 'Manage gateways'.
3. Select your registered gateway.
4. Click 'Add data source'
5. Provide the following information:
  - Data Source Type: SQL Server
  - Server and Database name
  - Authentication method (Windows or Basic)
  - Credentials with read access to the database
6. Save the configuration and verify that the data source status is 'Online'.

### Upload Dashboard and Configure Semantic Model

1. Upload the .pbix file to your desired workspace in Power BI Service.
2. After the upload, go to 'Datasets + dataflows' in the workspace.
3. Click the 'Settings' icon next to the uploaded semantic model.

### Update Parameters and Map to Gateway Data Source

1. In the settings page of the semantic model:
  - Under 'Parameters', modify any environment-specific values (e.g., server names).
  - Click 'Apply' after updating parameters.
2. Under 'Gateway connection', select the registered gateway.
3. Use the mapping tool to link the semantic model's data source to the correct gateway data source.
4. Ensure that credentials are authorized and valid.

### Configure Refresh Schedule

1. In the same settings page, scroll to the 'Scheduled refresh' section.
2. Enable 'Keep data updated'.
3. Configure the following:
  - Frequency (e.g., daily, multiple times per day)

- Time zone and preferred refresh times
  - Email notification for failures
4. Click 'Apply' to activate the refresh schedule.

## Share Reports and Manage Access

1. To grant access to users:
  - Navigate to the Workspace in Power BI Service.
  - Click on 'Workspace settings' > 'Permissions'.
  - Use 'Add people' to invite users.
  - Assign appropriate permissions:
    - Viewer: Can only view reports and dashboards.
    - Member or Contributor: Can edit content, depending on the assigned role.
  - All users must have the appropriate Power BI license (Pro or PPU).
2. To create an App from the Workspace:
  - In Power BI Service, open the target Workspace.
  - Click on 'Create app' from the top menu.
  - Configure the app name, description, and navigation layout.
  - In the 'Audience' section, define who can access the app (individual users, groups, or entire organization).
  - Click 'Publish app' to distribute.
  - Users will access reports via the app without needing direct access to the Workspace.

## Note on Workspace Type for PPU Users

If your organization uses Power BI Premium Per User (PPU) licensing and intends to publish paginated (.rdl) reports, you must ensure that the Workspace is created as a 'PPU-enabled workspace'.

- When creating the Workspace, under 'Advanced', select 'Premium capacity: Premium per user'.
- Only PPU-enabled Workspaces support publishing and viewing of paginated reports (.rdl).