pitney bowes

Ship & Mail
Mailing Software

Relay Unify uSecure & uProtect

User Guide

US English Edition
January 2025

Table of Contents

Introduction

Security is quickly becoming the most significant issue in the industry, and we believe it will continue to increase in significance. More compliance laws are coming out every day and the penalties are becoming more expensive and more publicized. Customers are looking for ways to decrease the risk associated with regulatory compliance regarding security of confidential data, as well as create opportunities for new business. As with any customer considering outsourcing the delivery of critical and confidential information, they are primarily focused on two key areas of concern: A) Quality Control Procedures and B) Data Security. Relay Unify uSecure was born from the need to better address industry-critical issues specific to Data Security – how to persistently protect confidential data and limit the risk associated with regulatory compliance. It's a digital protection technology not previously available for protecting digital assets. We feel that this addition further sets Relay™ Unify, Powered by Transformations apart from any other solution on the market with the ability to offer protection that travels with the file keeping data protected at all times; we call this technology Smart Data. In addition, it offers true closed-loop protection from file receipt to output management along with full audit capabilities regarding data access among many other unique features. The technology greatly minimizes an organization's exposure to compliance violations and fines (i.e. HIPAA). It is also a true differentiator for those looking to minimize risk while gaining a significant competitive advantage around true data protection.

Relay Unify uSecure is an entirely new approach to data security. Instead of following the traditional approach of placing data within silos and requiring keys to encrypt and decrypt it for processing or to make changes, Relay Unify uSecure embeds an intelligent data object with 256-bit AES encryption that travels with each data file. The intelligent object lets users control the network and server on which data can be accessed. Only Relay Unify uSecure enabled applications can access the data when all verification parameters, as set by the data owner, are satisfied. These may include whether access is within a permitted time frame, a certain location, or is within the correct application. If an attempt is made to move files from a production network to removable media or a personal or unauthorized machine, access is denied and the attempt logged and reported. The intelligent security object offers full audit capabilities by logging all access of who, what, when, and where, along with detailed forensics such as machine UUID, IP address, hardware and software serial numbers. Controlling accessible locations from within the data is the only way to ensure that a file is used correctly, and Relay Unify uSecure ensures optimal security and authentication for when and where data can be accessed and used.

The current pricing model for Relay Unify uSecure is on a per client usage basis (nothing to pay upfront).

Relay Unify uSecure pricing is based on the number of customers you require to use it and the size of their files. For example, you would have a fixed monthly fee (base) for the set amount of customer licenses. There would then be an additional cost per secured record. We are pricing it anywhere from $150 to $250 a month per customer license (your customer…….data owner) and $0.002-$0.01 per record secured. This was the best way for us to manage costs across different customer sizes. Pricing is flexible and can be reduced for many required licenses.

Item Description	Monthly License Fee Per Data Owner	Per Record Secured Charge
Relay Unify® - Relay Unify uSecure	**$150-$250**	**$0.003-$0.01**

Implementation Summary

1. Install Relay Unify uSecure.
2. Request a global level license.
3. Request a customer level license.
4. Setup client level security settings.
5. Setup submission level security settings.
6. Install Relay Unify uProtect at your client's site, so the data files you receive are already encrypted.

Submit data files as part of a secure workflow!

Requirements

UXPHOME environment variable

The user running Relay Unify uSecure must be able to access the UXPHOME environment variable. This variable must point to a directory that contains the file smartfile.rsf. The directory should also include subdirectories Data, Log, and Queue. The Data subdirectory should contain the file watch.dat. The Queue subdirectory should contain the file watch.dat. After the UXPHOME variable is setup, the server will have to be rebooted.

Relay Unify uSecure DLL's

The following DLL's must be in the directory where the programs are located. The directory must be read/write.

icudt52.dll
icuin52.dll
icuuc52.dll
libeay32.dll
libgcc_s_dw2-1.dll
libGLE.dll
libGLESv2.dll
libstdc++-6.dll
libwinpthread-1.dll
msvcp100.dll
msvcp110.dll
msvcp120.dll
msvcr100.dll
msvcr110.dll
msvcr120.dll
Qt5Core.dll
Qt5Gui.dll
Qt5Network.dll
Qt5Widgets.dll
Qt5Xml.dll
SmartFileApi1.dll
Ssleay32.dll
Relay UnifyUXP.dll
wpsapi.dll

All must be the same bitness. The bitness must match the program bitness. To check the bitness you can run Relay Unify Ver program in the directory. It will generate a list of all the programs and DLL's in the directory and subdirectory.

Relay Unify uProtect also uses Libeay32.dll and ssleay32.dll for testing Email settings.

A license File (.lic) must also be present.

To access Relay Unify uSecure documents, the following programs require the dlls:
Relay Unify uCompose.exe UBrkpackapp.exe RPprintapp.exe Pngdll.dll URecsub.exe UQueFile.exe Relay Unify uProtect.exe

Relay Unify uSecure License

The Relay Unify uSecure License file, Relay Unify uSecurePSPLic.lic must be in the directory with the programs. This file is the PSP Relay Unify uSecure License file. The DLL's will load, but Relay Unify uSecure will not work without this file. The Relay Unify uCompose, rpprintapp, Ubrkpackapp and pngdll.dll programs should create this file (if necessary) if Relay Unify uSecure is properly set up.

The directory where the programs and dll's reside should be read/write. Some Relay Unify uSecure functions may attempt to write information to the license file.

Logging

For most Relay Unify uSecure programs a log file will be created during processing. The file will be in the logfiles subdirectory. In most cases if no error occurs the log files will be deleted. If any error occurs the log file will remain.

For most programs the Logfile will be name UXP_YYYYMMDDHHMMSSmmm.log. For Urecsub the file will be UrecSubYYYYMMDDHHMMSS_submid.log. Expanded Logging can be enabled for Urecsub by editing the DBSERVICES.ini file and setting Urecsub logging to 1

[URecSub]

Logging=1

Programs

Relay Unify uProtect.exe
Secures the data using Relay Unify uSecure.

URecsub.exe
Reads the Relay Unify uSecure Data and processes into Relay Unify. This program is called automatically. It will be in the same directory as the RPSubFTPSrv.exe (Relay Unify FTP Service Program)

UBrkpackapp.exe
Reads the Relay Unify uSecure Data and Populates the Database with Document Information. This program is called automatically. It will be in the same directory as the BrkPackSrv.exe (Relay Unify Breakpack Service Program)

UPrintapp.exe
Reads the Relay Unify uSecure data and Database and generates output print stream. If the Print Stream is sent to Relay UnifyPM (Relay Unify Print Manager) then the Print Stream is secured using Relay Unify uSecure. This program is called automatically. It will be in the same directory as the RPPrintSrv.exe (Relay Unify Print Service Program)

Pngdll.dll
Generates PNG's or PDF's on the Web for Relay Unify uSecure Documents. This is called by the Web program automatically. It will be in the Datascripts directory of the Web3 system.

UQueFile
In using Relay UnifyPM (Relay Unify Print Manager) this program moves the Print Stream to the Printer. This program is called automatically. It will be in the same directory as the Relay UnifyPQSvr.exe (Relay Unify Print Queue Service Program)

Install and Configure Relay Unify uSecure

Before installing, upgrade the system and databases to the latest version of Relay Unify.

DLLs

Backup programs that use Relay Unify uSecure: Relay Unify uCompose.exe, uSetup, RPPrintapp.exe, and PNGDLL.dll.

The following have a new version to work with Relay Unify uSecure: RPSubFTPSrv.exe, RPSubWebSrv.exe, Relay UnifyPQSvr.exe, uQueFile.exe, and urecsub.exe.

Replace the Relay Unify uCompose.exe and uSetup in the Main Relay Unify directory.

In the Programs directory replace Rpprintapp.exe, Rpsubftpsrv.exe, Rpsubwebsrv.exe, Relay Unifypqsvr.exe, and Uquefile.exe.

Install urecsub.exe to the directory where rpsubftpsrv.exe and rpsubwebsrv.exe are located.

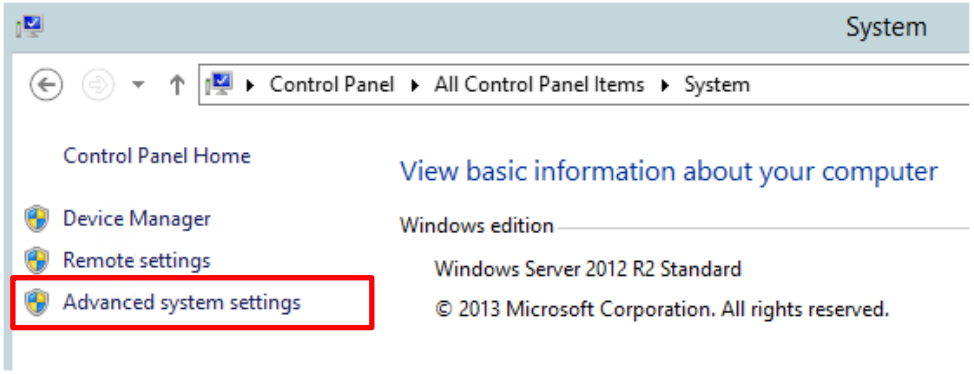
In the Web directory (datascripts for web30) replace pngdll.dll with the latest version.

The common dlls must be copied into the directory where any of the Relay Unify uSecure programs are running. Make sure the directory allows the users running the programs to edit files in the directory. The file TI-sdk.lic must be editable by the programs.

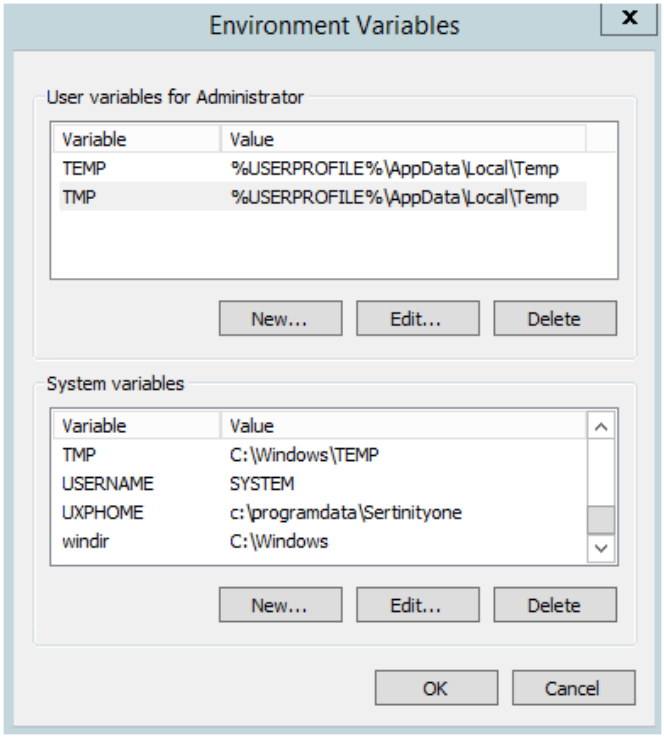
Setup UXPHome Environment Variable

Relay Unify uSecure requires that each system have an environment variable named UXPHome be setup.

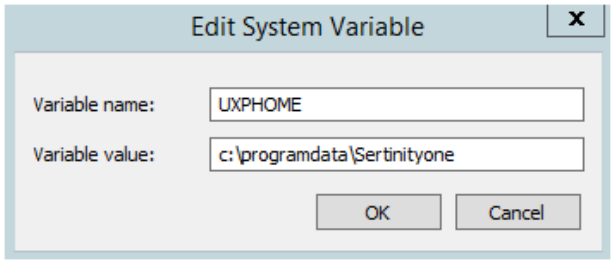
Go to the System control panel and select Advanced System settings



Then click on the environment Variables button.



In the System Variables section verify that UXPHOME does not exist and add the variable.

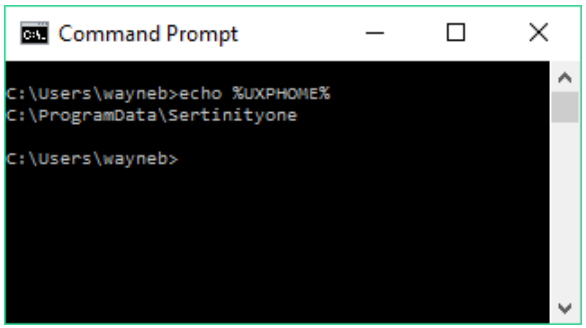


Set the Variable value to the location of the main Relay Unify Directory (where Relay Unify uCompose.exe exists).

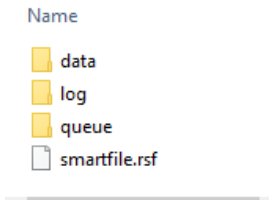
A UXPHOME Environment Variable is required. It must point to the Sertinity one directory.

To check for the UXPHOME Environment variable open a Cmd Window and type the following:

Echo %UXPHOME%



The UXPHOME Environment variable will point to the directory that contains smartfile.rsf and 3 directories. The directories are data, log and queue.

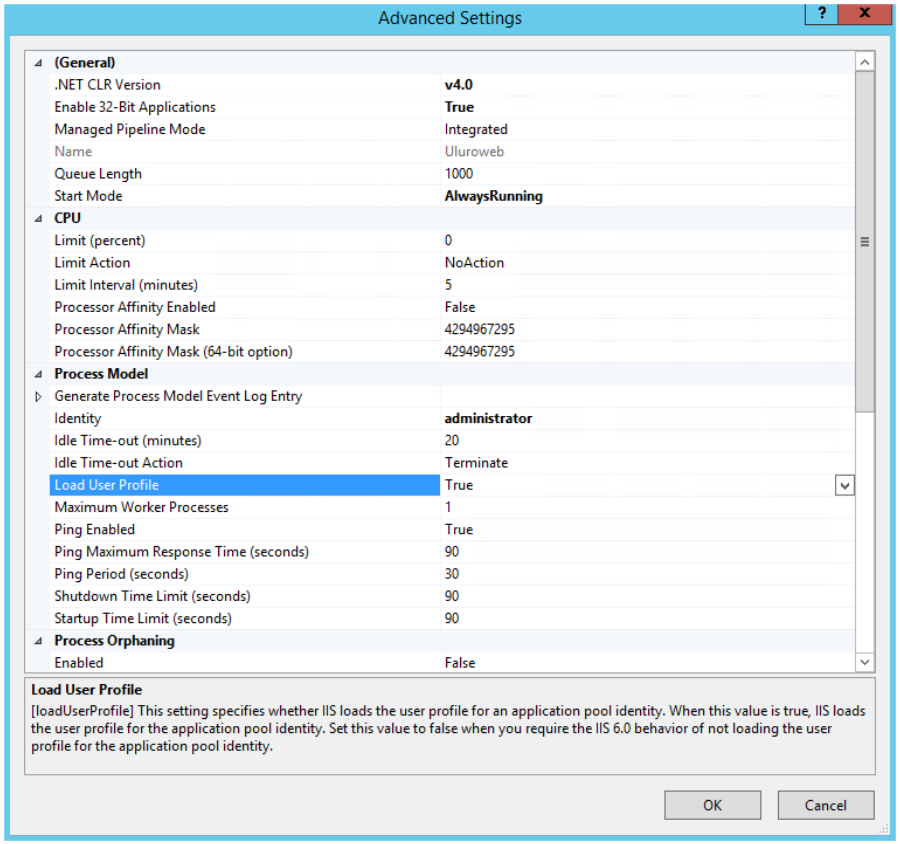


In each of the data and queue directories there should be a watch.dat file.

The log directory may be empty or contain log files.

For the Relay UnifyWeb programs to work the Application Pool must be set up to “Load User Profile”. In IIS locate the application Pool running the web.

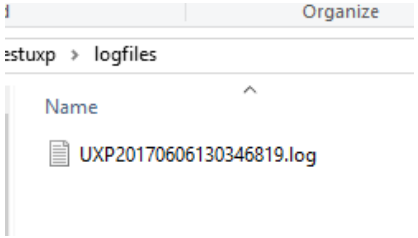
Select the Application pool and edit the advanced settings.
Change load user profile to true. This allows the system to see the UXPHOME variable. The Web Server may need to be rebooted.



Log Files

If the Relay UnifyUXP.dll is located in the program directory a logfiles directory should be created when attempting to access Relay Unify uSecure Functions.

When you attempt to use the Relay Unify uSecure function a logfiles directory will be created and a UXPxxxxx.log file will be created.

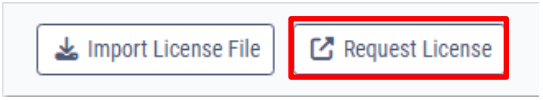


The .log file will contain information about what is happening.

The .log files are deleted if no error occurs when processing.

Activation

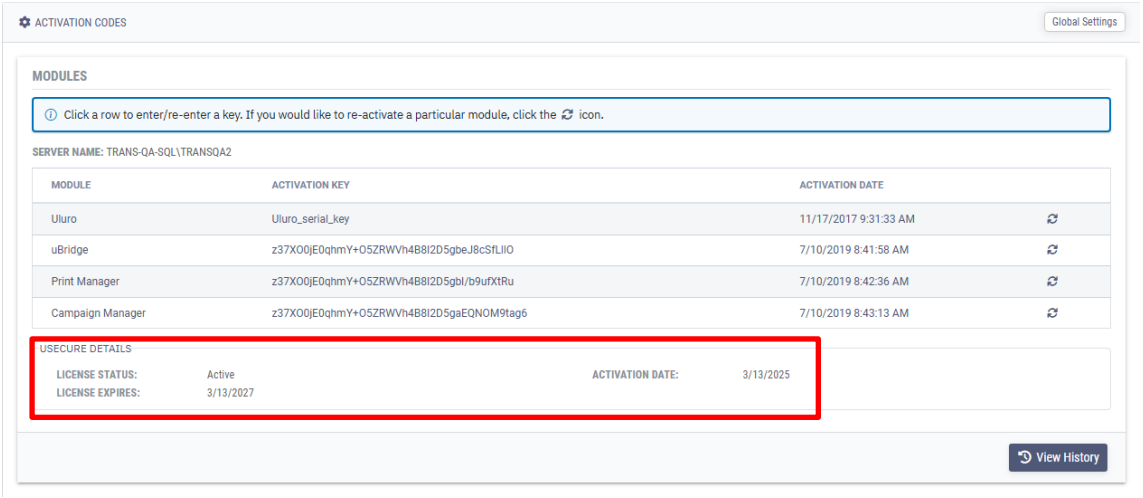
Before Relay Unify uSecure can be used the user must obtain a license from Pitney Bowes Support. One license will be needed per database, so most clients will need a license for their development as well as their production environments.

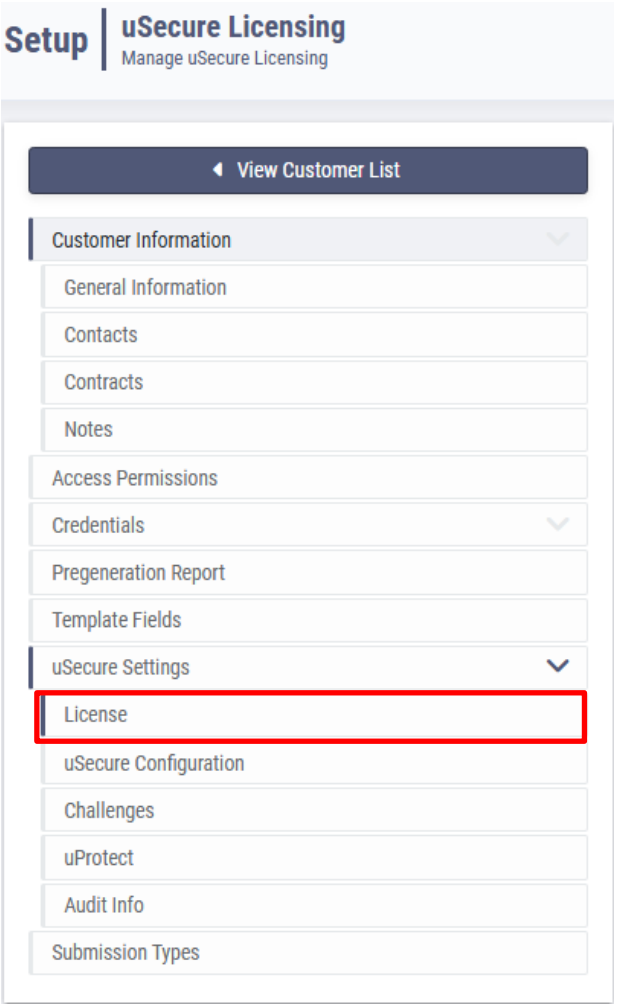


You will need to request the license in uSetup. From the dashboard, select Global Settings > Relay Unify uSecure > License.

Select Relay Unify. Click the “Request License“ button.

The License File will be generated for you after you accept the agreement.



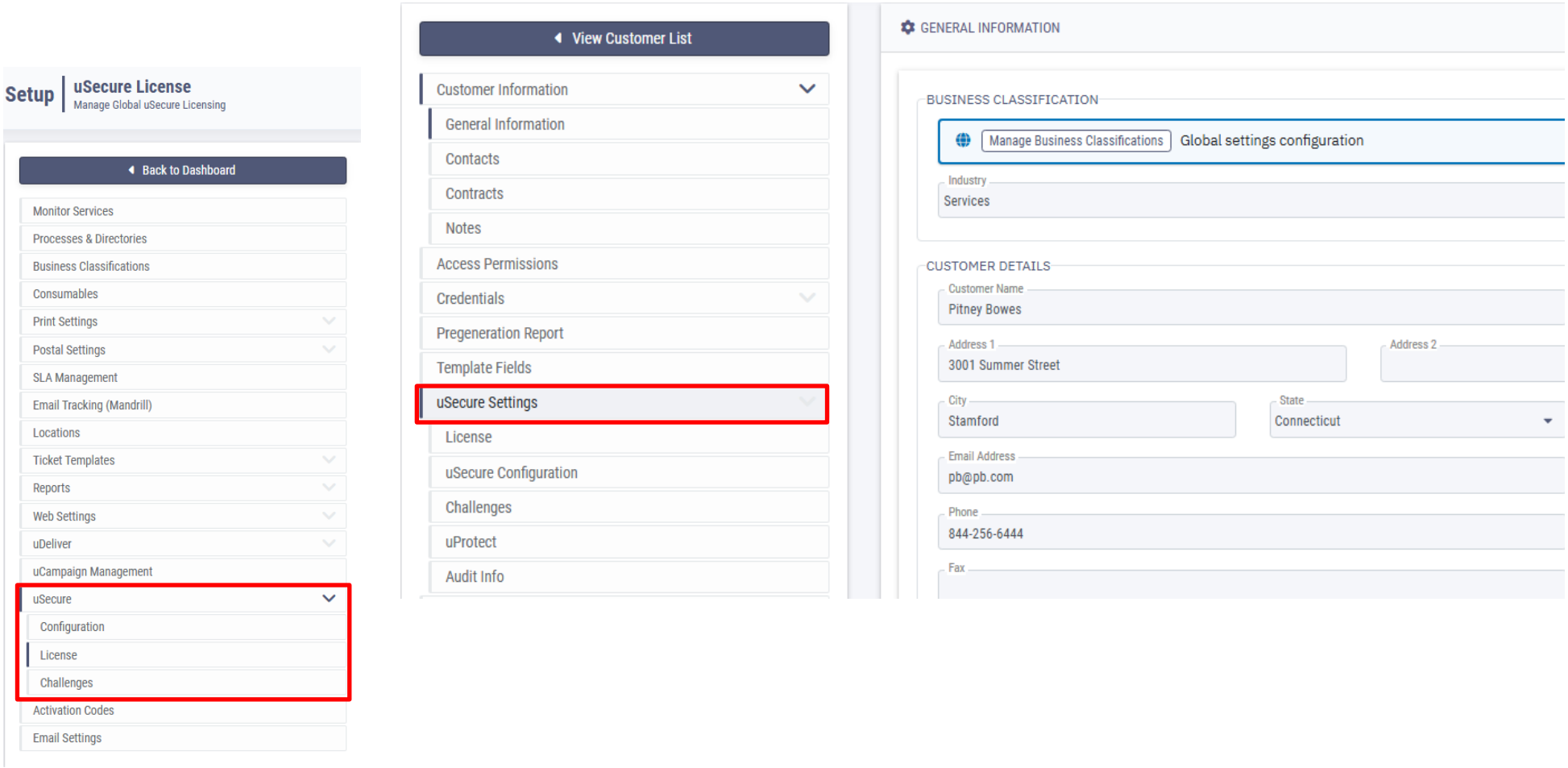


Once Relay Unify uSecure has been activated, the user will see the Relay Unify uSecure option in the Global Settings menu and the Manage Customer section as well.

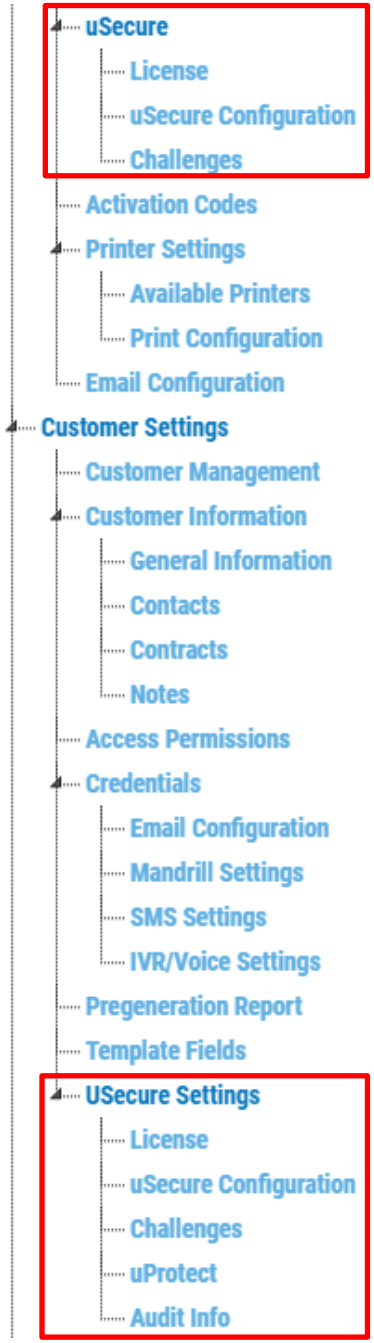
Global Settings

Permissions: User Maintenance

For the Relay Unify uSecure options to be available for the Relay Unify user, those settings must be checked in View Users. If not checked, the Configure menu items will be grayed out. Once Relay Unify uSecure is installed, all clients will have the Security Sentinel button available and can request a license for the selected customer.



Under the Users & Groups section in uSetup, select View Users. Select a user from the Relay Unify users already created. The middle tab, Feature Permissions, click **+ Add a Feature**. Then choose from the list what you would like to give the user permissions for.



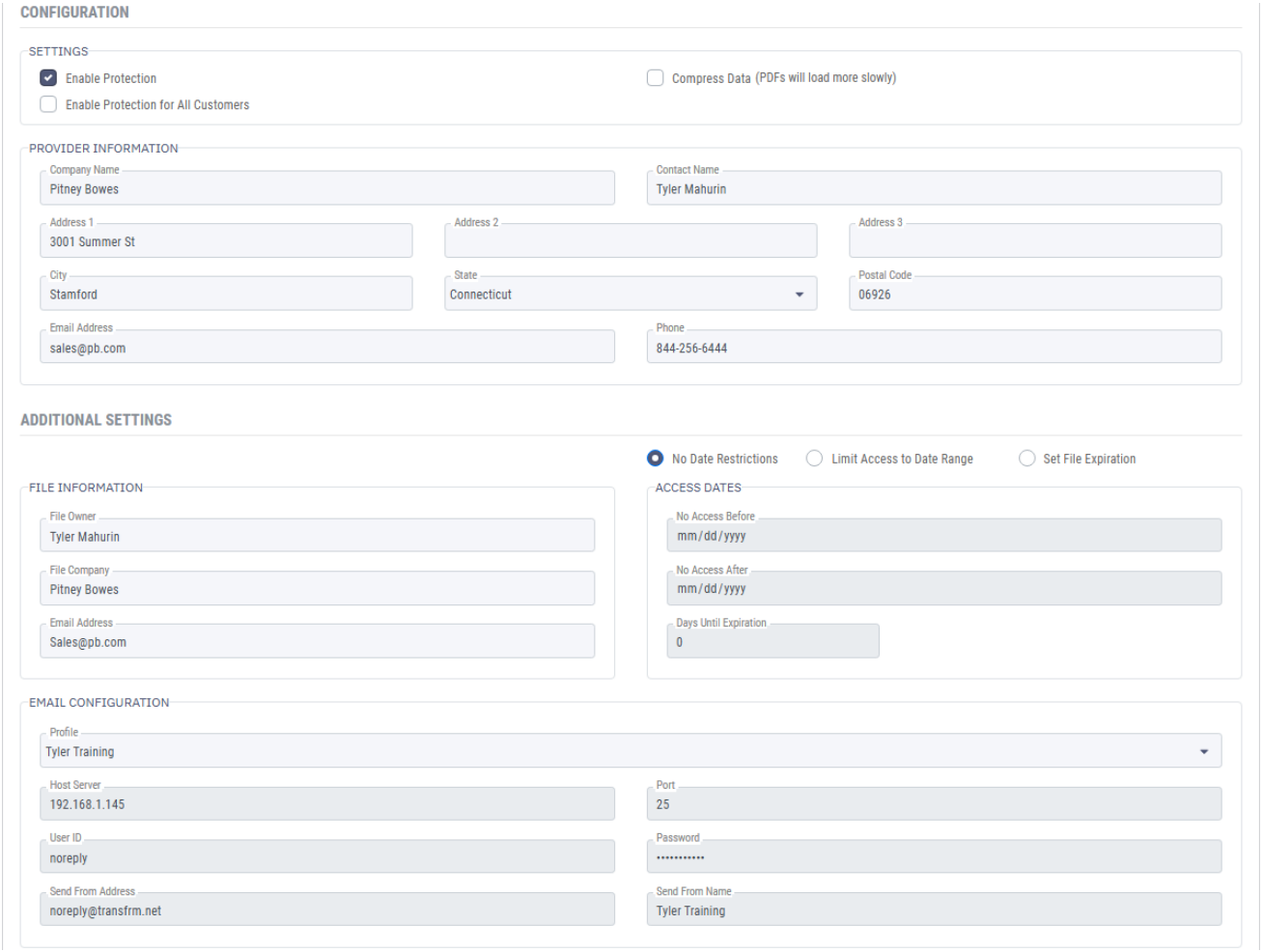
Global License

Requesting and Importing a Global License Manually

To request a global license, import the license, and enable global settings, select Global Security Sentinel from the configure menu in Relay Unify.

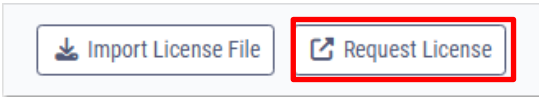
Enter the Provider Information. The email address(es) entered will be the email address(es) that will receive the license file.

Enter the email settings. The email account will be used to send out your customer license requests.



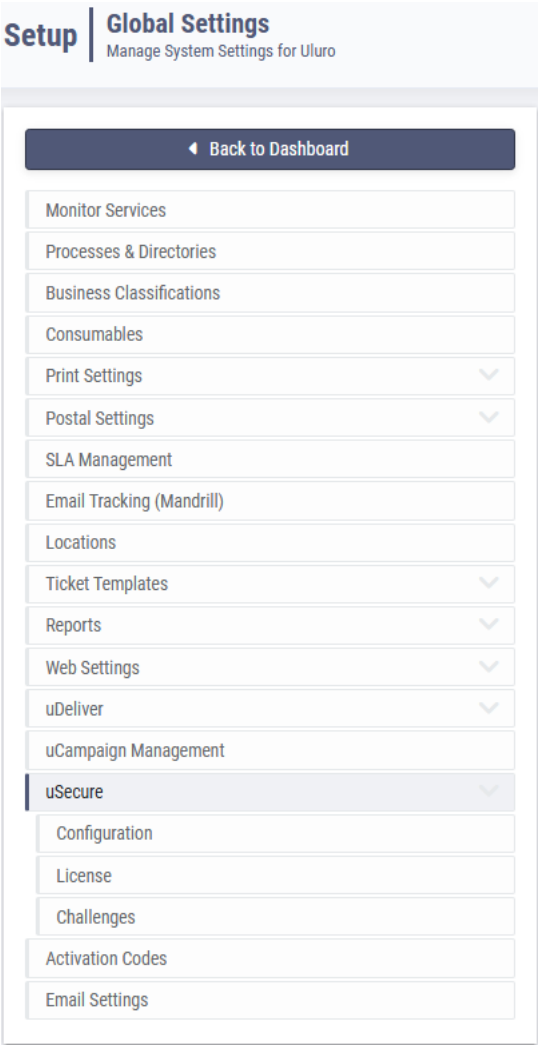
Save your information by clicking the Save button.

Click on the Request License button on the License tab.

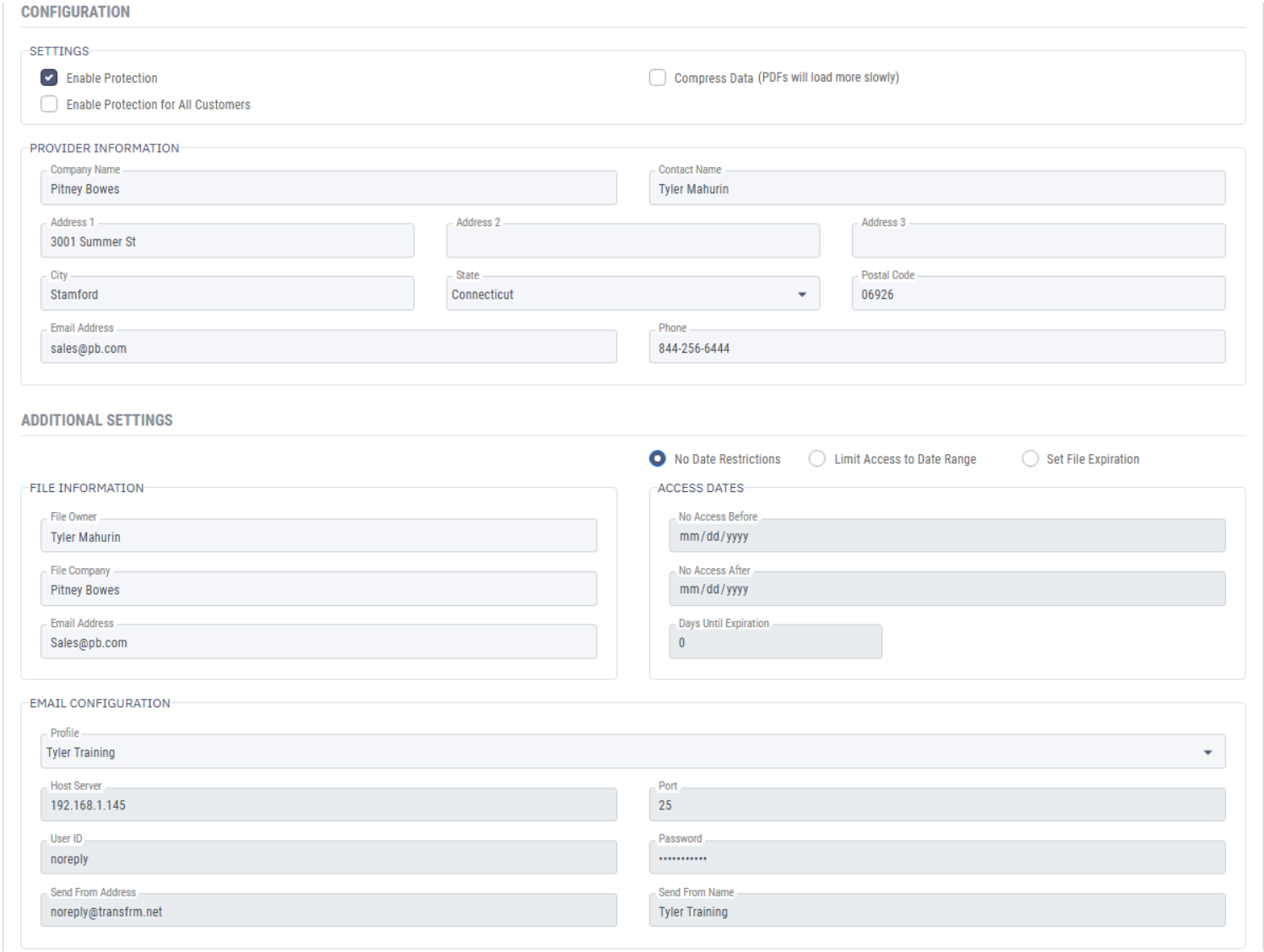


Upon receiving your license from Pitney Bowes, click on the Import License File button.

Once the license file has been imported and verified, you will then be able to turn on protection.



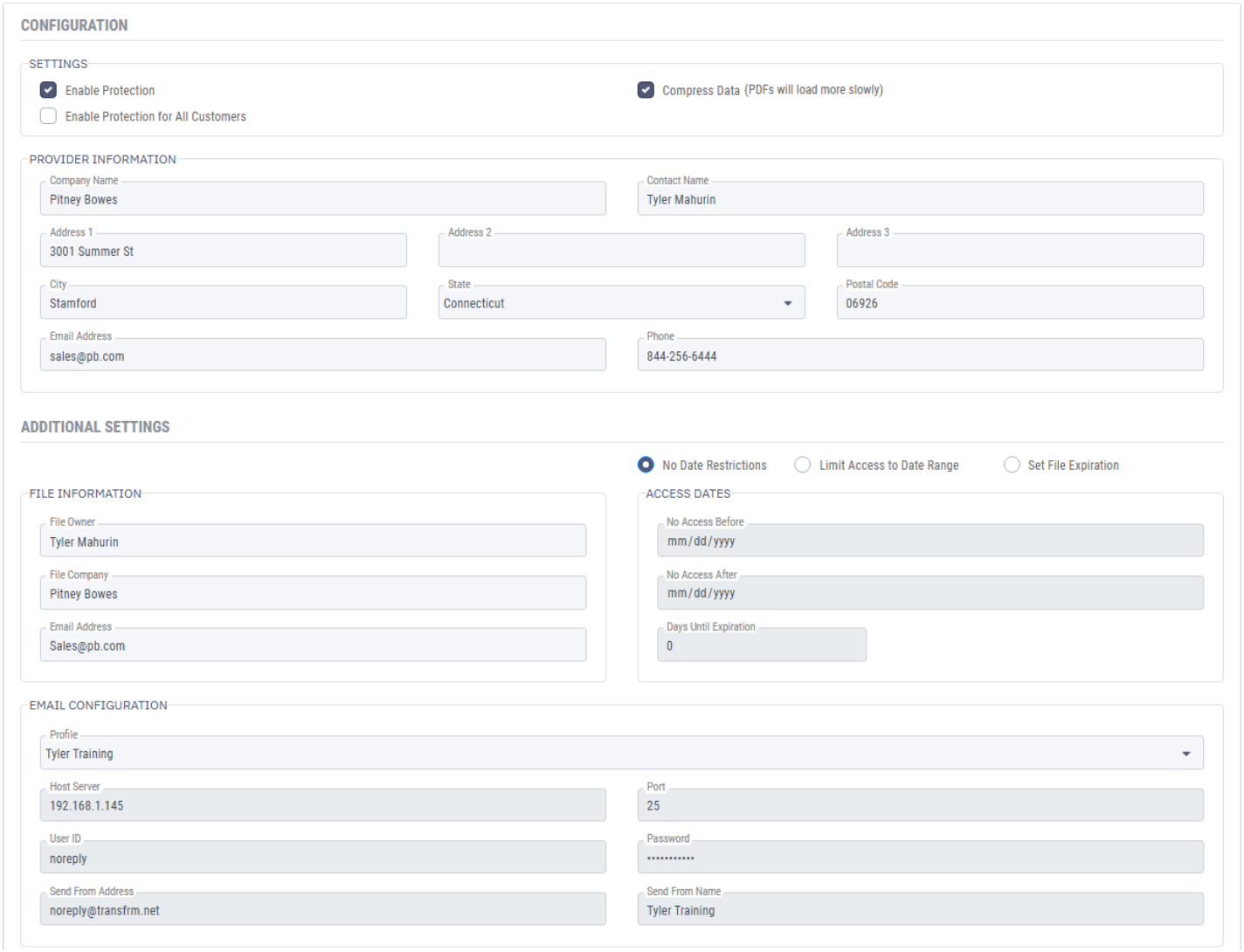
Once all the Provider information and Email Settings have been filled in, click on the **Save** button.



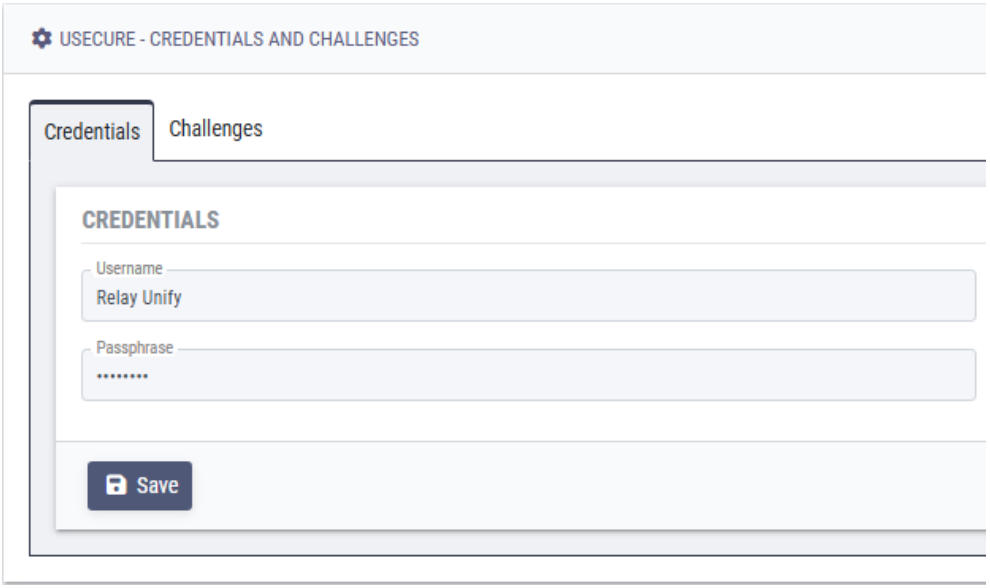
Global Level Protection Settings

Check the **Enable Protection** checkbox to enable Protection.

Check the **Compress Data** checkbox to enable compression.



Switch to the Challenges tab to set the **User Name** and **Passphrase** for Protected files. Challenges are Question/Answer criteria that are used to access the file. You can Add additional challenges by entering the **Challenge Name** and **Challenge Value**. Check the **Required** checkbox if the challenges are required. Click Save to add the Challenges. These Global Challenges are used with Customer level and Submission type level challenges to secure the protected files.



Customer Settings

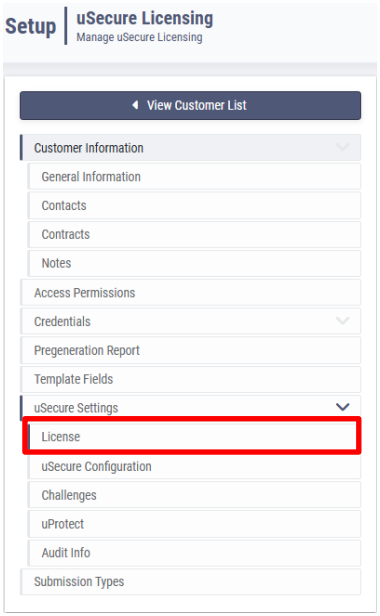
Customer License

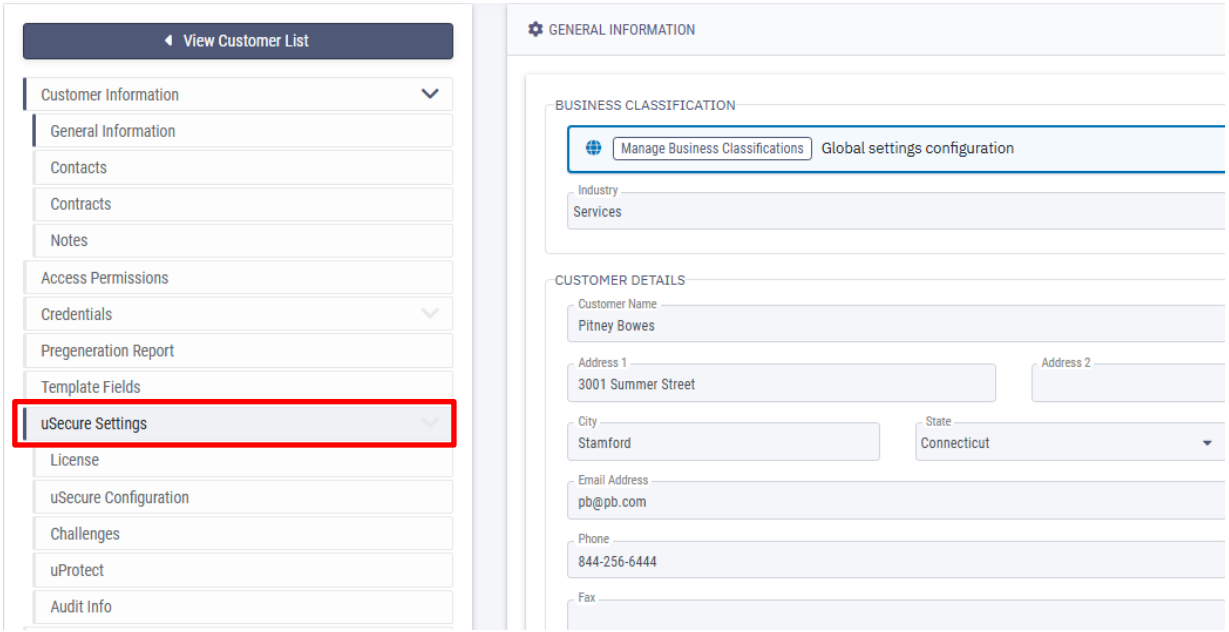
Requesting and Importing a Customer License Manually

Customers with Relay Unify uSecure already enabled will have a secure icon beside the CLID in uSetup.
Customers with enabled protection not yet enabled or turned off will have an unlocked icon.

To Edit or Enable Relay Unify uSecure on a Customer, select the Customer and click the Relay Unify Tab.

Select the License tab to request a customer level license and configure the customer security settings.

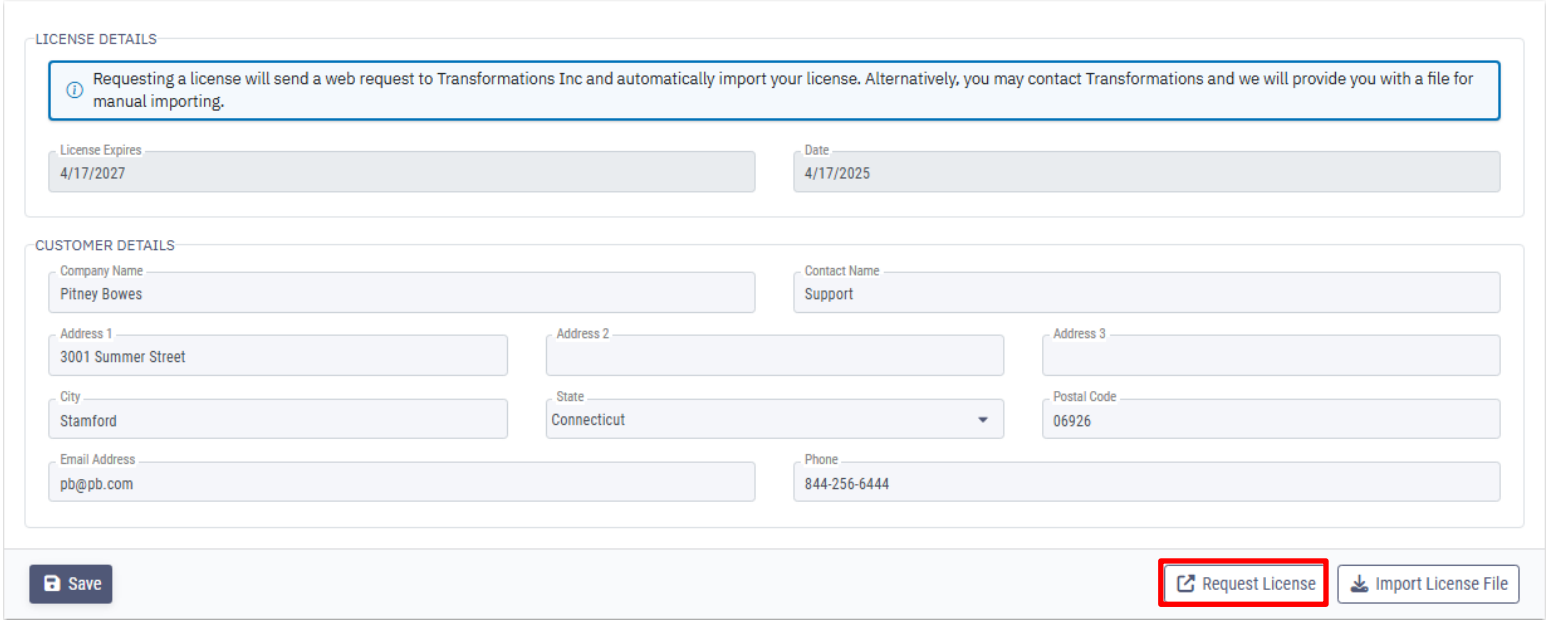




Customer level Relay Unify License tab displays the Details screen for Individual Customer Security. When enabling protection on a Customer you will need to request a license.

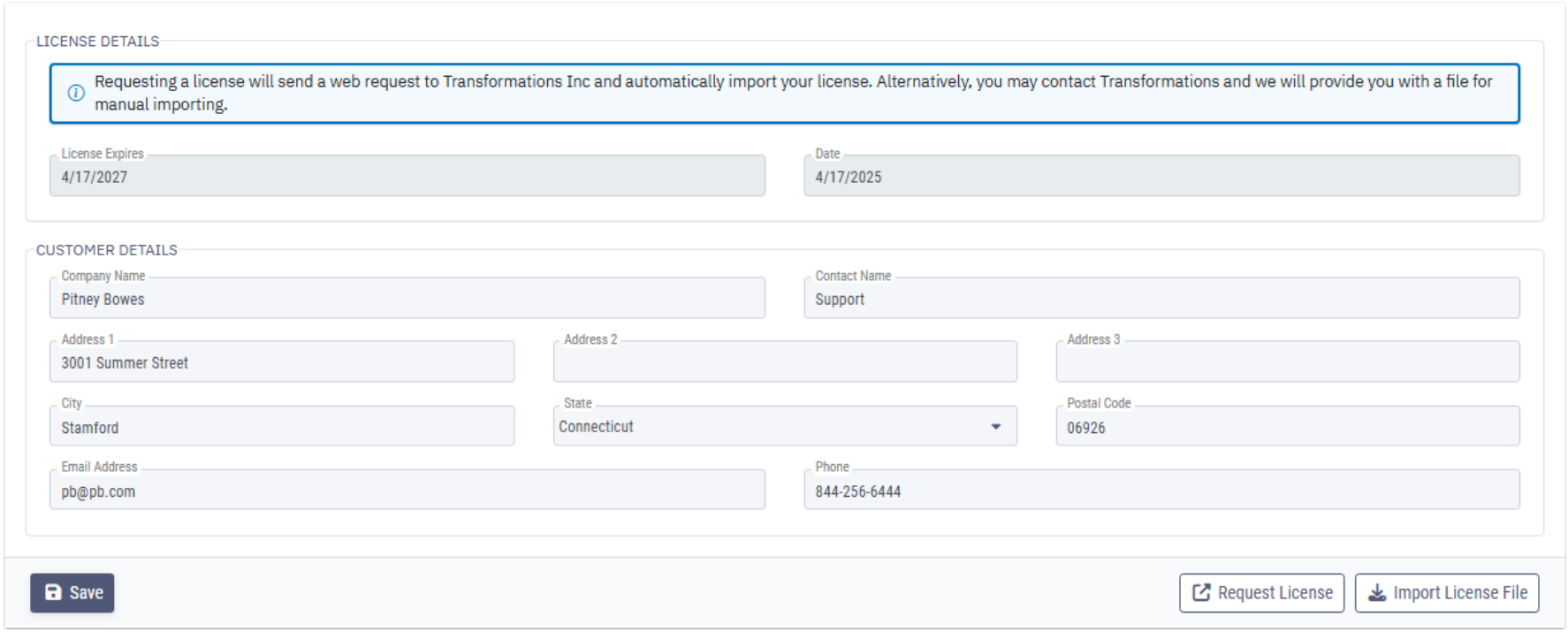
To request a customer license, Enter the Company's information.

Click on Request License.



Automating the Request and Import of a Customer License

Once all the client information below is filled out, click **Request License**.



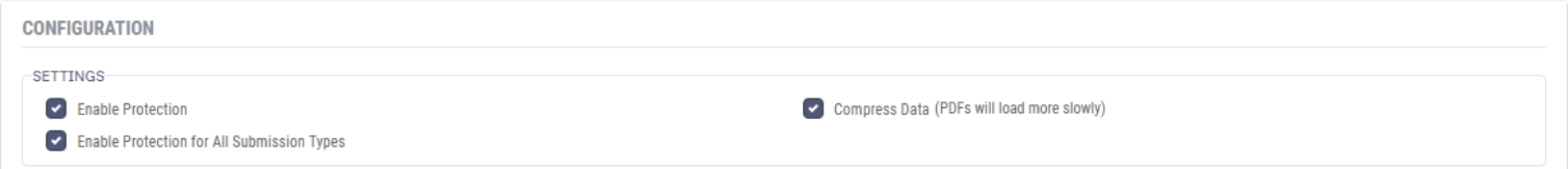
Customer Level Protection Settings

Within the Customer Relay Unify tab, go to the Configuration tab to enable protection for this customer.

Check the **Enable Protection** checkbox to enable Protection.

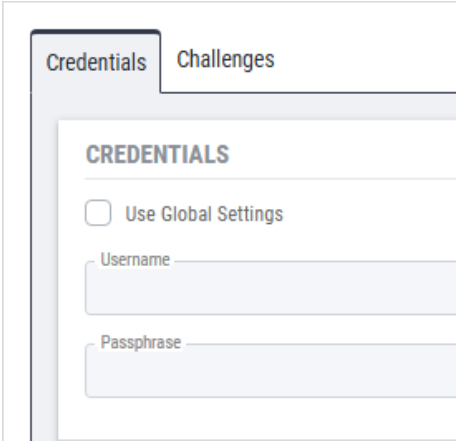
Check the **Compress Data** checkbox to enable compression.

Check the **Enable Protection for All Submission Types** checkbox to enable protection on all submission types for the Customer including future submission types.



Challenges

Switch to Challenges tab to set the challenges.



Use Global Settings – If checked the Username and PassPhrase from the Global settings will be used.

Additional Challenges can be added for the Customer by setting the **Username** and **Passphrase** for Protected files. Challenges are Question/Answer criteria that are used to access the file. You can Add additional challenges by entering the **Challenge Name** and **Challenge Value**. Check the **Required** checkbox if the challenges are required. Click Save to add the Challenges. These Global Challenges are used with Customer level and Submission type level challenges to secure the protected files.

Under the Configuration tab, you'll see Additional Settings for more security settings.

Notifications

If **Allow Emails** is checked the Email Settings section will be visible. Enter the email credentials for sending emails for this customer. Send a Test Email to verify the credentials.

Notify on Failed Access – This will send an email if access to the protected file fails.

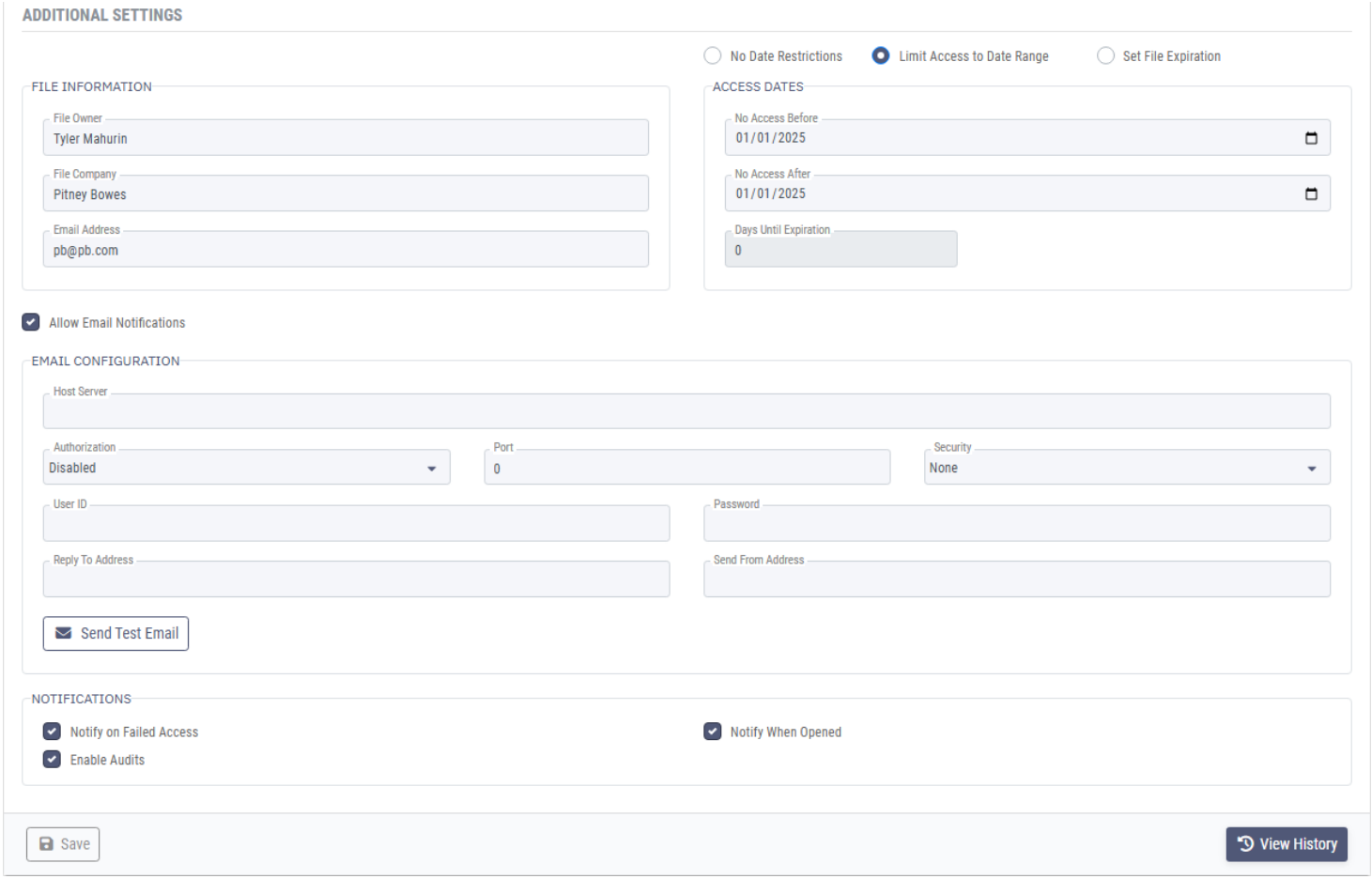
Notify when opened – This will send an email every time the protected file is accessed. Be careful enabling this option. Relay Unify will access the protected file multiple times during processing and printing. Each access will send an email.

Enable Audits – This will enable audits on file access. The Audit will be sent to Relay Unify if the file is accessed by Relay Unify.

Checking the Allow Emails checkbox will enable the Email Settings area. This area must be populated for emails to be generated. The Protected file will perform the emailing operations.

Reply to – This is the reply to email address.

Server – This is the Name or IP address of the Email server that will send the email. Contact your IT Department for this information.



Port – This is the port for sending Emails. Default is port 25. Contact your IT Department for this information.

Security – This is the type of security used by your Email server. The possible values are None, SSL, or TLS. Contact your IT Department for this Information.

Authorization – This allows enabling Authentication.

Sender – This is the Email Sender name. This is required if Email Auth is enabled.

User ID – This is the Email Sender User id. This is required if Email Auth is enabled.

Password – This is the Email Password. This is required if Email Auth is enabled.

Click the **Send Test Email** button to test the email settings. An email will be sent to the Email Address specified in the **Test Email Send To** field.

Access Dates

The dates the data can be accessed can also be limited.

If **Limit Access To Date Range** is checked, then calendars are displayed to set the access dates. Click on the preferred dates for No Access Before and After.

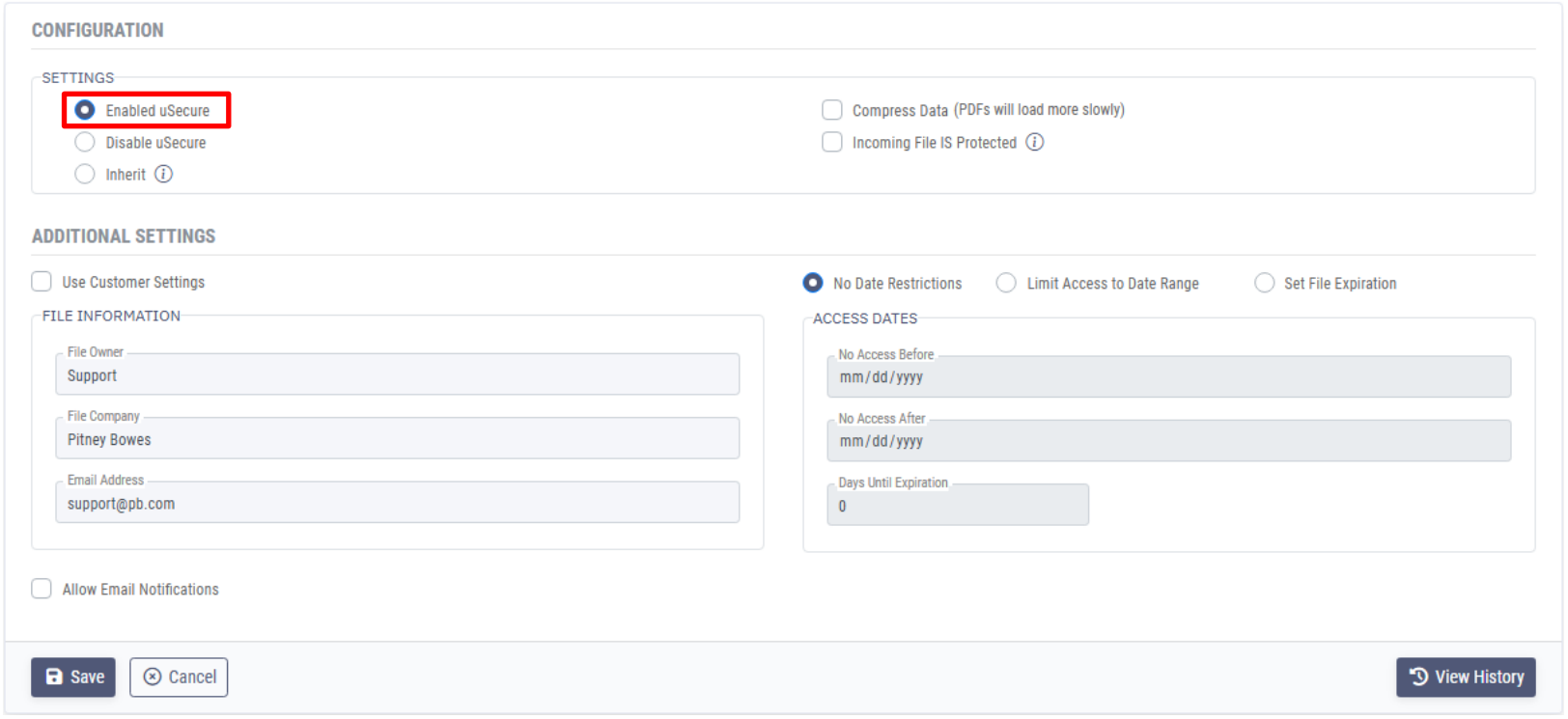
Checking the **Check To set Days to Expire** will enable the setting of the number of days to expire. This will set the expiration date of a Submission to the specified number of days after the submission is created. The default number of days is zero and must be changed to a positive number of days.

Click the Save button to save the changes. Click Cancel to close without saving.

Submission Level Protection Settings

Submission Types with Relay Unify uSecure already enabled will have a secure icon beside the Sub ID in uSetup. Submission Types with enable protection not yet enabled or turned off will have an unlocked icon.

To Edit or Enable Relay Unify uSecure on a Submission Type, click on the submission type. Go to the Relay Unify uSecure tab and click on the Configuration tab.



This displays the Relay Unify uSecure Configuration for the Submission Type.

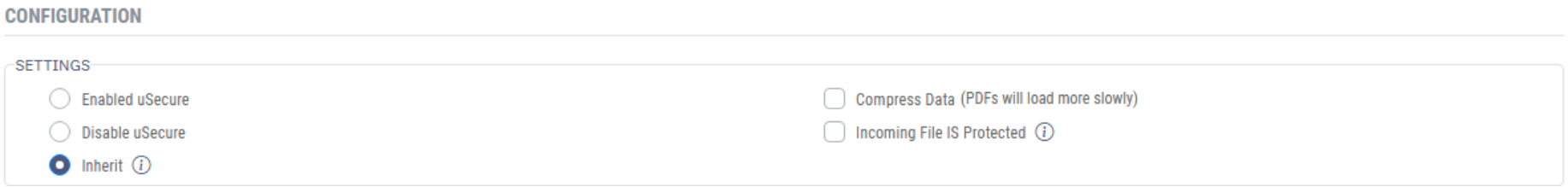
Enabled – Select to enable protection for this submission type.

Disabled – Select to disable protection for this submission type.

Inherit – Select to use the Enable setting from the Customer. If the customer is set to use the global setting, the global settings will be used. If the customer is set to use the customer level settings, the customer settings will be used.

Compress Data – Compress the data when stored in a protected file.

Incoming File is NOT Protected – Check this if the data is not being provided in Protected Files using Relay Unify uProtect. If unchecked, then the data is expected to arrive in Relay Unify uSecure protected files created by Relay Unify uProtect using the Permissions file sent to the Customer. If the data is not protected and this is unchecked the submission type will error.

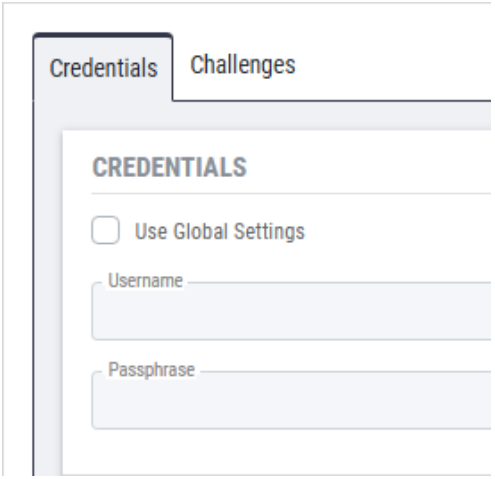


Challenges

Click on the Challenges tab to set the challenges.

Use Customer Settings – If checked the Username and Passphrase from the customer settings will be used.

Additional Challenges can be added for the Customer by setting the **Username** and **Passphrase** for Protected files. Challenges are Question/Answer criteria that are used to access the file. You can Add additional challenges by entering the **Challenge Name** and **Challenge Value**. Check the **Required** checkbox if the challenges are required. Click Add to add the Challenges. These Global Challenges are used with Customer level and Submission type level challenges to secure the protected files.



Switch back to the Configuration tab for more security settings.

Notifications

If **Allow Emails** is checked the Email Settings section will be visible. This area must be populated for emails to be generated. The Protected file will perform the emailing operations.

Reply to – This is the reply to email address.

Host Server – This is the Name or IP address of the Email server that will send the email. Contact your IT Department for this information.

Port – This is the port for sending Emails. Default is port 25. Contact your IT Department for this information.

Security – This is the type of security used by your Email server. The possible values are None, SSL, or TLS. Contact your IT Department for this Information.

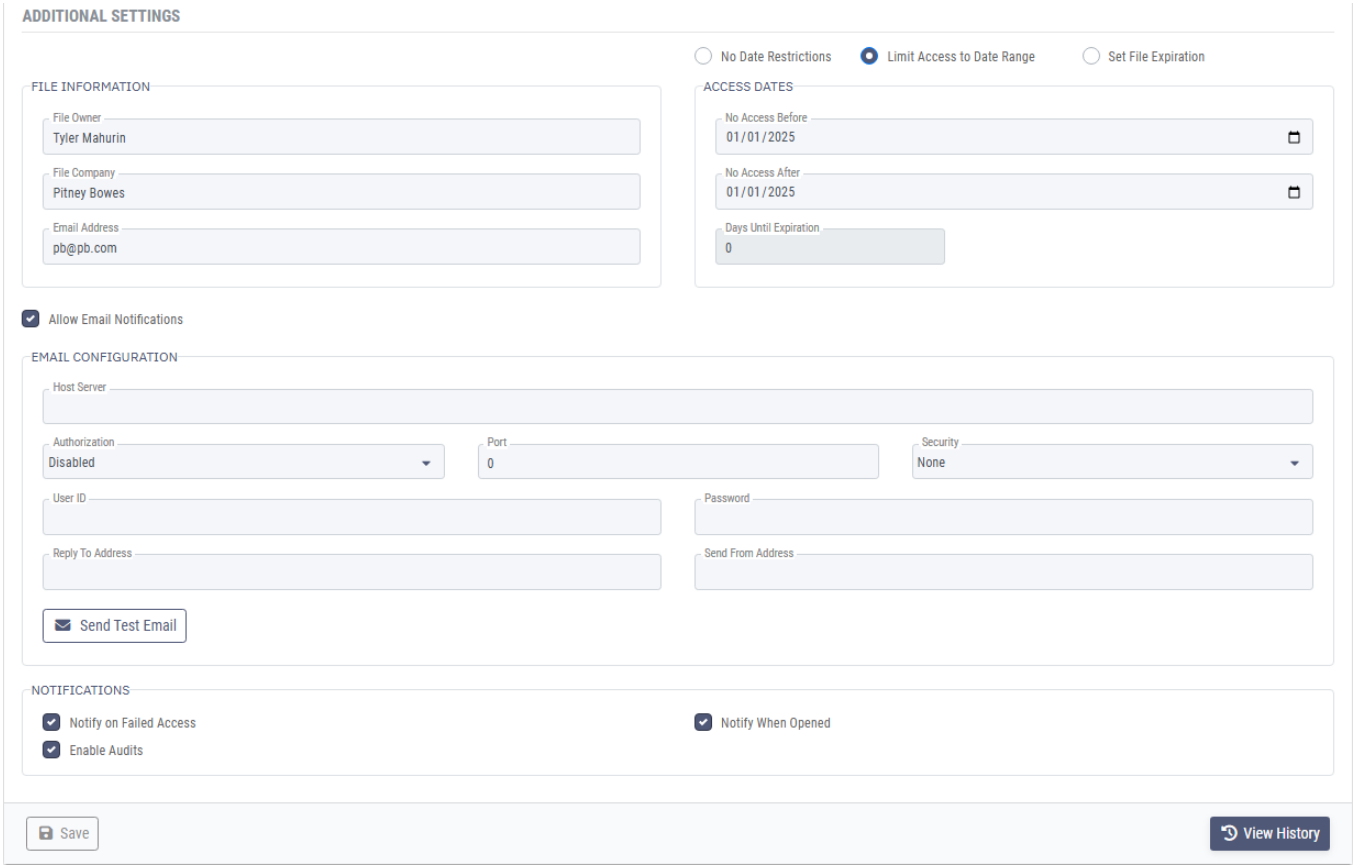
Authorization – This allows enabling Authentication.

Send From Address – This is the Email Sender name. This is required if Email Auth is enabled.

User ID – This is the Email Sender User id. This is required if Email Auth is enabled.

Password – This is the Email Password. This is required if Email Auth is enabled.

Click the **Send Test Email** button to test the email settings. An email will be sent to the Email Address specified in the **Test Email Send To** field.



Notify on Failed Access – This will send an email if access to the protected file fails.

Notify When Opened – This will send an email every time the protected file is accessed. Be careful enabling this option. Relay Unify will access the protected file multiple times during processing and printing. Each access will send an email.

Enable Audits – This will enable audits on file access. The Audit will be sent to Relay Unify if the file is accessed by Relay Unify.

Access Dates

The dates the data can be accessed can also be limited.

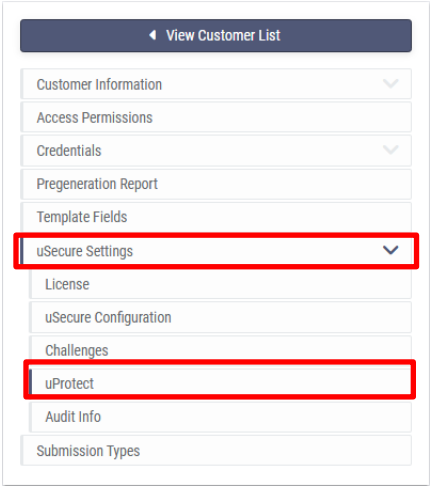
If **Limit Access To Date Range** is checked, then calendars are displayed to set the access dates. Click on the preferred dates for No Access Before and After. The file will not be accessible outside of the set date range. If the file is not accessible, processing, printing, web display of the documents, etc., will error.

Checking the **Check To set Days to Expire** will enable the setting of the number of days to expire. This will set the expiration date of the data file to the specified number of days after the submission is created. The default number of days is zero and must be changed to a positive number of days. This should be the same value as the submission type expiration settings to avoid errors.

Click the Save button to save the changes. Click Cancel to close without saving.

Relay Unify uProtect

Customer Level Relay Unify uProtect Permissions



Within the Relay Unify uSecure tab for the customer, select Customer Relay Unify uProtect tab to set the Permission that will be granted to the Customer for Relay Unify uProtect.exe.

This will display the Relay Unify uProtect Customer Permissions Configuration screen.

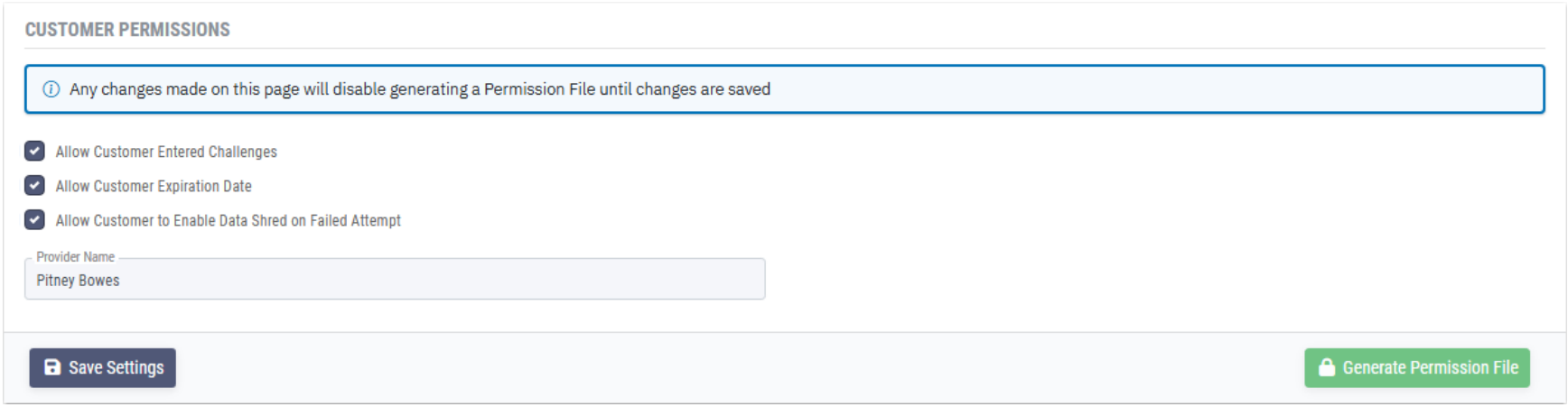
Allow Customer Entered Challenges – Checking this will allow the Customer to set additional Challenges for Access.

Allow Customer Expiration Date – Checking will allow the Customer to set Expiration date on protected files.

Allow Customer to Enable Data Shred on Failed Attempts – Checking will allow the Customer to enable data Shred and the number of failed attempts before the data is shreded.

Provider Name – Allow setting the PSP name displayed in Relay Unify uProtect.

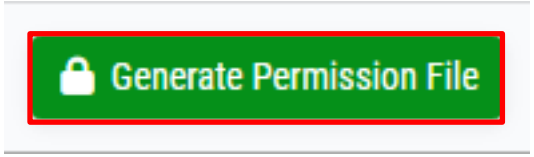
Enter the desired selections and click the save button.



Generating a Customer Permission File

Generate Permission File will generate a Permission File (.kke file) for use by the Customer.

Permission files are sent to the Customer for use with Relay Unify uProtect.exe. It enables Functions in Relay Unify uProtect for the Customer. When the Button is clicked the User will be asked for the Location and name for the Permission File.



Relay Unify uProtect.exe

This program is used to protect files that will be sent to your print service provider.

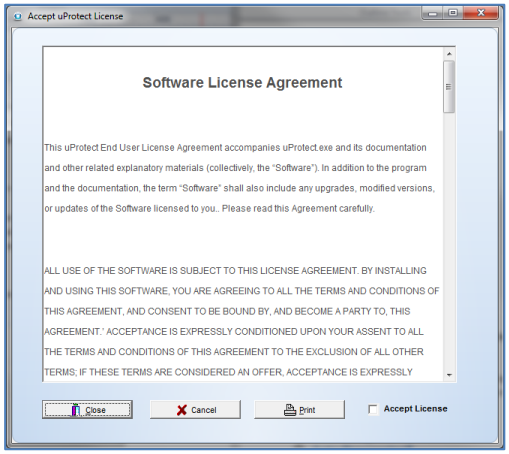
Double-click on Relay Unify uProtect.exe or the desktop shortcut for Relay Unify uProtect.exe. This will start the Program. The Relay Unify uProtect Splash screen will be displayed for 3 seconds. Clicking anywhere on the Splash screen will close it.

The first time you run the Relay Unify uProtect program (and when the Relay Unify uProtect License changes) the Accept Relay Unify uProtect License screen will be displayed.

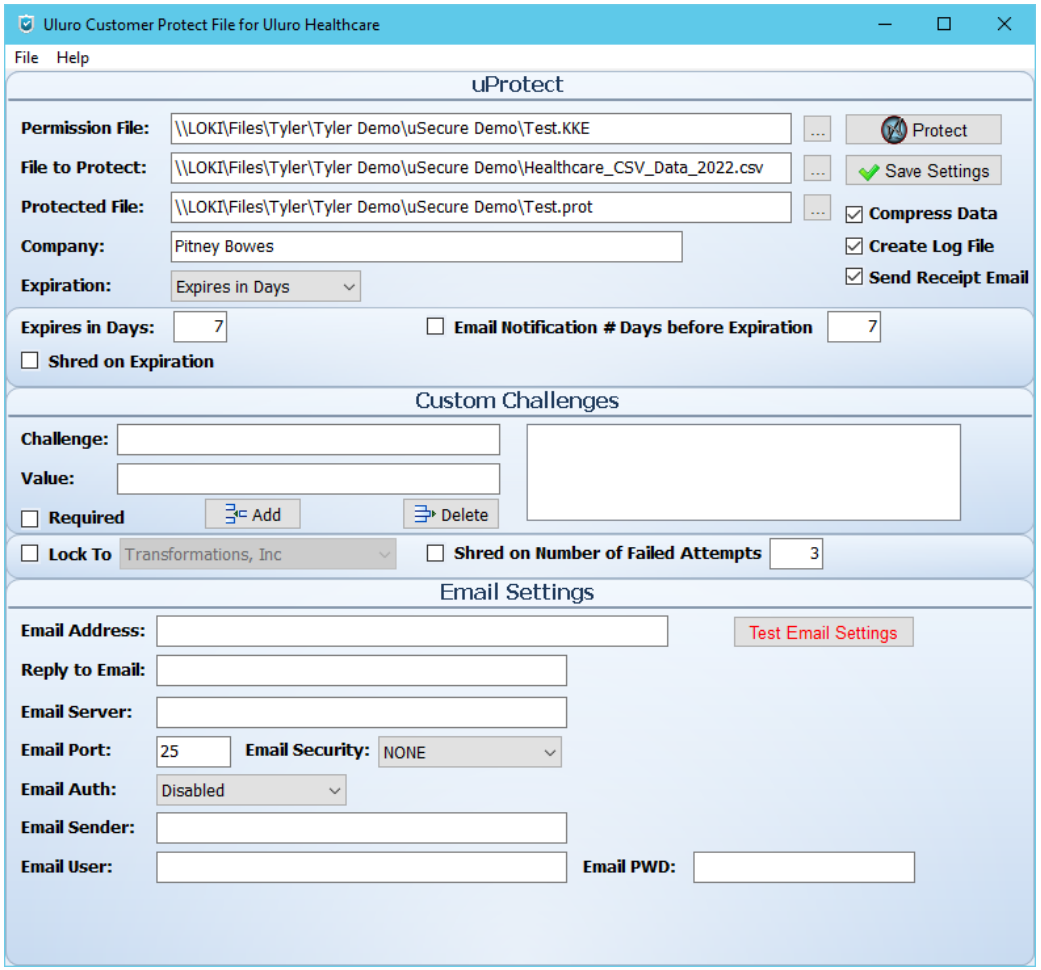
The License must be accepted, or the program will terminate. To Accept the License, click the Accept License checkbox and click close. Clicking Cancel or clicking on the X in the upper corner will cause the program to terminate.

The License may be printed by clicking the Print button and selecting the printer.

The license can be accessed at any time from the Help menu.



When Relay Unify uProtect starts the Relay Unify uProtect main form is displayed.



Permission File – This is the file provided by the Print Service Provider. This contains configuration information from the Print Service Provider that enables additional functions. To load a permission file, enter the path and name of the Permission file in the Permission File entry field. You can also browse for the file by clicking the Ellipsis next to the Permission File entry field. If the file is manually entered, then tab to the next entry field. This will load the Permission file.

File to Protect – This is the file that will be protected. This cannot be the Permission file. This is the data file before protection.

Protected File – This is the file that will be created during Protection. This cannot be the Permission file or the File to Protect. This is the data file after protection that will be sent to the PSP to generate documents.

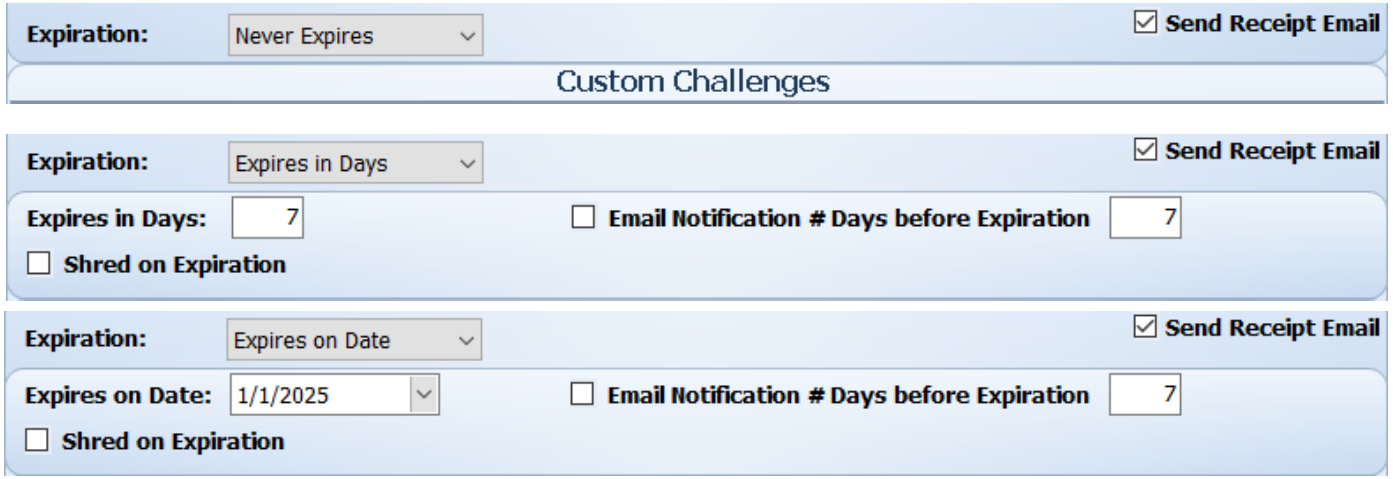
Company – Enter the Company Name.

Expiration – Select the time for the data file before expiration.

Never Expire – The Protected file never expires.

Expire in Days – The Protected file will expire in a set number of days after creation. Enter the number of days for the **Expires in Days** field.

Expires on Date – The Protected file will expire on a specific date. Select the date to expire in the **Expires on Date** field.



If an email notification is desired before Expiration, then check the **Email Notification # of Days before Expiration** and enter the number of Days.

If **Shred on Expiration** is checked the File will shred itself if accessed after the expiration date.

Checking the Email Notification # of Days before Expiration checkbox or the Send Receipt Email checkbox will enable the Email Settings area. This area must be populated for emails to be generated. The Protected file will perform the emailing operations.

Send Receipt Email – Check this to receive an email when the Print Service Provider receives and accesses the Protected file. This email will be sent only the first time the Protected file is accessed.

Email Address – This is the email address to which the emails will be sent.

Reply to Email – This is the reply to email address.

Email Server – This is the Name or IP address of the Email server that will send the email. Contact your IT Department for this information.

Email Port – This is the port for sending Emails. Default is port 25. Contact your IT Department for this information.

Email Security – This is type of security used by your Email server. The possible values are None, SSL, or TLS. Contact your IT Department for this Information.

Email Auth – This allows enabling Authentication.

Email Sender – This is the Email Sender User id. This is required if Email Auth is enabled.

Email PWD – This is the Email Password. This is required if Email Auth is enabled.

Click the **Test Email Settings** button to test the email settings. An email will be sent to the Email Address specified using the email settings. If the settings work the Test Email Settings button font color will be black instead of red.

When enabled, a Custom Challenges entry area will be displayed. This allows you to enter Challenges that are required before the protected file can be accessed. When the Protected file is accessed, the system requesting access will be presented with Challenges. The accessing system must respond by entering the corresponding value. These Challenges will not be visible to the Print Service Provider.

Enter the **Challenge** and the **Value**. Check the **Required** checkbox if the Challenge is required. Click the **Add** button to add the challenge to the list.

To Delete a Challenge, select the Challenge in the List and click the **Delete** button.

If enabled, the **Lock To** checkbox will be visible. Check to enable locking of the Protected file to the Selected Location.

If enabled the **Shred on Number of Failed Attempts** checkbox is visible. Check and enter the Number of Failed attempts. If the designated number of Failed Attempts occurs, the protected file will be shredded. The failed attempts counter increments on each failed access attempt and is reset to 0 when a successful access occurs.

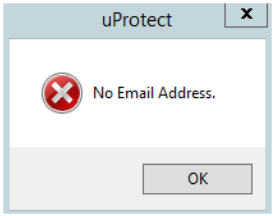
Compress Data – Check this to compress the data during protection. This will reduce the size of the Protected data file.

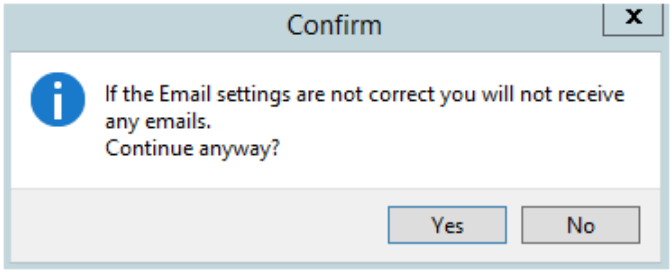
Create Log File – Check this to create a log file during protection. The Log file will be created during the Protection process. The file will be created in the Logfiles directory below the directory where the Program is located. The logfile name will be CPFYYYYMMDDHHMM.log

Instead of entering all the information every time the program is run Relay Unify uProtect can remember the settings and retrieve them automatically. To Save the current set of information click the **Save Settings** button. This will save Permission File, Email Settings. Lock Settings, Challenges, and Expiration settings. The settings are saved in the Directory with the program in the file CustPro.ini. When the Program is started the Saved settings will be retrieved.

To Protect a File, click the **Protect** button. The Entered information will be validated and then the File will be protected.

If Email settings are entered and not tested the following message will be displayed. If no credentials have been entered, you will receive an error message.

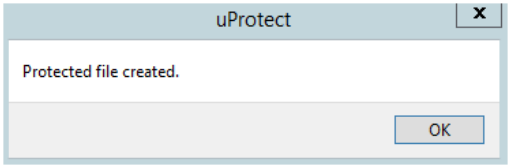




Click yes to continue.

A Progress window will be displayed.

When completed the following message will be displayed.



The Protected file can now be transmitted to the Print Service Provider.

Auto Processing

The Relay Unify uProtect program can be run in Automatic mode. This allows processing files by automated systems. To run in Automatic mode, you will need to run the program manually on the computer where the Automatic processing will occur. Select the Permissions file, set the desired values for the options. Then click the Save Settings button. This sets the default information for the system.

The Relay Unify uProtect program can be run automatically by-passing Command Line Arguments to the Relay Unify uProtect program. The Arguments can be Uppercase or Lowercase but must begin with -. The Command Line Arguments are:

-L This enables logging.

-P”Permission File path and Name” This sets the Permission File. Replace the text with the actual Permission file name and path. Surround the name with “.

-R”File to Protect path and Name” This sets the File to protect. Replace the text with the actual file to protect. Surround the name with :.

-N”Protected File path and Name” This sets the name of the protected file. Replace the text with the actual protected file name. Surround the name with “.

-XY - This will enable Compression. UseXY to enable and XN to disable compression.

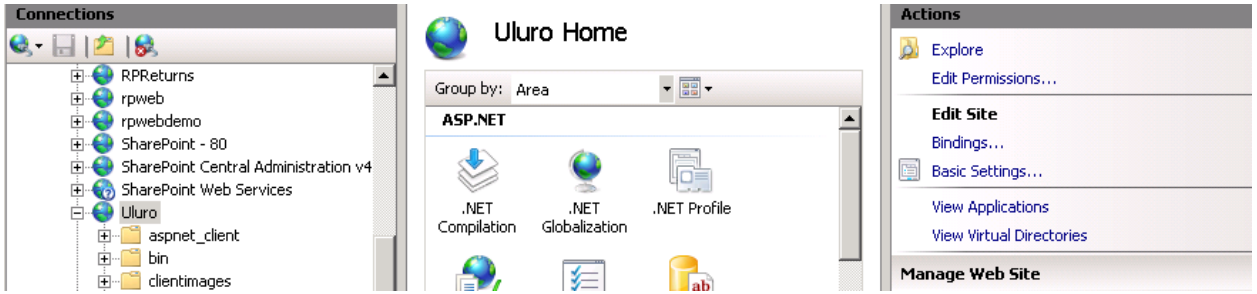
-A This enables automatic processing. Without this the other Arguments will only set the appropriate entry fields.

A Batch command file can be created with the above. The batch file would contain the line.

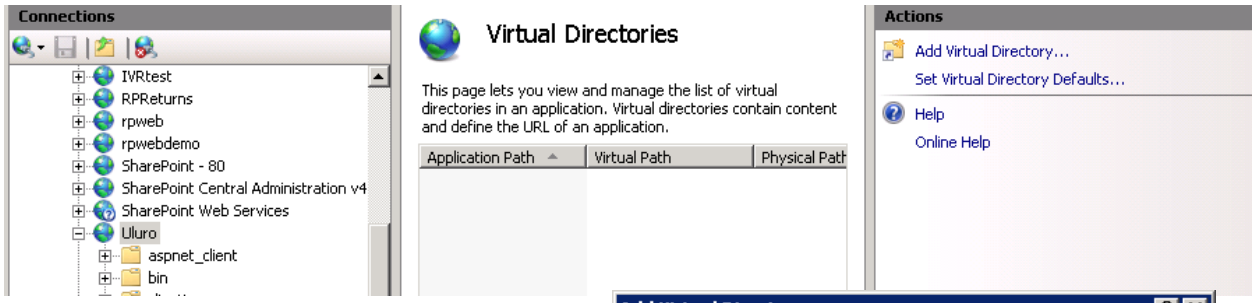
Relay Unify uProtect.exe -L -P"C:\Users\Desktop\test.kke" -R"C:\Users\Desktop\PaymentServerAdminManual.pdf" -N"c:\test.prot" -C"TransCust" -A -XY

Setup a Download Directory

In IIS select the Web Site.



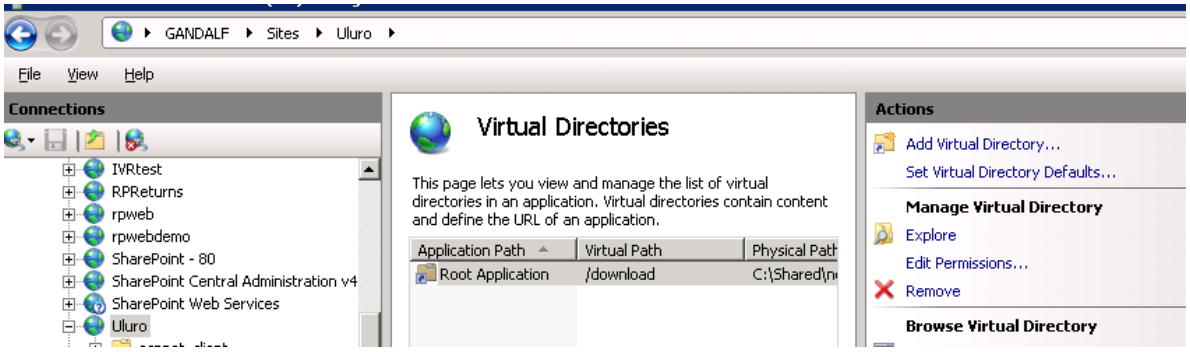
Then Select the View Virtual Directories under actions.

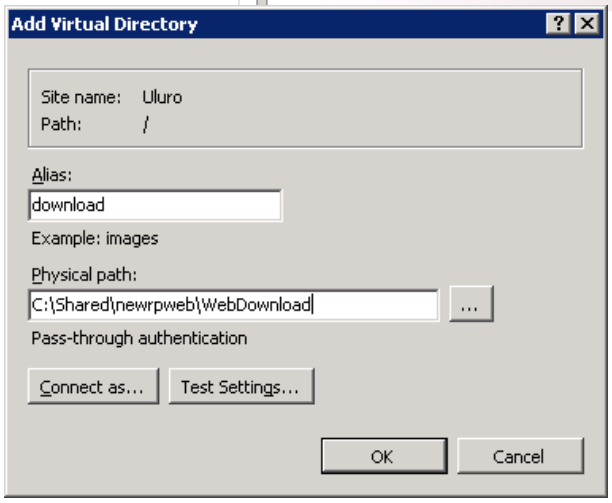


Then select Add Virtual Directory under Actions.

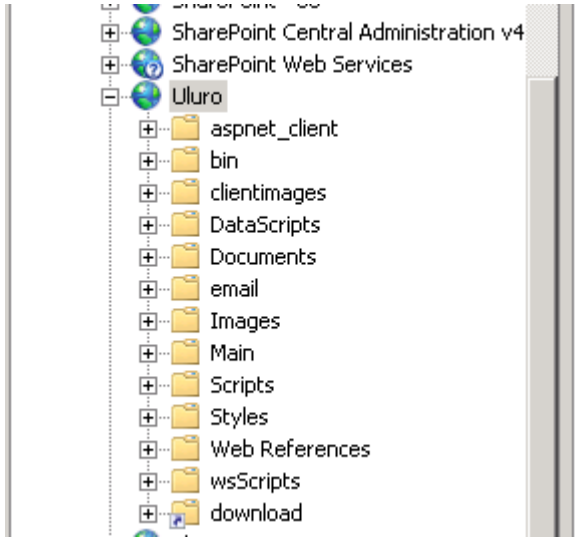
Add a Download Directory. Set the Physical Path to any path on the System.

Click OK.



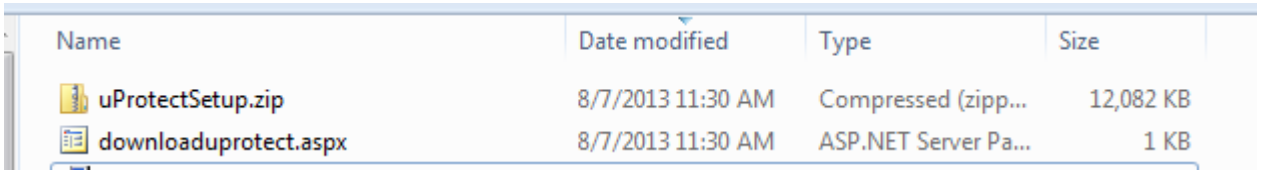


The download directory must be at the Root level (not under any other directory in the Web).



Now you can add the Program to the Download Directory.

The Customer Permission file should be emailed to the Client instead of a download. You may place the Permission file in the Download directory, but anyone could download.



You must create an aspx file for the download. Name the file downloadRelay Unify uProtect.aspx. In the file place :

Download Relay Unify uProtectSetup.zip

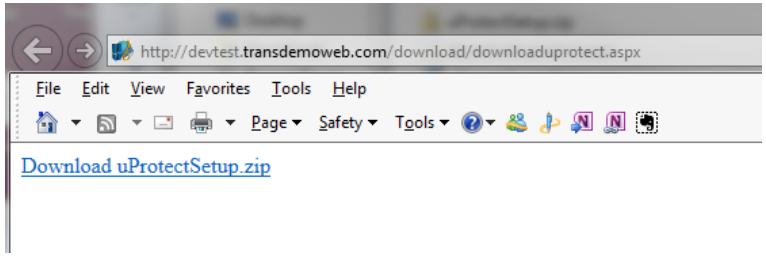
Use the correct web site instead of devtest.transdemoweb.com.

To download the file, send the link to the file to the Customer.

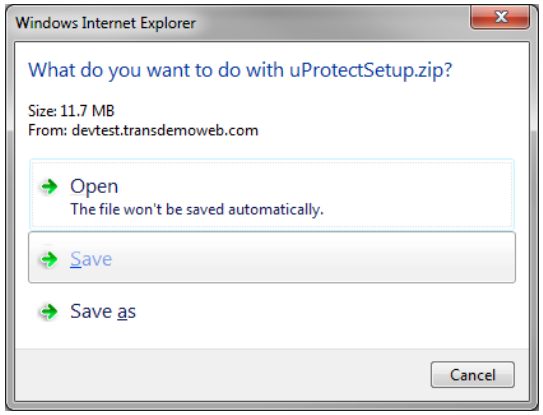
When using the ASPX page you would send the link as:

http://devtest.transdemoweb.com/download/downloadRelay Unify uProtect.aspx

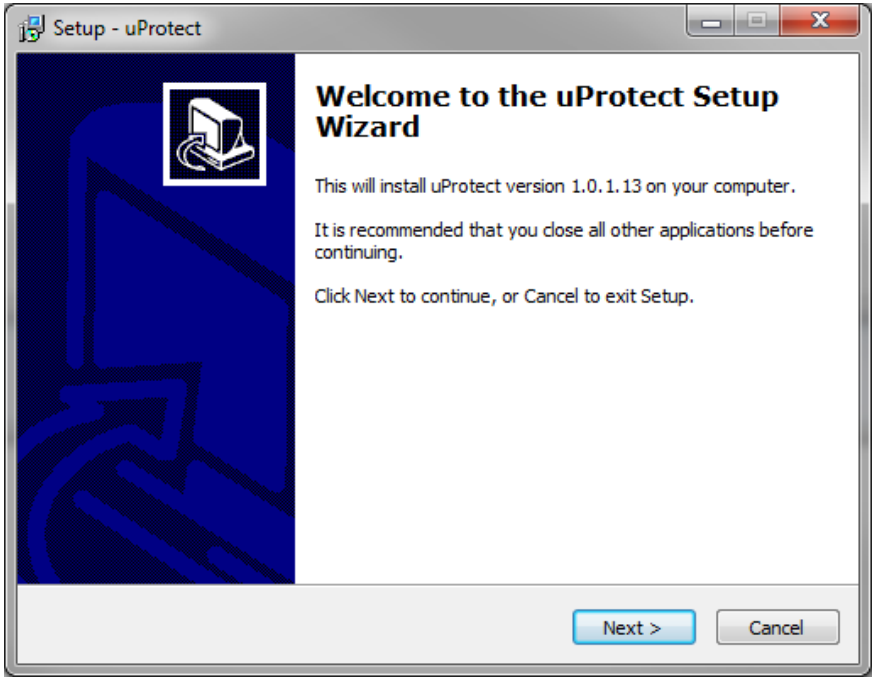
This would display as:

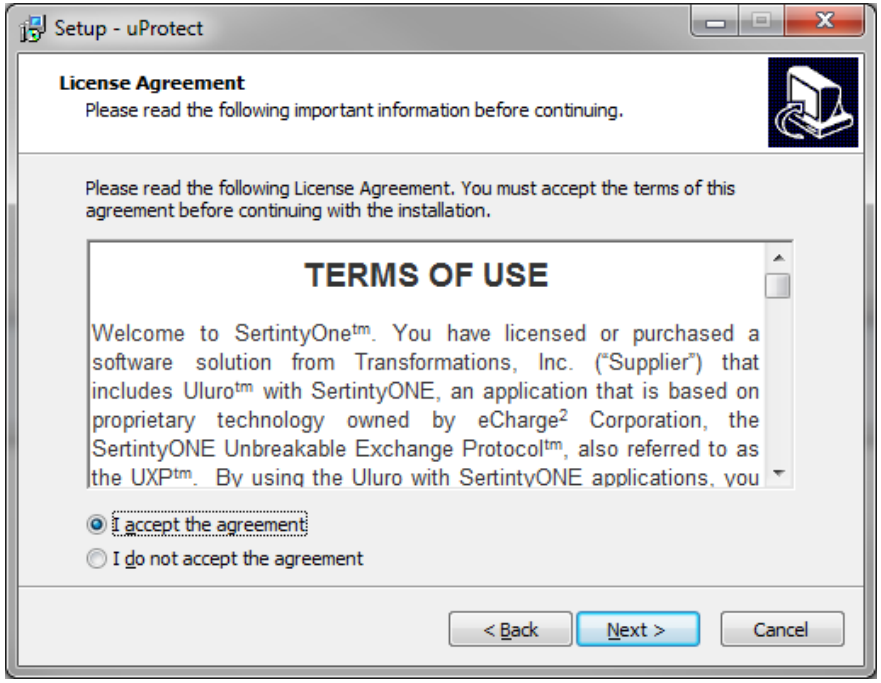


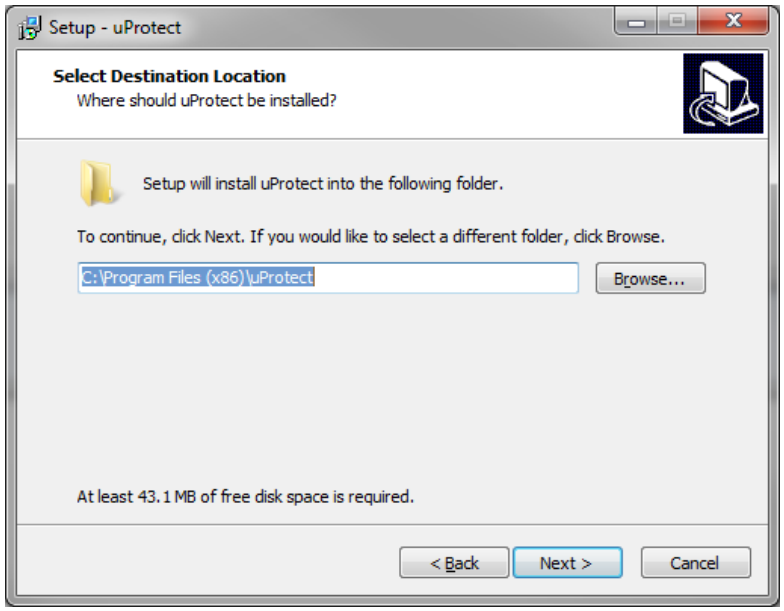
This directory should work for all clients that are available on the web. You do not have to set this up for each Relay Unify web client.

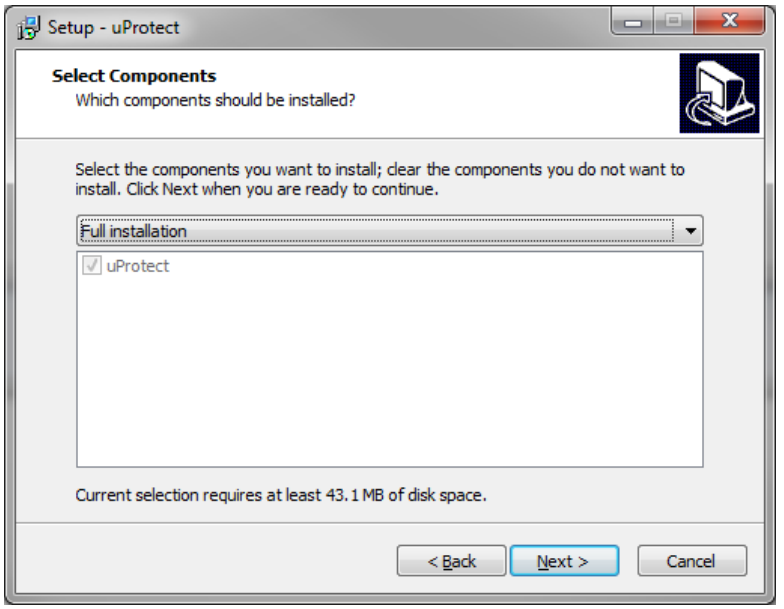


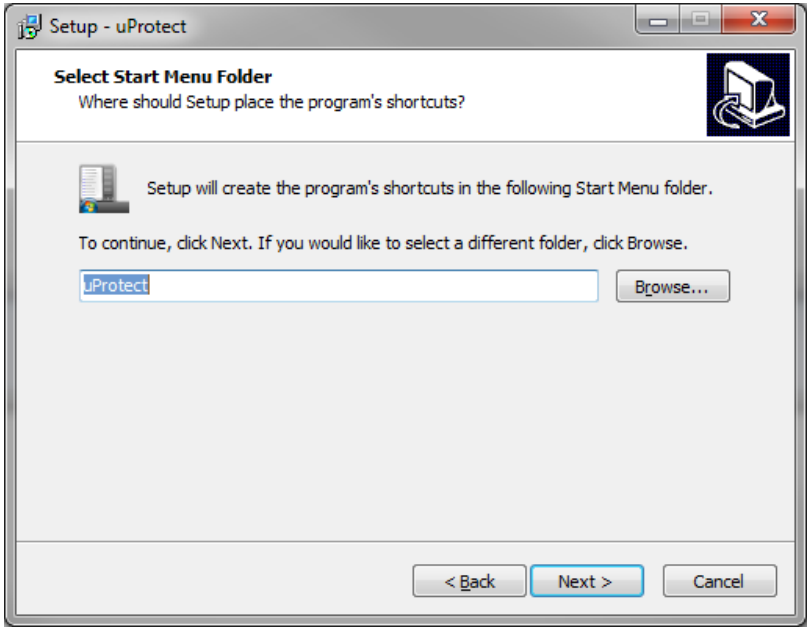
Save the File. Open and Run the Relay Unify uProtectSetup.exe.

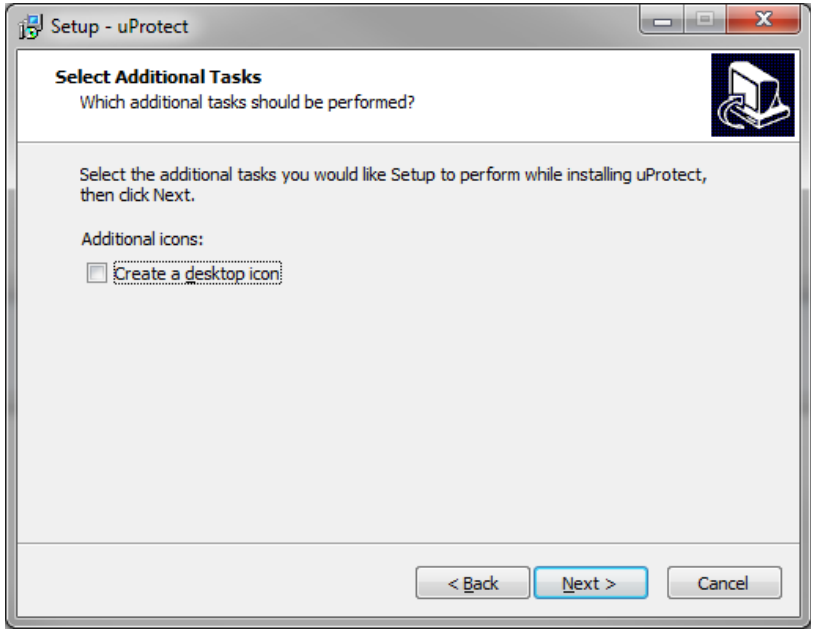


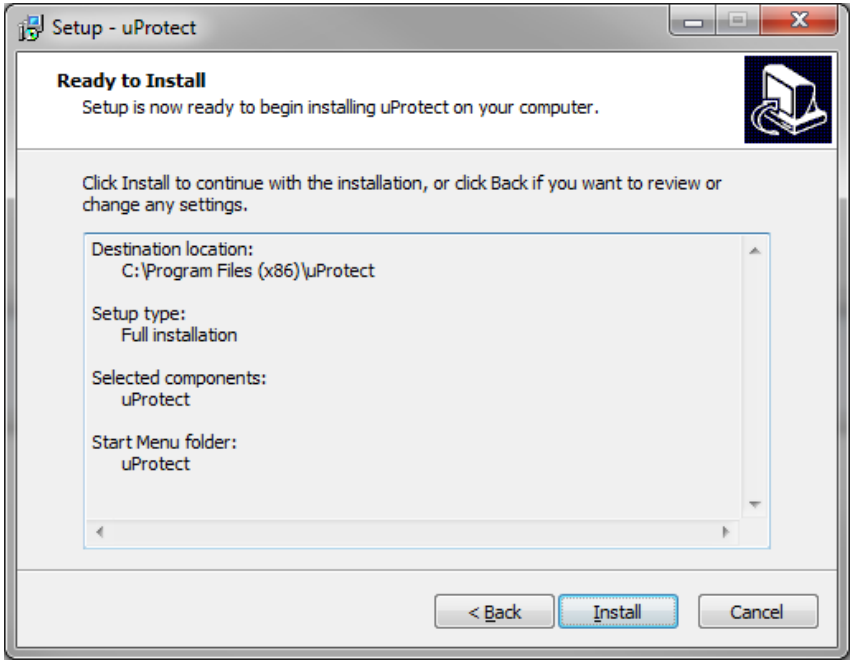


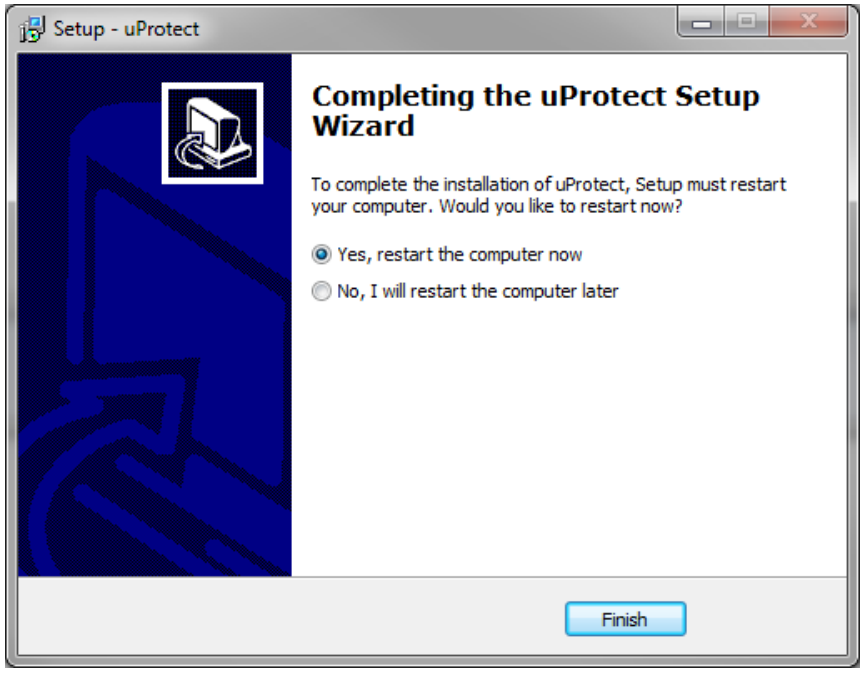






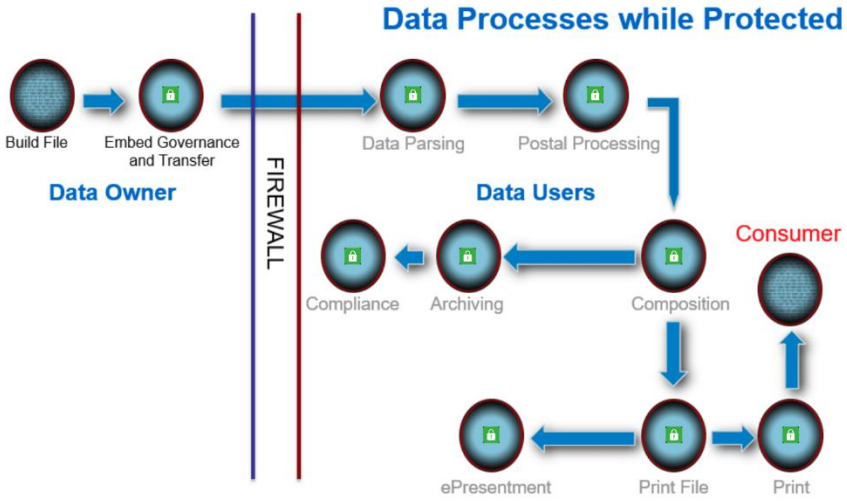






Processing a Secure Data File

This image shows a secure workflow using Relay Unify uProtect. Relay Unify uSecure can be configured to receive files that have had protection applied at customer's customer site by Relay Unify uProtect. This is the preferred method. A Secondary method is to receive unprotected file from customer's customer and have Relay Unify uSecure apply protection after file is received. This allows the customer to perform preprocessing scripts on data before processing through Relay Unify. This method removes many of the advantages in Relay Unify uSecure and is not our recommended method. This leaves customer data vulnerable on file system until Relay Unify uSecure applies SmartData protection to data.



The data is encrypted using 256-bit AES encryption along with the custom challenges; There is no key code management because there is no need for unencrypting the data in order to process the file.

The current version of Relay Unify uSecure does not protect the items listed below.

- RFT Files on disk system
- PDF image files (backer files)
- Image files

Tips:

The settings for the submission type and client are enbedded in the data file at the time it is processed. Changing those settings in uSetup will only effect future submissions.

The items below are not allowed when Relay Unify uSecure is enabled:

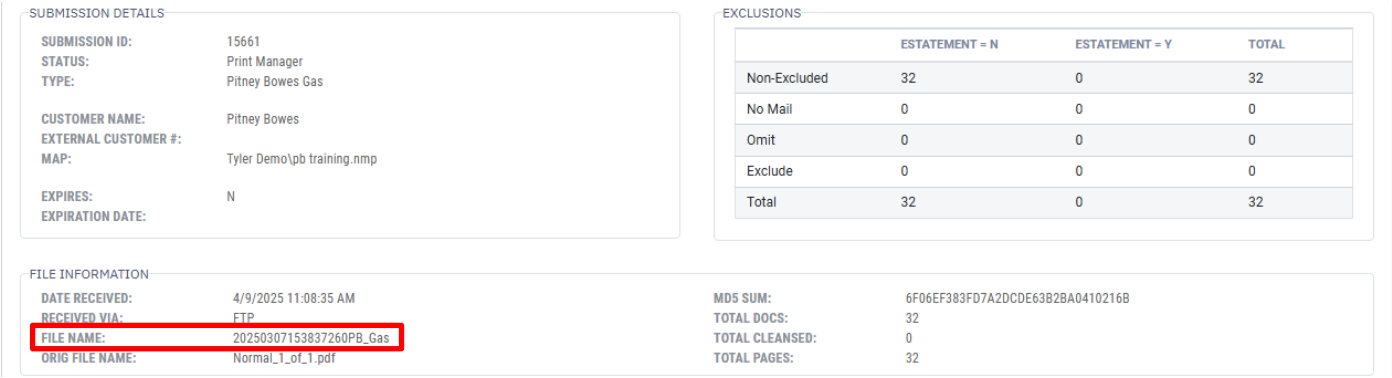
- Pre-generated PDF's

Implementing Relay Unify uSecure without using best practices will limit the ability of Relay Unify uSecure to protect customer's data. Even when using Relay Unify uSecure with best practices it may still be possible for unauthorized agents to access customer data.

Composition

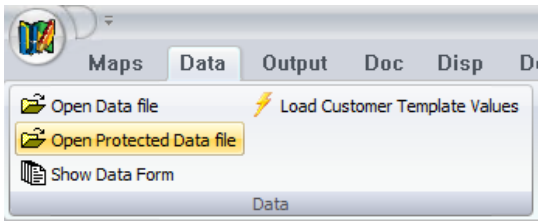
Relay Unify uSecure allows authorized composition users to remove data from the SmartData object and save customer data into an external SQL database. After data is removed from the smart data, Relay Unify uSecure can no longer protect your customer's data and you must rely on SQL protection and credentials. We strongly recommend that HIPPA and PCI information be kept as much as possible in the SmartData set and not placed into SQL.

The Relay Unify uSecure data for a submission can be opened if Relay Unify uCompose can determine the submission from the file name and path. This Path and Filename can be seen in uControl in the Submission Transaction Details.

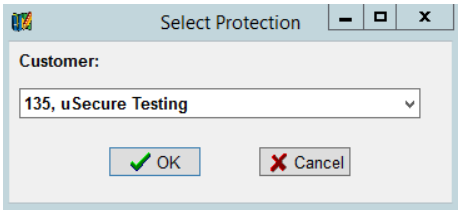


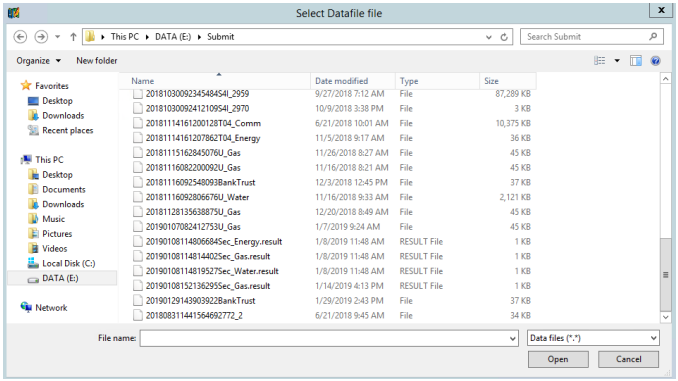
Secured data that has not been moved to a submission or that has been processed as a submission can be accessed from Relay Unify uCompose.exe.

In Relay Unify uCompose, the user must select the Open Protected Data file option under the Data ribbon.

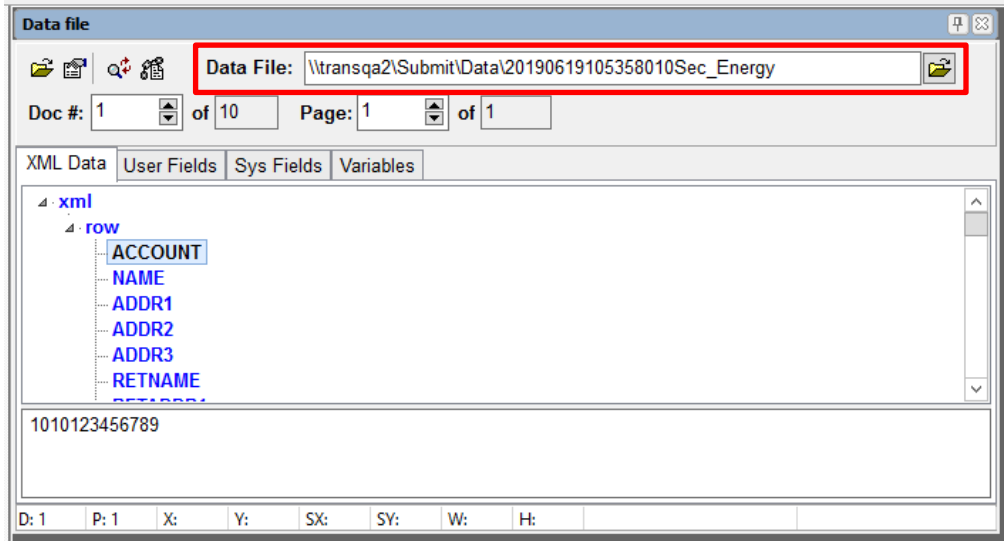


Then select the Customer for the Protection and the Protected file using the full UNC path from uControl.

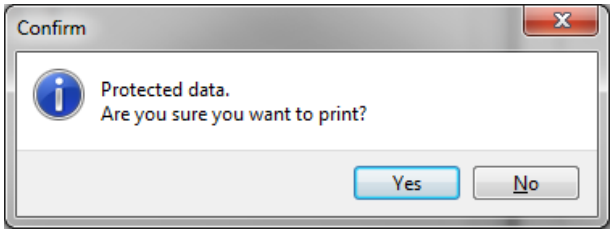




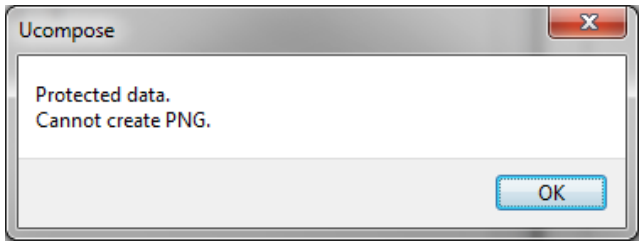
The protected file will be accessed and displayed unprotected.

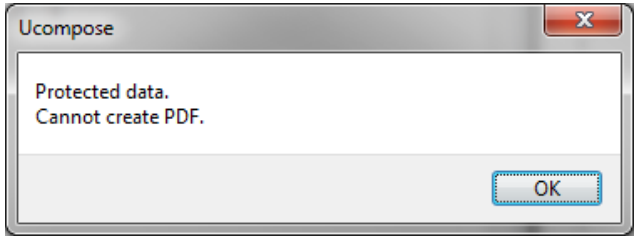


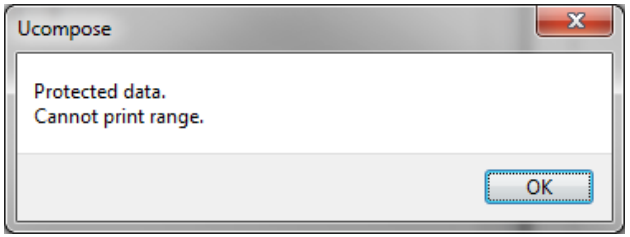
Any attempt to print the document will display confirmation dialog.



Protected data cannot be used to create a PNG or PDF or print a range of documents.





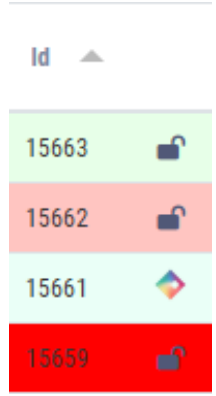


Any protected data file viewed in Relay Unify uCompose to build the map or make any edits prior to processing will be logged in the customer's Audit Info in uSetup.

uControl

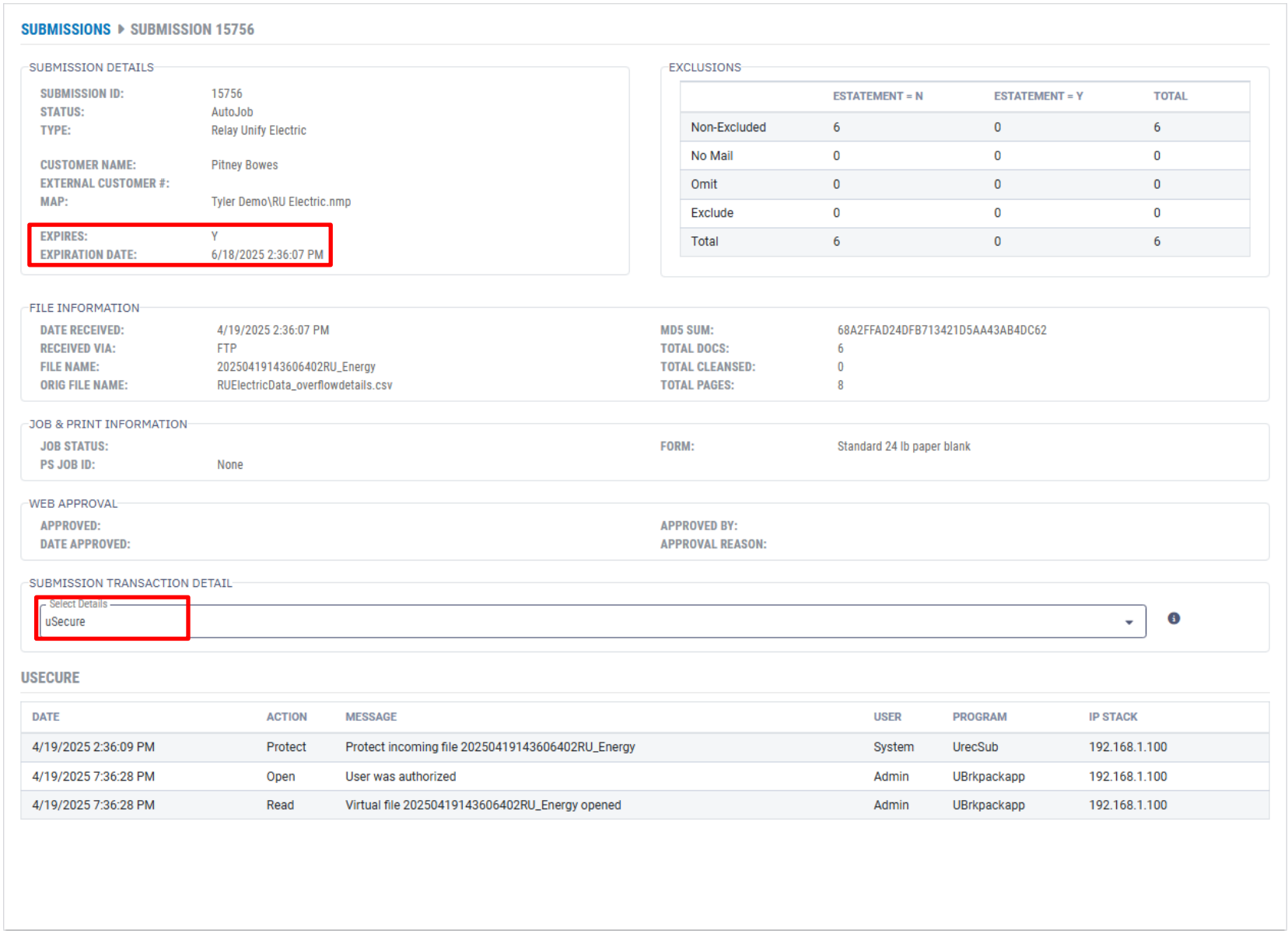
uControl does not need the Relay Unify uSecure DLL's. It displays information from the database and does not directly access the Relay Unify uSecure Data.

Secured Submissions will display with the Security icon; files not processed using Relay Unify uSecure will display the unlocked icon.



Right-clicking on a Submission and clicking View Details will display the transaction details. There is a dropdown tab to display the Relay Unify uSecure information.

The Expiration date of the file will be displayed in the submission details.



The Expiration date of the file will be displayed in the submission details.

Print Output

If the output print file is created using a print driver the entire file may reside on disk for a small amount of time until it is protected by Relay Unify uSecure. After the file is spooled to disk, Relay Unify uSecure will add SmartData protection to file (if the file has been created for the Relay Unify Print Manager) and delete the original print file. Therefore, the directory the print files reside in should be restricted, preferably for only Relay Unify to have access to the directory. The latest version of the Relay Unify Native PDF driver protects the output file as it is created.

If the output print file is not created for Relay Unify Print Manager the output print file will not be protected by Relay Unify uSecure. We strongly recommend using Relay Unify Print Manager with Relay Unify uSecure and not creating print jobs from uPrint.

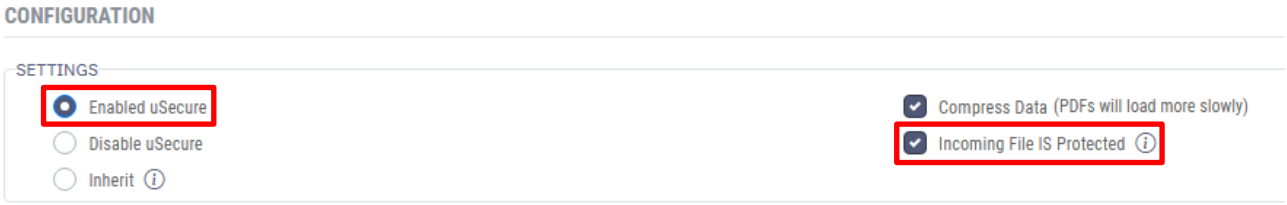
The print files for Relay Unify Print Manager will be unencrypted as they are sent to the printer at the time of print.

Using Relay Unify uSecure with Pre-processing

Relay Unify allows pre-processing of data before protecting the data with Relay Unify uSecure. The following are requirements for using Relay Unify uSecure with pre-processing.

Relay Unify uSecure must be installed, Licensed and enabled for the Submission Type.

To perform Pre-processing the Incoming data file must not be protected by Relay Unify uSecure.



Security

Incoming data is not secured with Relay Unify uSecure. Data is not secured until after pre-processing. Only after successful pre-processing is the data and original Archived data secured.

The Pre-processsing program has access to the unsecured data.

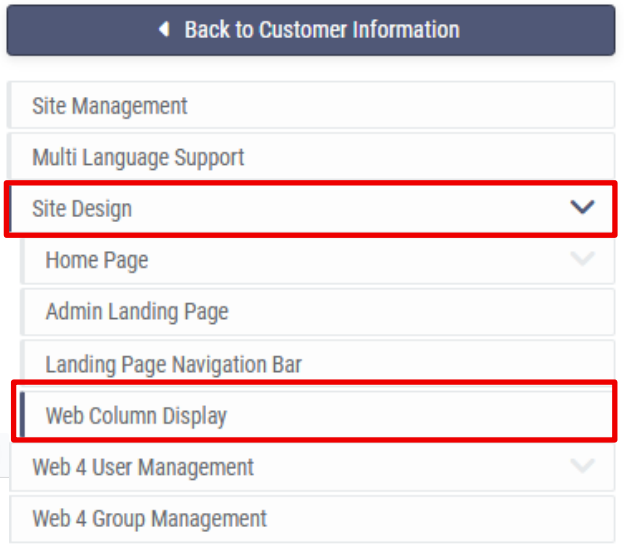
Full Audit records exist for Protecting and unprotecting the Archived data and Pre-processed data file.

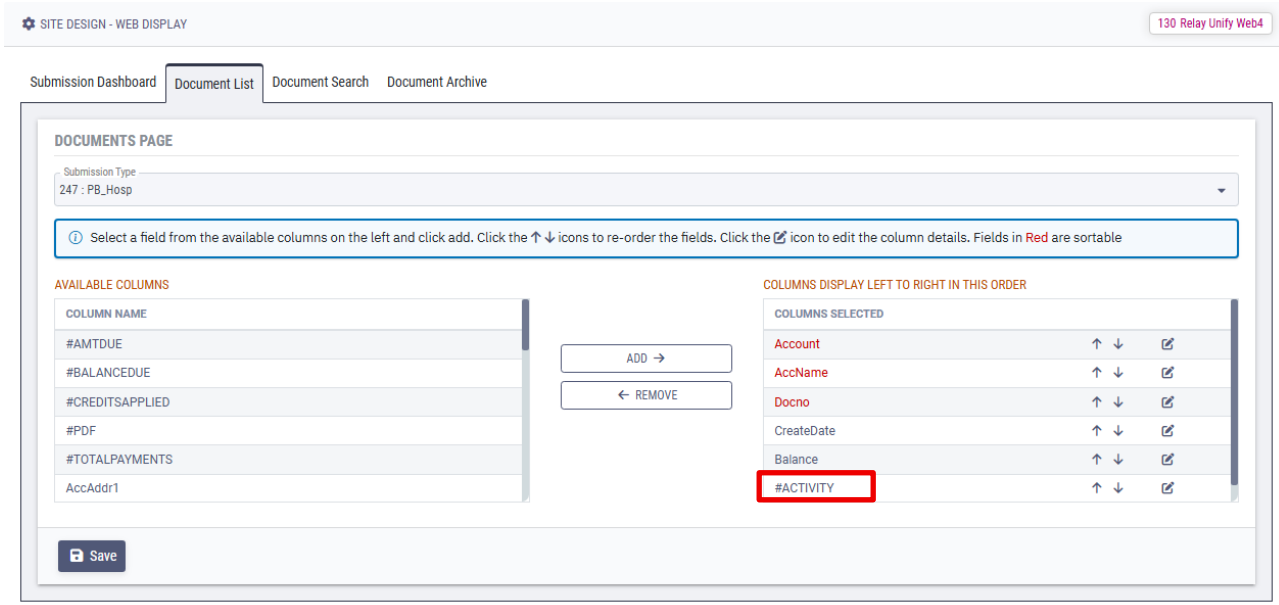
Reports & Audit Trail

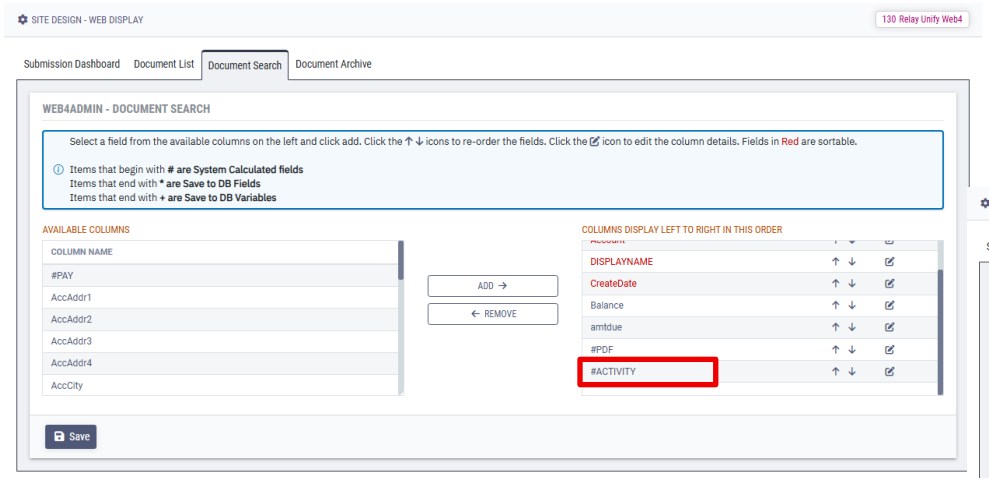
Activity Log

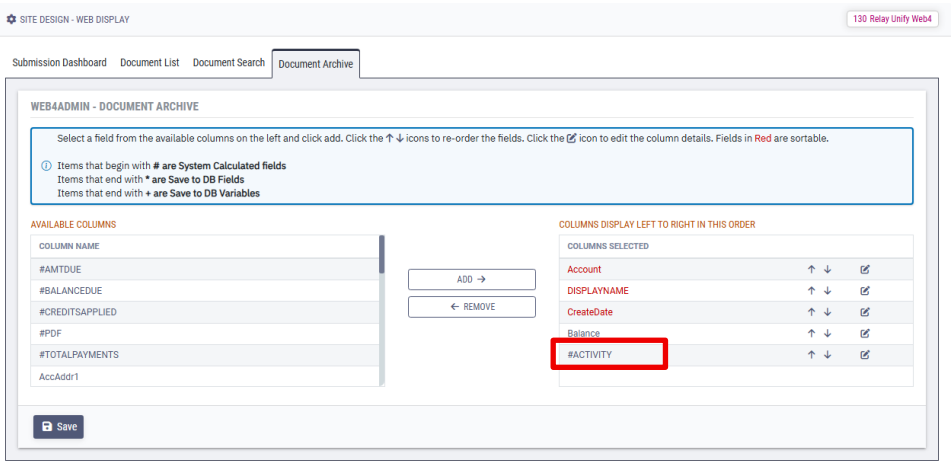
To set up activity log go to uSetup > Web Portal Setup > Site Design > Web Display Tab.

Add #ACTIVITY for the User Display or the search page as desired.

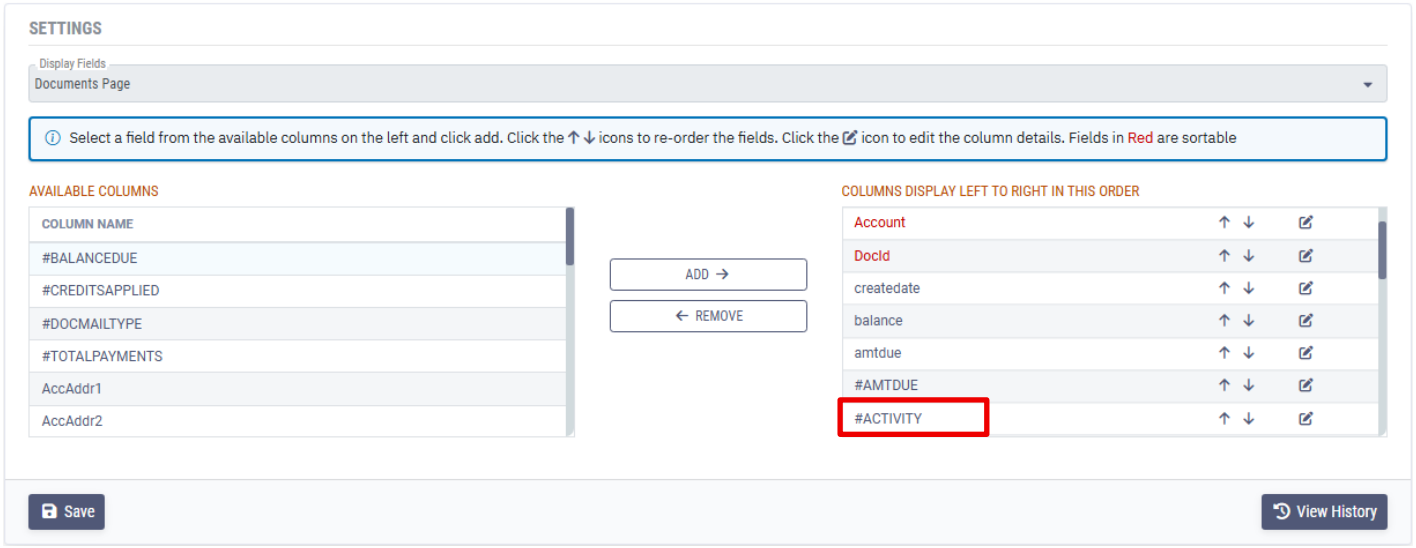






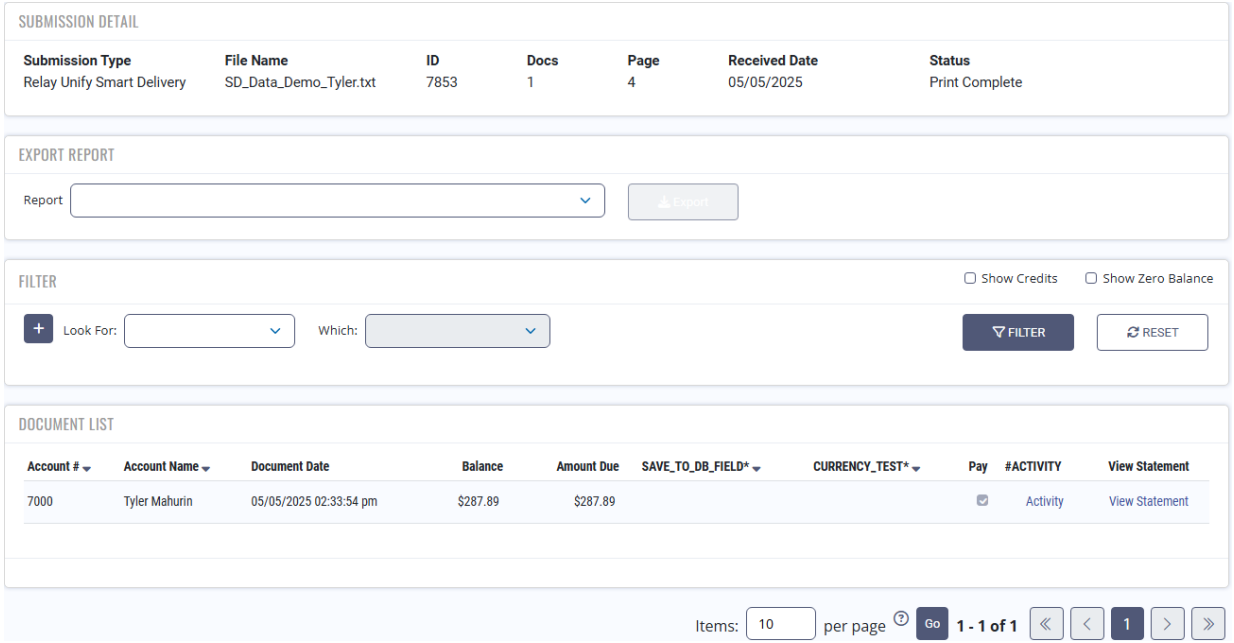


To add it to the custom search page once a submission is selected from the Customer, go to the Web tab of the submission and select Web Display.



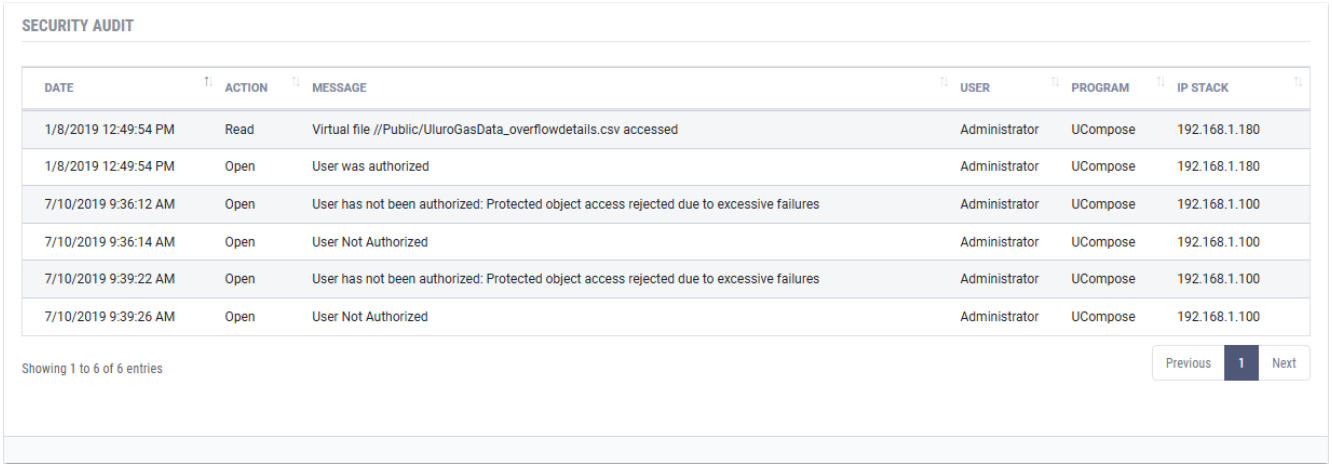
Permissions do not need to be granted to specific user types to see the Activity Log. Log in as any of the Admin type users that have been set up to see the Activity Log in the appropriate locations. Access any of the pages you have displayed #ACTIVITY on and you will see the Activity Log button next to the icon to view the document.

Click on the Activity button. This will show the activity of the document including the timestamp of each event and by which users. It includes the Proof of Delivery Verification, Document Opened Verification, Registration and Access Attempts and Successes for the document.



Audit Info

View Audit Information Allows viewing of File Access to Relay Unify uSecure files that have not been added to Relay Unify (Relay Unify uSecure files created by Relay Unify uProtect but not received into Relay Unify).

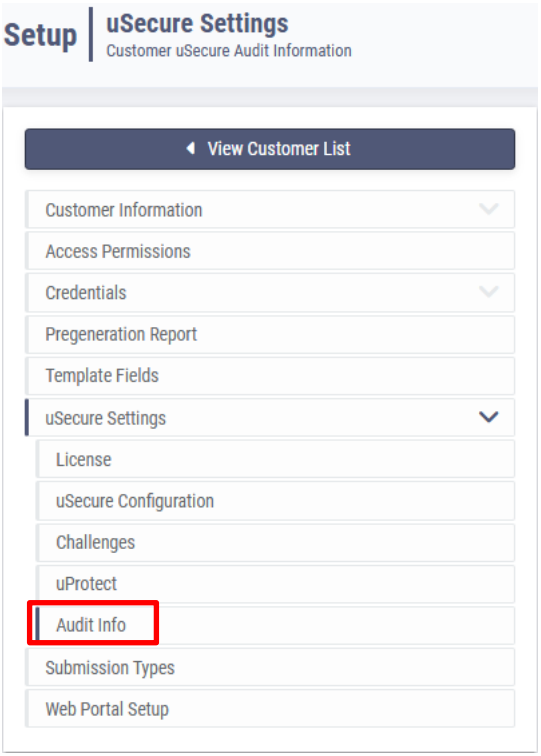


SECURITY AUDIT

DATE	ACTION	MESSAGE	USER	PROGRAM	IP STACK
1/8/2019 12:49:54 PM	Read	Virtual file //Public/UluroGasData_overflowdetails.csv accessed	Administrator	UCompose	192.168.1.180
1/8/2019 12:49:54 PM	Open	User was authorized	Administrator	UCompose	192.168.1.180
7/10/2019 9:36:12 AM	Open	User has not been authorized: Protected object access rejected due to excessive failures	Administrator	UCompose	192.168.1.100
7/10/2019 9:36:14 AM	Open	User Not Authorized	Administrator	UCompose	192.168.1.100
7/10/2019 9:39:22 AM	Open	User has not been authorized: Protected object access rejected due to excessive failures	Administrator	UCompose	192.168.1.100
7/10/2019 9:39:26 AM	Open	User Not Authorized	Administrator	UCompose	192.168.1.100

Showing 1 to 6 of 6 entries

Previous 1 Next



Relay Unify Glossary

Users:

- ***Relay Unify User*** – User created that has access to all of the Relay Unify programs on the Relay Unify database. This includes every module except for Relay Unify Print Manager.
- ***Relay Unify Print Manager User*** – A user that is created in Relay Unify Print Manager and only has access to log into Relay Unify Print Manager. This user is setup in addition to the Relay Unify user because Relay Unify Print Manager is on the Print Queue database and not the Relay Unify database
- ***Web User*** – A user from admin level to end user that has a login to the web portal.
- ***User Type*** – There are three user types by default: admin, CSR, and end/standard user. Additional user types can be created and customized. Each user type can have multiple users.

Inserts – This would be a physical "buck slip" that is inserted on the inserter.

Onserts - This would be an add-on attachment (i.e. PDF of some special notification or marketing piece) that is meant to be printed in-line with the document that now becomes part of the document.

CLID/Client/Customer – These terms are used interchangeably and refer to the client setup in uSetup. Each client can have multiple submission types under it. The CLID is the unique number given to each client.

Map – The document that is created using Relay Unify uCompose, our composition tool.

Omit – Documents marked not to get printed (excluding e-statements).

Exclude – Documents that do not get presorted; can still be printed but not with the standard run.

No Mail – Documents that are printed but not mailed (ex: send to customer).

Presort – In bins for mailing.

Cleanse – Make sure addresses are correct and updates them.

Submission Type – This is where the business rules are set up for a document.

Submission – Every time a data file is submitted, and a submission type is processed it is called a single submission. A submission type can have a submission run every month for example.

Job – A job consists of one or more submissions.

Merge Job – Consists of two or more submissions. Documents from either submission are merged into one document (mail piece) based on certain criteria. This can be done by Name, Address, or Account Number.

Combine Job – Consists of two or more submissions. Generally multiple submissions of smaller size are combined to get through Presort at once to receive presort discounts. The number of documents from each submission remains the same during a combine job.

Print Job – Created using a print configuration or manually in uPrint. One job can generate multiple print jobs.

Print File – The file(s) created as part of the print job that is sent to the printer. One print job can have multiple print files created by size or number of documents for example.