

# **Supplemental Guide**

## **Using the mySD Encrypt Service**



Revision 1.2  
October 2011

## Table of Contents

Purpose of this Document .....	4
About mySecureDelivery .....	4
About mySD Encrypt Service.....	4
The Components of the mySD Encrypt Service .....	6
Secure Publisher .....	6
Secure Open.....	6
Administrative Portal (Gateway) .....	6
The mySecureDelivery Trail .....	6
mySecureDelivery Threading .....	7
Registration Screen .....	8
Authentication Screen .....	11
Using the Secure Publisher .....	13
Now Let's Protect and Secure Your Electronic Information - Overview .....	13
Now Let's Protect and Secure Your Electronic Information - Detail.....	14
Setting an Expiration Date .....	15
Setting an Open On Date .....	19
Selecting Authorized Users .....	22
Save File .....	26
Using the Secure Open.....	29
Summary .....	32

## Purpose of this Document

The purpose of this document is to familiarize you with the features of the mySD Encrypt Service, which is a supplemental feature of the mySecureDelivery Service. This supplemental guide is designed to be used after you have familiarized yourself with the mySecureDelivery Service “Getting Started” guide, and assumes you have a good understanding of the offering.

## About mySecureDelivery

mySecureDelivery launched its' eInformation security service to allow anyone to protect, monitor, measure, and manage their information when sharing with partners, customers and other parties, whether on the Internet or Mobile.

We ensure that information security is available to anyone, anywhere, at anytime (the AnyWhere Network), all while minimizing the resources - time, talent, and money - required. By offering the mySecureDelivery Service as a Software-as-a-Service (SaaS), we enable individuals and companies to take full advantage of our service without implementation hassles, administrative overhead, and capital expenditures.

These guiding tenets position mySecureDelivery to be the trusted partner for anyone - individuals and Small and Mid-Sized Businesses (SMBs), using mobile platforms and the Internet, wanting safety and security in an easy to access, easy to use service.

## About mySD Encrypt Service

The mySD Encrypt Service is an additional feature to the mySecureDelivery Service. This Service provides a solution to the challenges of protecting, monitoring, measuring, and managing secure delivery for any type of file. The files available include all of those that can be handled in the mySecureDelivery Service (for reference, any file type that can be printed can be secured through the mySecureDelivery Service), but are ***now expanded to include file types such as video, audio, etc.***

All of the features of the mySecureDelivery Service are available with the mySD Encrypt Service, including:

- Industrial strength encryption – 256-bit AES;
- Password management
- Selection of the Security Profile
  - Setting an Expiration Date
  - Setting an Open On Date
  - Identify as a Private (Specified Users Only) or Public
  - Setting number of Views (Opens)
  - Setting number of Devices
- Creation of the Protected Information with the .msd file type
- Managing the Protected Information
  - Automatic Disable upon exceeding of Security Policy thresholds
  - Manual Disable or Enable through the Administrative Portal (Gateway)

- Thread Graphing and Management
- Monitoring the Protected Information
  - Collect all information on all Opens and Attempted Views Opens (Note: with mySD Encrypt Service the function of Views in mySecureDelivery Service is now replaced with Opens):
    - All device information (IP Address, MAC Address, Device Name)
    - Userid of Viewer
    - Date and Time of activity
    - Identifiers of prior opens for multi-point distributions

Whereas the mySecureDelivery Service protects, monitors, measures, and manages the Protected Information throughout its distribution lifecycle, the mySD Encrypt Service serves as a secure distribution process from point to point. Should the Viewer be authorized for the Protected Information, they will be able to Open the file which will in turn decrypt the Protected Information and store it on the Viewer device in its *native format*.

As an example, in the recording industry a major challenge is prerelease leaks. It seems as though this is something that is virtually unavoidable in the digital age.

One recent attempt to avoid the leaks was undertaken by two major artists with their new album. Although pirates and freeloaders are typically a major motivation to try and stop the leaks, their desire was to create that moment of unwrapping the CD and listening to it for the first time – for all of their fans.

In order to have this occur, they had to take extraordinary measures, including limiting WIFI in sessions, removing emails as a communications method, secret sessions at makeshift studios, biometric fingerprint security on drives, travel to key locations to even hear a track, securing artwork, vaulting almost everything for fear of discovery, and last minute deliveries to CD manufacturing plants. This type of process, although successful in this instance, proved to be very expensive, resource intensive and exhausting for key personnel.

Every artist would like to have leaks prevented, but the time, effort, resources, and costs of doing it in the fashion described above significantly lessens the number who could take advantage of it.

However, by using the mySD Encrypt Service, we can assist in these scenarios in a very cost effective and secure way.

Throughout this manual, we will be using the example of securing an audio file such that all the fans can only open it on August 24, 2011 at 7:00am and create that moment of unwrapping the CD and listening to it for the first time. This is a very simple example; however, the tenets of handling one track should be easy to extrapolate into the secure distribution of an entire album, complete with artwork and lyrics if desired.

# The Components of the mySD Encrypt Service

## Secure Publisher

mySecureDelivery provides you with the ability to secure your information for distribution. The main component of the Secure Publisher is the mySD Encryption Engine, which provides the processes for protecting and securing your electronic information. We have implemented the mySD Encryption Engine to allow you the flexibility and capability to protect any electronic information, including all types of audio, video, and graphic files.

The mySD Encryption Engine provides you with a step-by-step process to define all of the business rules necessary to secure the access to your Protected Information, such as:

- Identify whether the document is Public or Private document;
- Specify an embargo date (a.k.a. “Do not open until this date/time”);
- Expiration date/time; and
- Maximum number of opens and devices allowed.

This Secure Publisher is available only to subscribers of the mySD Encrypt Service.

## Secure Open

mySD Encrypt Service features a Secure Open where all valid recipients of your Protected Information will be able to open it and save it on your device. The Secure Open works in conjunction with the mySecureDelivery Service servers to:

- Authenticate Users;
- Allow/Deny opening based on Business Rules established;
- Provide information of activities for the mySecureDelivery Trail.

The Secure Open is provided at no charge to any recipient of mySD Encrypt Service Protected Information and can be downloaded from here.

## Administrative Portal (Gateway)

The mySecureDelivery Administrative Portal provides you with the ability to:

- Manage your account(s) information;
- Manage your contacts;
- View detailed information on all of your Protected Information (both from the mySecureDelivery Service and the mySD Encrypt Service); and
- Ability to manage your Protected Information (such as disabling your Protected Information or a particular User or thread of that Protected Information).

This Administrative Portal is available only to subscribers of the mySD Encrypt Service or the mySecureDelivery Service.

## The mySecureDelivery Trail

A key feature, and differentiators in the marketplace, is our unique mySecureDelivery Trail. This event activity log contains critical information on the distribution of your secured Protected Information. The

mySecureDelivery Trail contains the following information for every action performed/or attempted to be performed, on your Protected Information, such as:

- Type of Activity
  - Opens or Closes
  - Time Viewed
  - Attempted Opens with Denial
  - Enable/Disable
  - Business Rules changes
- Date/Time of the activity
- UserID of the person attempting to perform the activity (if available)
- IP Address, MAC Address, and Name of the device where the activity was performed
- Identifiers of the prior and current Protected Information viewers

### mySecureDelivery Threading

The mySecureDelivery Threading provides a complete tracking and graphic display of the delivery trail of your Protected Information. By providing the digital fingerprints of the senders and receivers, the mySecureDelivery Service provides you with intelligence that, until now, was unavailable. In addition, you now have the ability to:

- graphically display the distribution routes of your Protected Information;
- manage each distribution thread individually – or collectively; and
- disable or enable each distribution thread individually – or collectively.

Use of this business intelligence will provide a strong foundation for continued process improvement for your future secured distributions.

The following sections will walk you through the:

- Using the Secure Publisher; and
- Using the Secure Open.

For information on the installation of the Service, use of the Administrative Portal (Gateway), the Audit Trail, or the Threading please refer to the Getting Starting with mySecureDelivery Service Manual available on our web site at [www.mysecuredelivery.com/resources](http://www.mysecuredelivery.com/resources).

## Registration Screen

Before you can utilize any of the capabilities of the mySecureDelivery Service, you must register. The Registration process can be found by either clicking on the “REGISTER” button available on any Login Screen, or by going to the URL [https://mysecuredelivery.com/reg\\_srv.html](https://mysecuredelivery.com/reg_srv.html).

No matter what route you take to go to the Registration Screen, you will be presented with the following screen to start the process:

The screenshot shows a web browser window with the mySecureDelivery logo in the top left. The main content area features a registration form titled "Please Fill Out This Registration Form". The form contains several input fields: "Email Address", "Repeat Email Address", "Password", "Repeat Password", "First Name", "Last Name", "Organization", and "Department". Below these fields are three buttons: "Submit", "Go to Login page", and "Skip to Validation". A small note at the bottom of the form states: "In order to confirm your email address, we will send you an email containing a Validation Token. If you have already submitted the above information and have received the confirmation email, skip to the Validation page to finish registering".

The Registration Process requires the following information:

- Your email ID. This will be your Login name to the mySecureDelivery Service and where you will receive email communications from the Service such as the Validation Token to complete the Registration Process and Denied Access attempts;
- Confirm your email ID;
- Enter a strong password that will be used to login to the mySecureDelivery Service. Do not share this password with anyone;
- Confirm your password;
- Your first name;
- Your last name;
- Your organization name;
- Your department within your organization.

All fields are required and must be filled in before you will be permitted to continue with the registration process.



Once filled in, please click on the “SUBMIT” button. At this time the system will send a digital Validation Token to the email address you provided on the Registration Screen. The email should be received shortly after you hit the “SUBMIT” button.

Please check your Inbox for an email from mySD. This will be your digital Validation Token. Please highlight the token with your mouse and then click on “COPY” to copy the Validation Token to the clipboard. You will need this in order to complete the Registration Process.

Once you have received and copied the Validation Token, please go back to the Registration Screen at [https://mysecuredelivery.com/reg\\_srv.html](https://mysecuredelivery.com/reg_srv.html) and then click on the “SKIP TO VALIDATION” button at the bottom right of the screen.

The screenshot shows a web browser window with the mySecureDelivery logo at the top. Below the logo is a registration form titled "Please Fill Out This Registration Form". The form contains the following fields: Email Address, Repeat Email Address, Password, Repeat Password, First Name, Last Name, Organization, and Department. At the bottom of the form are three buttons: "Submit", "Go to Login page", and "Skip to Validation". A yellow callout box with an arrow points to the "Skip to Validation" button, containing the text: "Please click on this button to continue the Registration Process". Below the form, a small note states: "In order to confirm your email address, we will send you an email containing a Validation Token. If you have already submitted the above information and have received the confirmation email, skip to the Validation page to finish registering".

You will be taken to the Registration Validation Screen to complete the Registration Process.

The screenshot shows a web browser window with the mySecureDelivery logo at the top. Below the logo is a validation form titled "Please complete this Registration Validation Step". The form contains the following fields: Email Address, Validation Token, and Password. Red arrows point from yellow callout boxes to each field. The callout for "Email Address" says "Enter you Email address used in Registration". The callout for "Validation Token" says "Paste the Validation Token from the Registration Email". The callout for "Password" says "Enter your Password from the Registration". At the bottom of the form are two buttons: "Back to Registration Form" and "Finish Registration". A yellow callout box with an arrow points to the "Finish Registration" button, containing the text: "Click this button to complete the Registration Process".

On the screen you will provide the following:

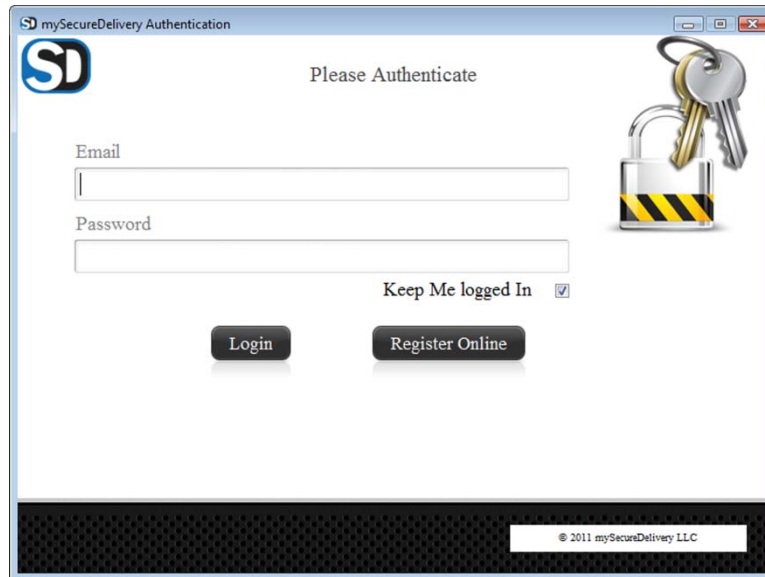
- The Email ID from the Registration Screen;
- Paste the Validation Token you received in the email after your completed the Registration Screen; and
- The password from the Registration Screen.

Once complete you will be registered to the mySecureDelivery Service and can login to the Service.

## Authentication Screen

Whether you are protecting information with the mySD Encrypt Service, or opening Protected information that was protected by the mySD Encrypt Service, if you are not currently logged in to the mySecureDelivery Service you will be asked to Authenticate yourself to the mySecureDelivery Service.

You will be asked to do this through the Authentication Screen as shown below.

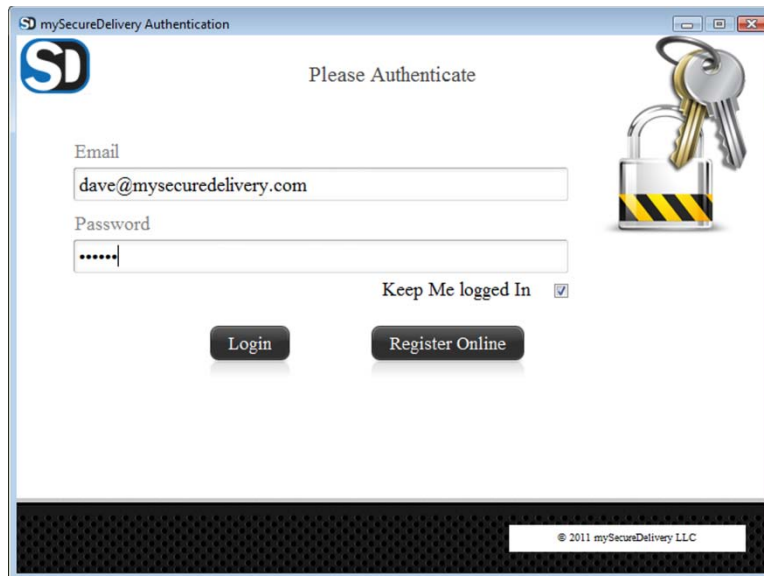


The screenshot shows a web browser window titled "mySecureDelivery Authentication". Inside the window, there is a logo with the letters "SD" in a blue circle. To the right of the logo, the text "Please Authenticate" is displayed. Below this, there are two input fields: one labeled "Email" and another labeled "Password". To the right of these fields is a graphic of a padlock with a key inserted. Below the input fields, there is a checkbox labeled "Keep Me logged In" which is checked. At the bottom of the form area, there are two buttons: "Login" and "Register Online". At the very bottom of the window, there is a footer that reads "© 2011 mySecureDelivery LLC".

In the input field underneath the Email label is where you will enter your Email ID. Your Email ID is the one you provided when you Registered for the mySecureDelivery Service (Subscribe, Free Trial, or the Free Secure Viewer). If you have not Registered for the mySecureDelivery Service yet, please click on the “REGISTER ONLINE” button and you will be taken to the Registration Screen.

In the input field underneath the PASSWORD label is where you will enter your password. Your password is the one you provided when you either subscribed to the mySecureDelivery Service or signed-up for the Free Trial.

There is a “KEEP ME LOGGED IN” checkbox on this screen. The default is checked, which means that the mySecureDelivery Service will keep you logged in on this device until you logout.



The image shows a screenshot of a web browser window titled "mySecureDelivery Authentication". The window has a blue header bar with the "SD" logo on the left and the text "Please Authenticate" in the center. On the right side of the header, there is an illustration of a padlock with a key inserted. Below the header, there are two input fields: "Email" and "Password". The "Email" field contains the text "dave@mysecuredelivery.com". The "Password" field contains six dots. To the right of the "Password" field, there is a checkbox labeled "Keep Me logged In" which is checked. Below the input fields, there are two buttons: "Login" and "Register Online". At the bottom of the window, there is a black footer bar with the text "© 2011 mySecureDelivery LLC" on the right side.

After you have filled in both fields please click on the “LOGIN” button.

If everything is correct, you will see a Green Check show, and then you will be taken to either the Secure Publisher or Secure Viewer. If there are any errors, you will receive them directly on the Authentication Screen and you will need to supply a valid Username and/or valid password in order to continue to the process.

## Using the Secure Publisher

The mySD Encrypt Secure Publisher has two components to it. The first is the mySD Encryption Engine, which utilizes industrial strength AES-256 bit encryption and a strong, true random number generator for key creation and password management system.

The second component is the Security Profile dialog boxes. This will lead you through a series of options available to manage the secure distribution behaviors of your Protected Information.

## Now Let's Protect and Secure Your Electronic Information - Overview

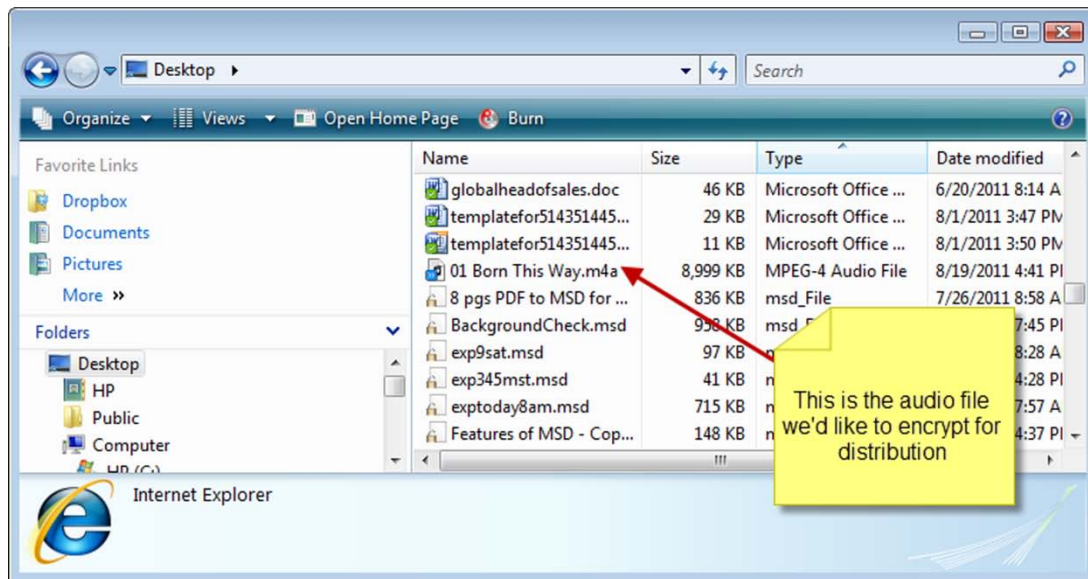
When you want to secure and protect your information, you will go through this simple process:

- Determine the electronic information that you want to protect;
- Right-click on the file and select the mySD Encrypt function;
- Go through the Security Profile dialog boxes presented to you which identify the parameters you want to have in effect for this Protected Information, such as:
  - Open after specified date/time;
  - Expiration date/time;
  - Business rule thresholds of open and devices; and
  - Specific Users, if required;
- Click the "FINISH" button and the mySD Encrypt Service will create your Protected Information, with a file name and in the location you've identified, ready for you to distribute.

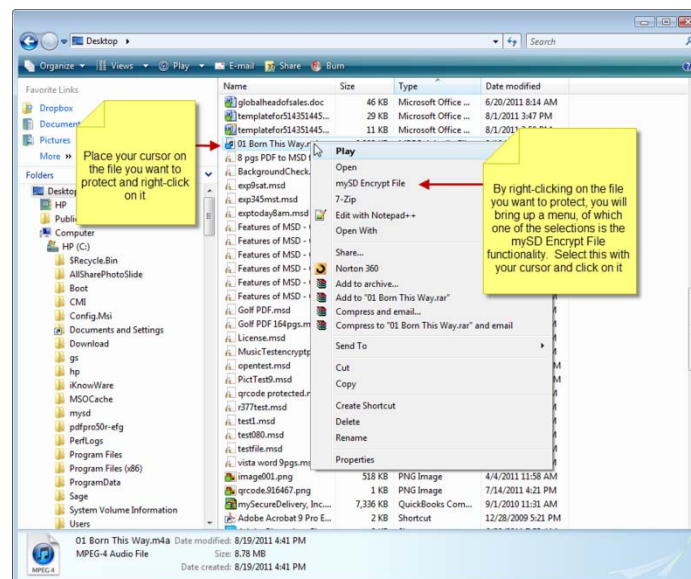
That's it! You're finished and ready to distribute your Protected Information through any process, such as E-mail, USB thumb drives, cloud storage, etc.

## Now Let's Protect and Secure Your Electronic Information - Detail

To protect any type of information, just locate the file you want to protect.



Right-click on the file you want to protect, "01 Born This Way.m4a", and you will bring up a menu of activities. Move your cursor over the mySD Encrypt File activity and left-click on it. You will launch the mySD Encrypt Secure Publisher.



At this point, the mySD Encrypt Service Secure Publisher set of dialog boxes you will be presented will be to establish the Security Profile for your Protected Information.

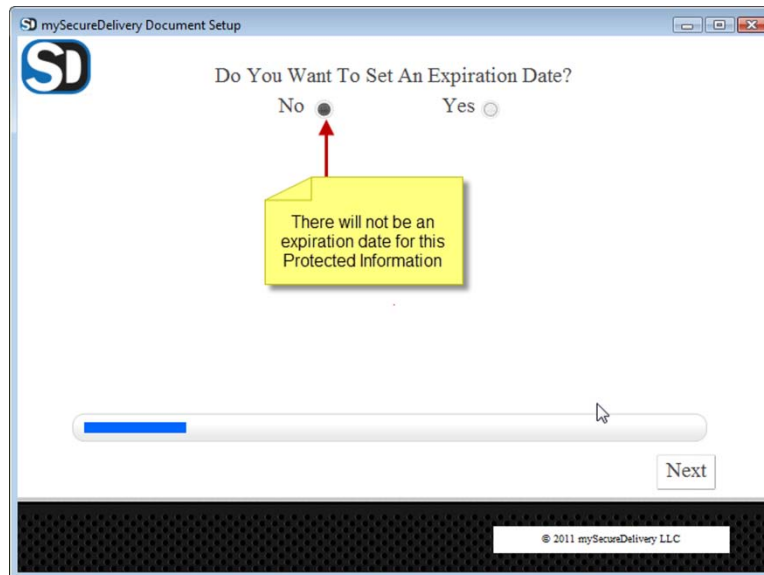
The Security Profile for the Protected Information can be one or any combination of the following elements:

- Expiration Date and Time
- Open On Date and Time
- Selecting Authorized Users (Private Document) or not (Public Document)

- Specifying limits on number of Opens or Devices a User can have.

### Setting an Expiration Date

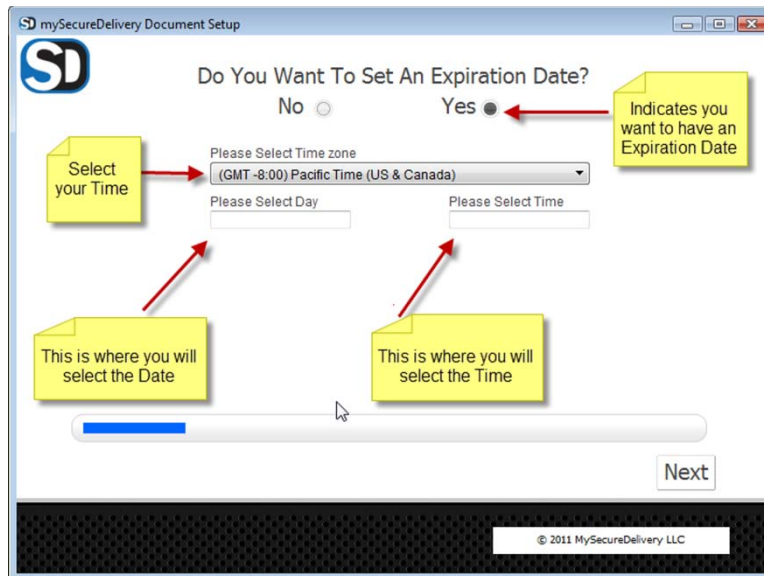
The first Security Profile dialog box will be to set an Expiration Date, if you require one. The Expiration Date tells the mySD Encrypt Service on what date, and at what time, this document should not be viewed after.



If you do not need an Expiration Date, please click the “NEXT” button on the bottom right of the screen. “No” Expiration Date is the default (as you see the “No” radio button is selected), and the “NEXT” button will take you to the “OPEN ON DATE” dialog box.

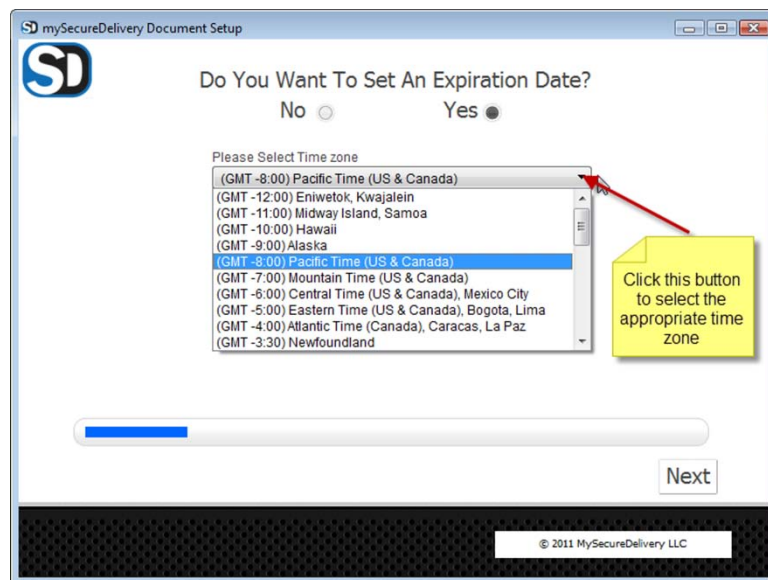
If you want an Expiration Date, you will click the “YES” radio button. As an example, you may have a demo track that you share with your partners that is only valid for one week. You can set the Expiration Date to be at 11:59pm on the last day of the week, which will automatically Disable the Protected Information at that time.

To set the Expiration Date, you would click on the radio button at the top of the dialog box, and you are presented with the details of setting the Expiration Date and Time.



With the details exposed, you can now select three items.

- The first is to select your Time zone. This field will be defaulted to your local time zone, but you can change by clicking on the down arrow and then selecting a value from the list. For select time zones you can choose between Standard Time and Daylight Savings Time.



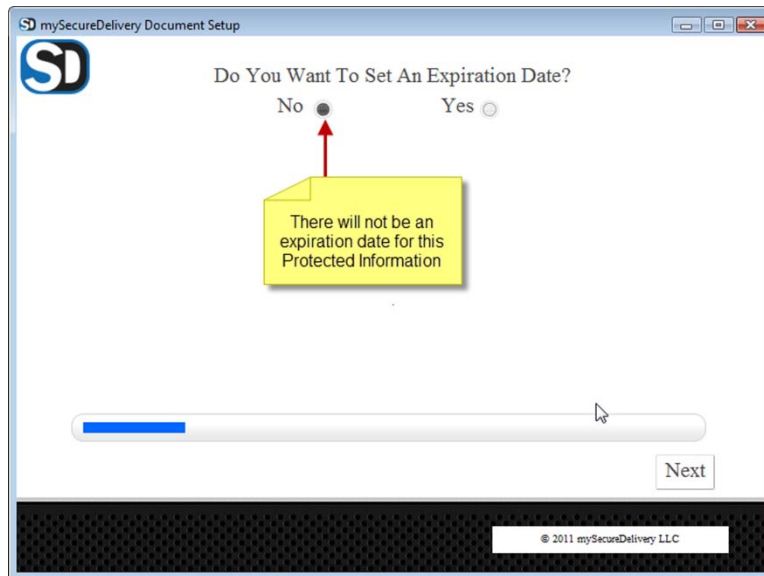
- The second is to select the Day you'd like to have the Protected Information expire on. Place your cursor in the input field under the "Please Select Day" and click on it. You will be presented with a month-at-a-time calendar, which you can navigate to the next month by clicking on the forward arrow at the top of the calendar box. Place the cursor on the date that you want the Protected Information to expire and click it. The date will then be placed in the input box for you. You can also type in the date you want in the input box directly in the format of MM/DD/YYYY.



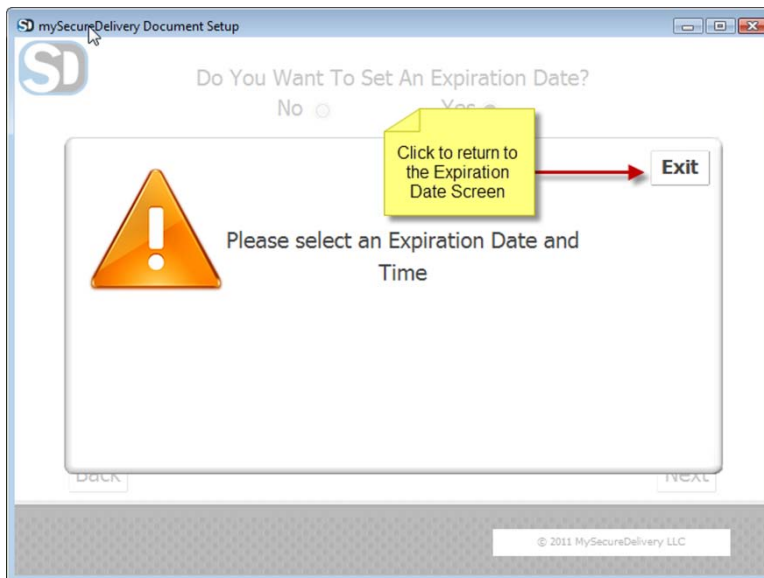
- The third is to select the Time you'd like to have the document expire on. Place your cursor in the input field under the "Please Select Time" and click on it. You will be presented with an Hour and Minute table where you can click on the Hour (in either AM or PM) and the Minute. The default will always be the current hour and the minutes will be 00. Click on the Hour you want – ensuring you choose the hour in the "AM" rows if you want after midnight but before noon or the "PM" rows if you want after noon until midnight. Then click on the Minutes, which are displayed in increments of 5 minutes. The time will then be placed in the input box for you, and the Hour and Minute Table will be closed. You can also type in the time you want in the format HH:MM AM (or PM).

When you have filled in three items, please click on the "NEXT" button to move to the next dialog box, the Open On Date.

For the purposes of our scenario, we will not have an expiration date for our Protected Information, so we would use the default of "NO" and click the "NEXT" button.

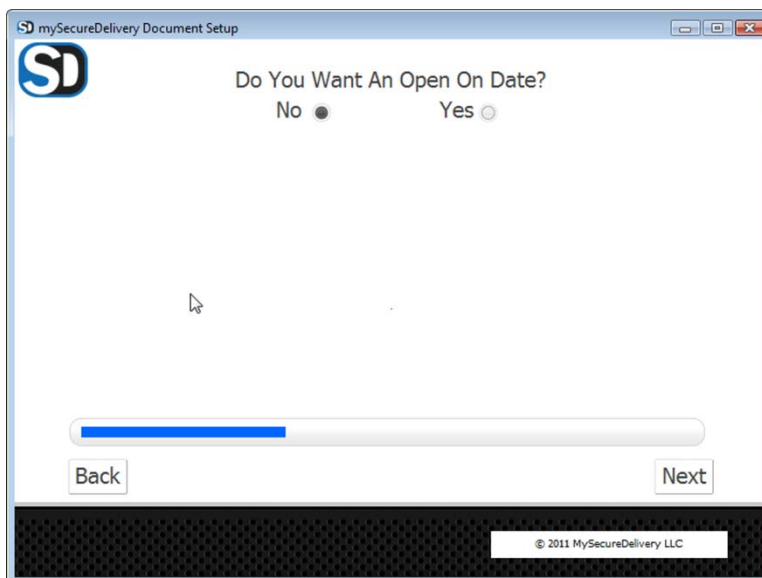


If there are any errors in filling in any of the three fields, you will be presented with the error message screen prompting you to correct the errors.



## Setting an Open On Date

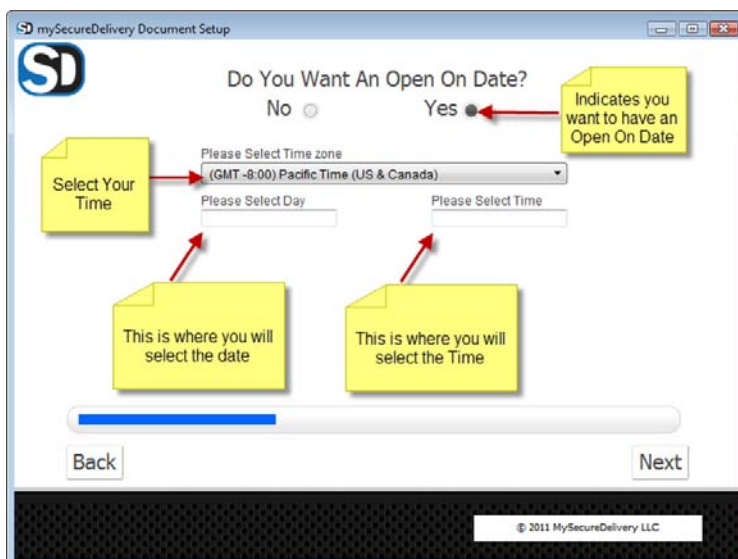
The second Security Profile dialog box will be to set an Open On Date, if you require one. The Open On Date tells the mySD Encrypt Service on what date, and at what time, this document should not be opened before.



If you do not need an Open On Date, please click the “NEXT” button on the bottom right of the screen. “No” Open On Date is the default (as you see the “No” radio button is selected), and the “NEXT” button will take you to the Select Authorized Users dialog box.

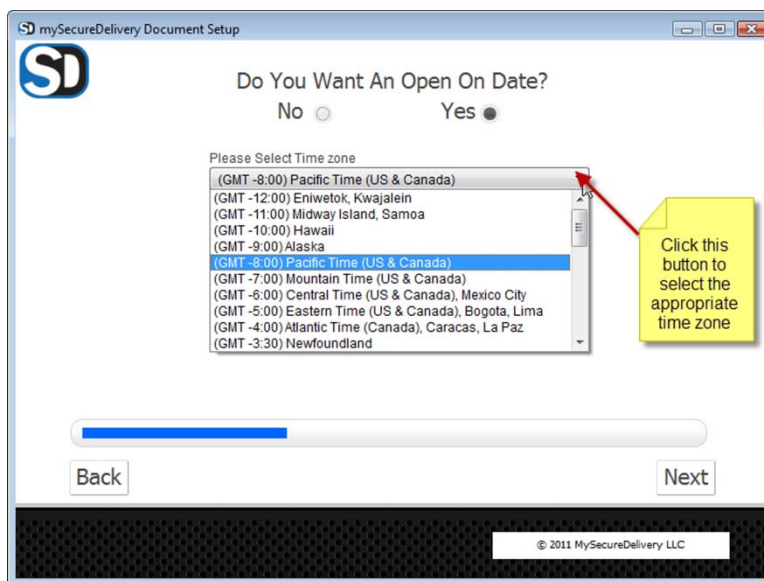
If you want an Open On Date, you will click the “YES” radio button. In our scenario, we don’t want anyone to open the audio track before August 24<sup>th</sup> at 7:00am. By setting the Open On Date to this date and time, you can ensure that all the fans have the Protected Information (audio track) but they will be unable to open and listen to the track until August 24th, 2011 at 7am.

To set the Open On Date, you would click on the radio button at the top of the dialog box, and you are presented with the details of setting the Open On Date and Time.

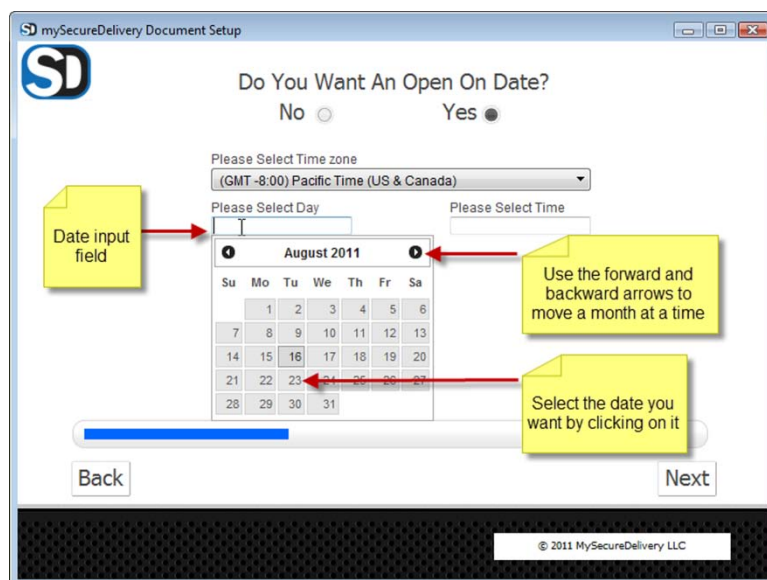


With the details exposed, you can now select three items.

- The first is to select your Time zone. This field will be defaulted to your local time zone, but you can change by clicking on the down arrow and then selecting a value from the list. For select time zones you can choose between Standard Time and Daylight Savings Time.



- The second is to select the Day you'd like to have the document not opened before. Place your cursor in the input field under the "Please Select Day" and click on it. You will be presented with a month-at-a-time calendar, which you can navigate to the next month by clicking on the forward arrow at the top of the calendar box. Place your cursor on the date that you want to have the document not opened before and click it. The date will then be placed in the input box for you. You can also type in the date you want in the format of MM/DD/YYYY.



- The third is to select the Time you'd like to have the document not opened before. Place your cursor in the input field under the "Please Select Time" and click on it. You will be presented

with an Hour and Minute table where you can click on the Hour (in either AM or PM) and the Minute. The default will always be the current hour and the minutes will be 00. Click on the Hour you want – ensuring you choose the hour in the “AM” rows if you want after midnight but before noon or the “PM” rows if you want after noon until midnight. Then click on the Minutes, which are displayed in increments of 5 minutes. The time will then be placed in the input box for you, and the Hour and Minute Table will be closed. You can also type in the time you want in the format HH:MM AM (or PM).

mySecureDelivery Document Setup

Do You Want An Open On Date?

No ☐ Yes ☒

Please Select Timezone

(GMT -8:00) Pacific Time (US & Canada)

Please Select Day

08/24/2011

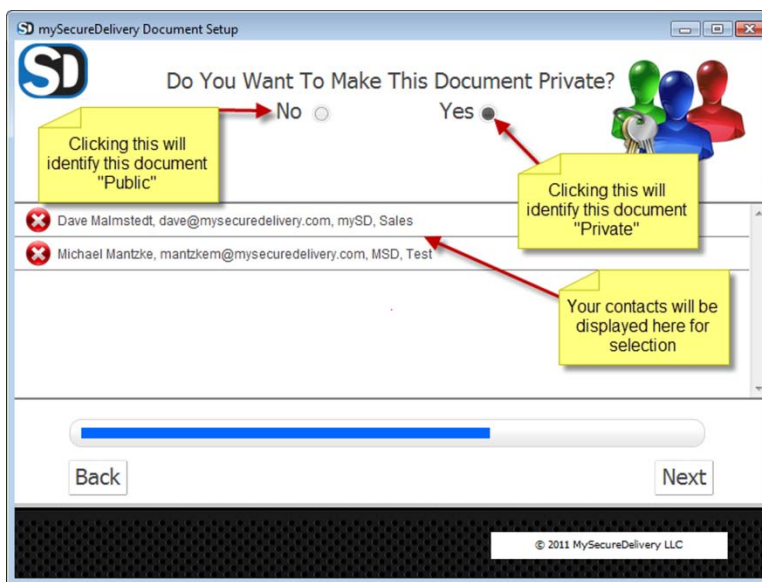
Please Select Time

07:00 AM

Hour	Minute
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10
11	00 05 10
12	00 05 10
01	00 05 10
02	00 05 10
03	00 05 10
04	00 05 10
05	00 05 10
06	00 05 10
07	00 05 10
08	00 05 10
09	00 05 10
10	00 05 10

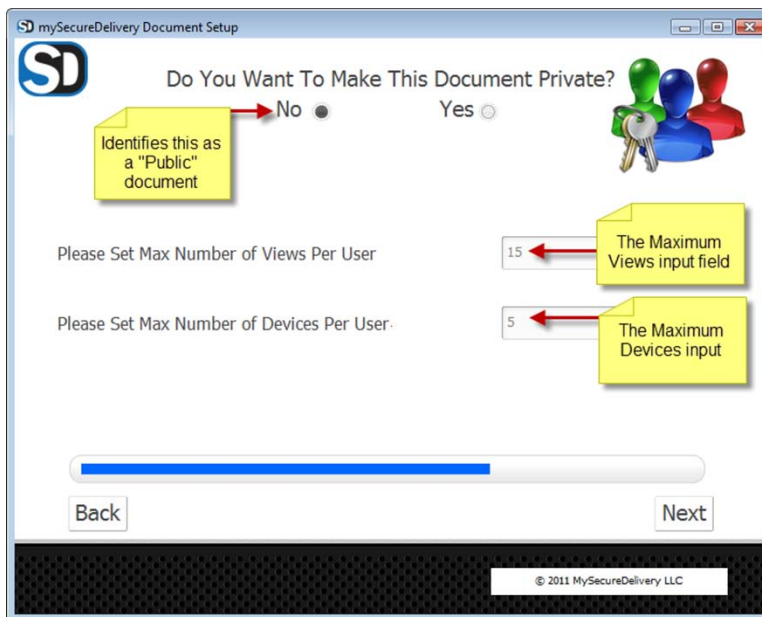
## Selecting Authorized Users

The fourth Security Profile dialog box will be to determine whether this document is Private, which means that you will select a User, or a number of Users, that will be authorized to open this Protected Information. You can also make this Protected Information Public, which means that anyone with a mySD Encrypt Secure Open and the Protected Information can open it – subject to all of the other business rules in the Security Profile associated with this Protected Information. Public documents will still be managed by all of the other business rules you put into place for this Security Profile.



## Public Documents

If you want the document to be Public click the “NO” radio button. You will then be presented with two additional items to complete for each recipient of the document. If you want a Private document, which means you will identify specific contacts that will be authorized to view this document, please go to the next section, Private Documents.



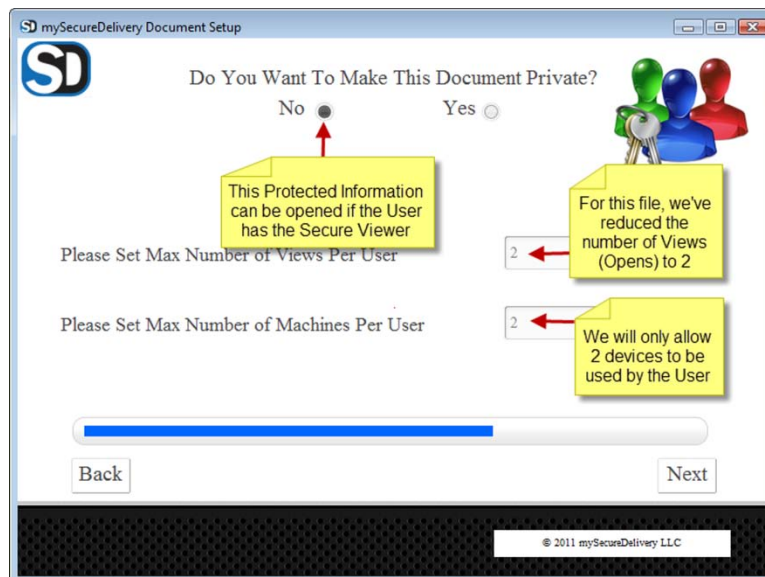
The two items, which have default values specified, are:



- Please Set Max Number of Views (Opens) Per User – you can set up the maximum number of Opens of the Protected Information each recipient can have. By default, each recipient will be limited to 15 opens. If you want less or more opens, please use the cursor to highlight the value and then type in the number of opens you wish to allow. This field will only accept numeric values.
- Please Set Max Number of Devices Per User – you can set the maximum number of devices (laptop, desktop, mobile device, etc.) that you want to allow a receiver to utilize. By default, each recipient will be limited to 5 devices. If you want less or more devices, please use the cursor to highlight the value and then type in the number of devices you wish to allow. This field will only accept numeric values.

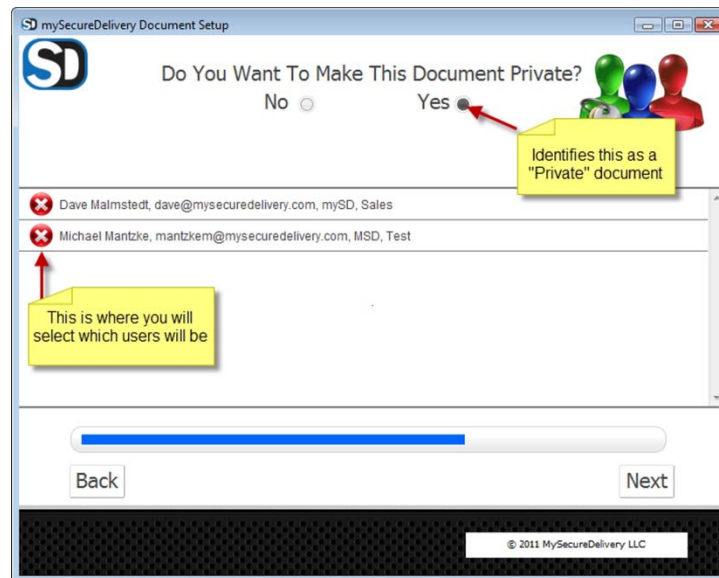
When you have set the values as you want, please click the “NEXT” button to go to the last Security Profile dialog box, Save File.

In our example, we will limit the number of Opens and Devices to be used to 2, and make this Public.

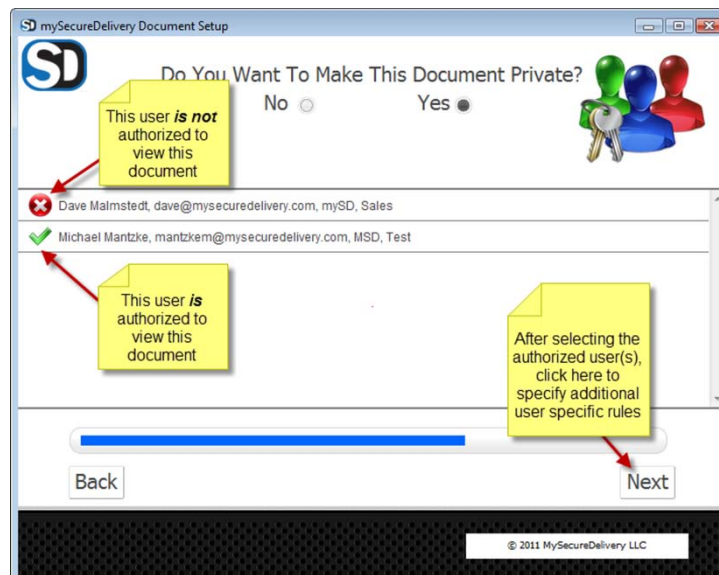


## Private Documents

If you want to select the specific Users who can open your Protected Information, you will click the “YES” radio button. You will then be presented with a list of your Contacts that can be chosen to be the only Users who can open this Protected Information.

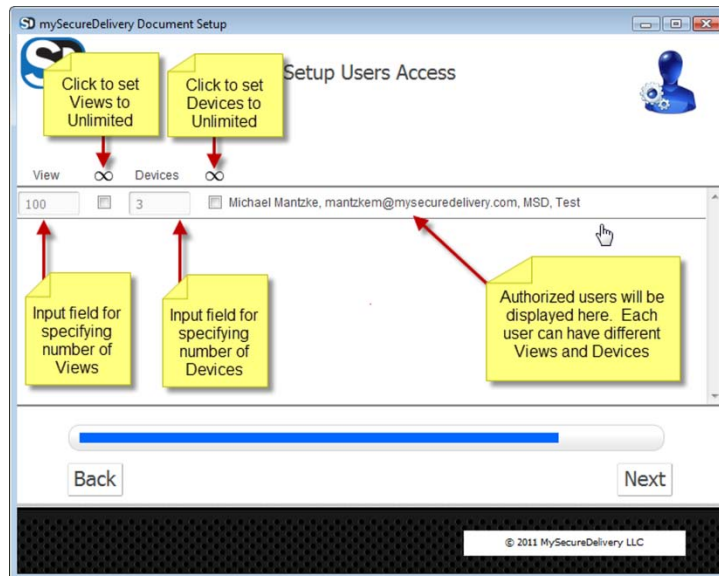


All of your Contacts in the mySD Encrypt Service will be displayed on your screen, including their User name, E-mail ID, company name, and department, preceded by a red “X”. The red “X” indicates that this User is not an authorized receiver of this document and will not be able to view. If you would like a User to be authorized, click on the red “X” and it will be turned to a green check mark. Do this for any Users you wish to be valid. In the example below, there will be one authorized User for this Protected Information.



After you have selected all the valid Users, please click the “NEXT” button, which will take you to the Setup Users Access dialog box.

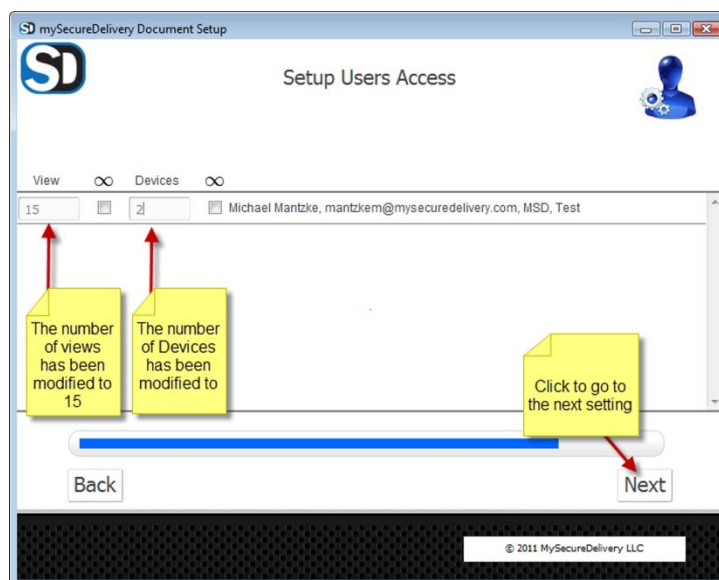




From this screen you can set up the number of opens and devices that each User will be authorized for. The default for Views (Opens) is 100 and the default for Devices is 3 for each valid User. You can also set the maximum Views (Opens) and/or Devices to be infinite by clicking the check box under the Infinity sign. If you check the Infinity box, you will see the value “UNLIMITED” in the input field.

If you are satisfied with the default values, please click the “NEXT” button and you will be taken to the last Security Profile dialog box, Save File.

To change the Views or Devices for a User, highlight either the Views or Devices input field on the specific User row and then type in a new numeric value.

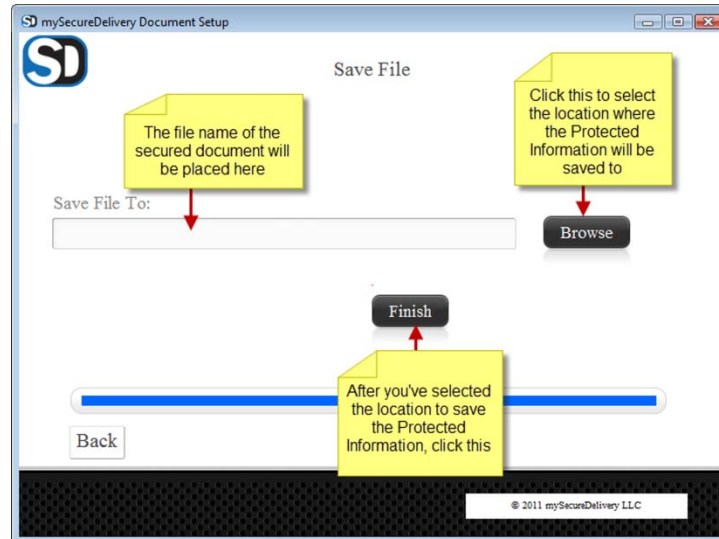


When you have made the modifications desired, please click the “Next” button and you will be taken to the last Security Profile dialog box, Save File.

You can also hit the “BACK” button which will take you to the prior dialog box, Select Authorized Users.

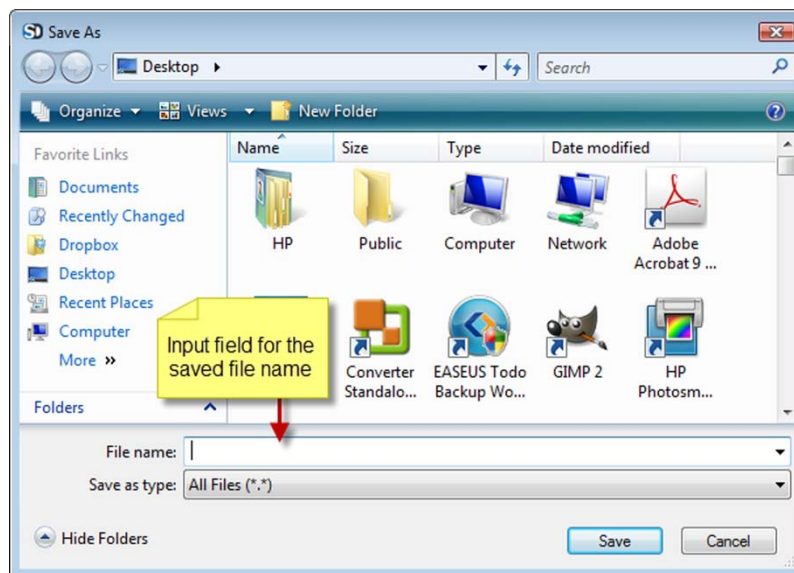
## Save File

The last Security Profile dialog box will be to determine where your Protected Information will be saved.



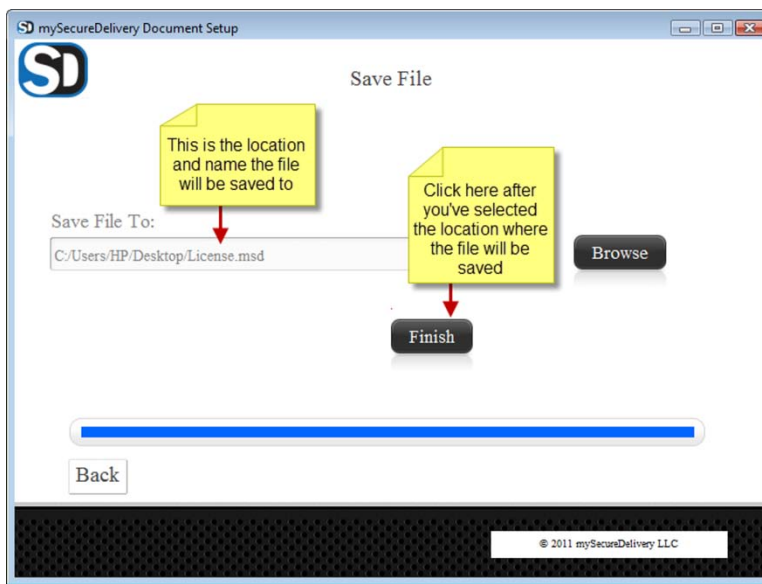
All Protected Information by the mySD Encrypt Service will be saved with a file extension of .msd. As an example, if you save the file with a name of AudioBTW, it will be saved as AudioBTW.msd. The .msd file extension is associated with the mySD Encrypt Secure Open which will be used to open the Protected Information.

To save the file, please click on the “BROWSE” button. You will be presented with the Save As dialog box, which is where you will specify the File Name and the location of where the file will be saved.



In the File name box please type the name of the file you want your Protected Information to be and click Browse Folders arrow to choose the folder you want to save the file to. By default we save the protected file in the folder you last used.

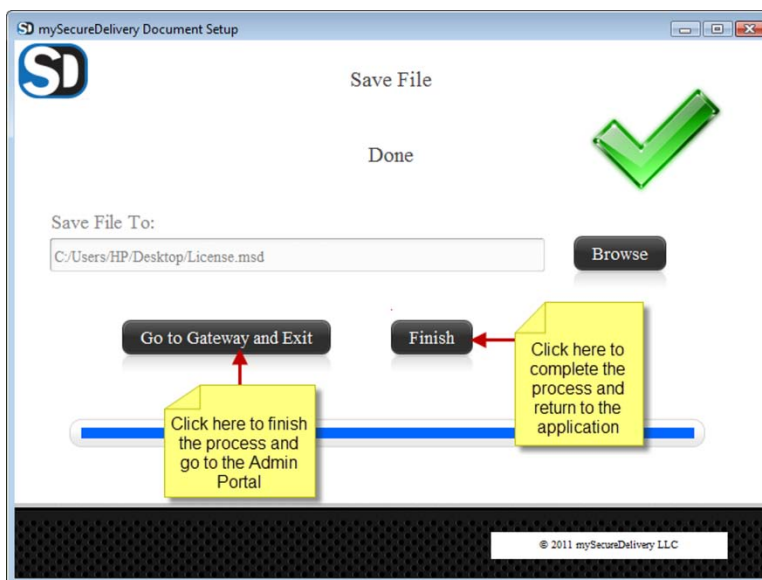
After you fill in the File Name and choose the appropriate Folder, please click the “SAVE” button. You will be taken back to the Save File screen with the Save File To field filled in with your desired location.



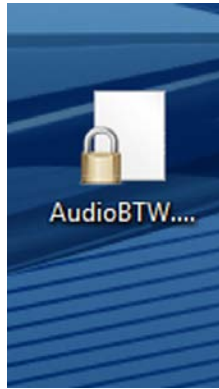
Please click the “FINISH” button to complete the Security Profile process and save the file.

You will be presented with an updated Save File screen that will display the message “Please Wait”, and then when the process is complete a green check mark will appear on the upper right hand side of the dialog box, and the “Finish” button will be replaced with two buttons: the first is the “GO TO GATEWAY AND EXIT” button, and; the second is an “EXIT” button.

If you would like to Exit and go to the mySecureDelivery Administrative Portal, you would click on the “GO TO GATEWAY AND EXIT” button. If you would just like to Exit the process, please click on the “EXIT” button.



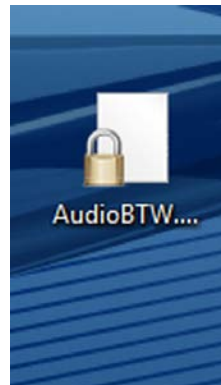
All mySD Encrypt Service .msd files are represented with the mySecureDelivery Icon. The illustration below shows the AudioBTW.msdc file as viewed on the Desktop.



Your Protected Information is now ready for you to distribute in any media form you want!

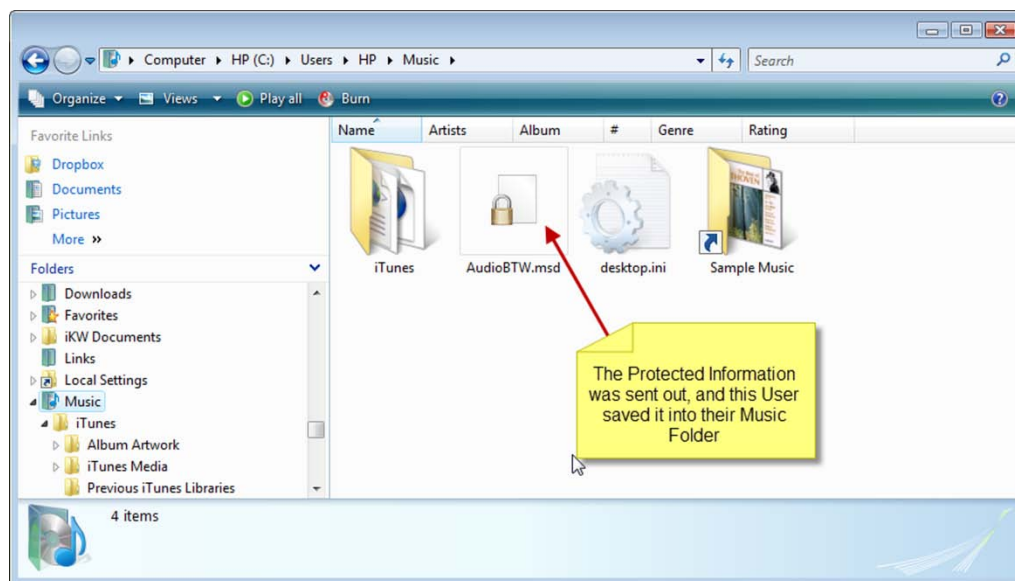
## Using the Secure Open

The mySD Secure Open is used to open any file which has been protected by the mySD Encrypt Service – as represented by the .msd file extension. The file will be displayed with an icon that contains a lock, representing Protected Information, as shown below.



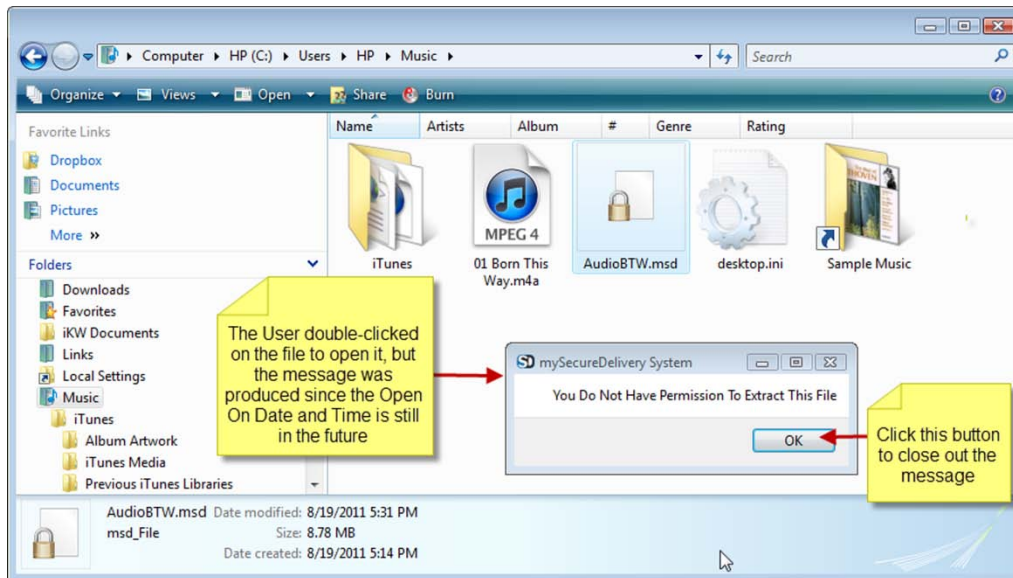
To open mySD Encrypt Protected Information, please double-click on the file. The Secure Open will: (1) validate that you are authorized; (2) decrypt the file and store it in the same folder as the mySD Encrypt file is located in; (3) store it with the same file name as it had when it was originally protected by the mySD Encrypt Service, and; (4) store it in the same file format as it was when it was originally protected by the mySD Encrypt Service.

In our example, the Protected Information was sent out and the User who received it saved it in the folder Music on their device, as shown below.



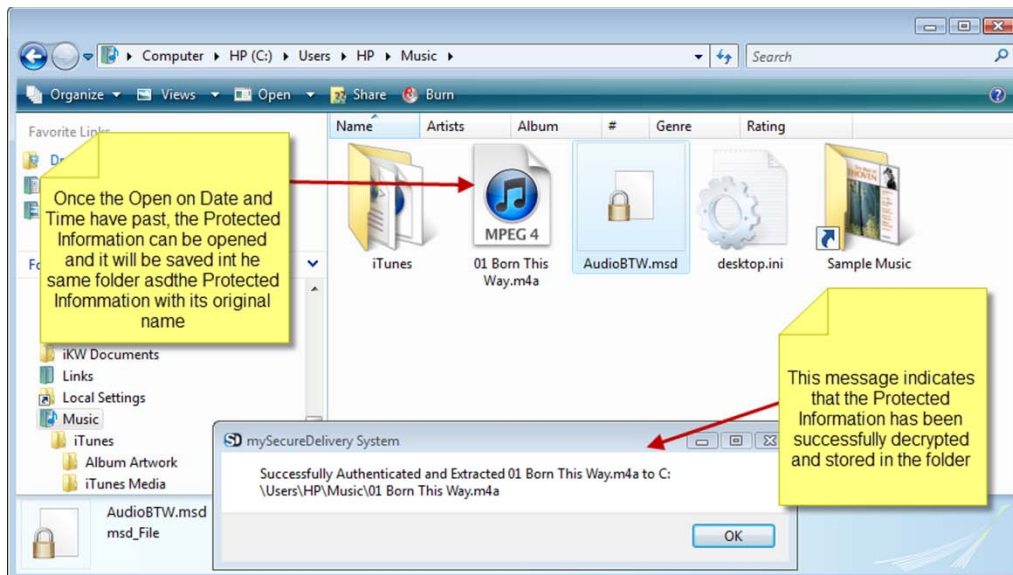
To continue with our example, we wanted all of the fans to receive this Protected Information, but anyone who tries to open it prior to August 24, 2011 would not be able to, since the Protected Information has a Security Policy that states the Open On Date is August 24, 2011 at 7:00AM, and we wanted all of the fans to open it at the same time.

If someone tries to open it prior to that date and time, the following error message will be displayed upon an attempt to open:



However, when the Open On Date has passed, the User can double-click on the file, and the mySD Secure Open will do the following:

- validate that you are authorized;
- decrypt the file and store it in the same folder as the mySD Encrypt file is located in;
- store it with the same file name as it had when it was originally protected by the mySD Encrypt Service;
- store it in the same file format as it was when it was originally protected by the mySD Encrypt Service; and
- display a message stating that the mySD Encrypt Service has successfully authenticated and extracted the file to the named folder.



As you can see in the illustration above, the Protected Information been placed in the Music folder, the same as the .msd file, and that the original name and file type is restored – “01 Born This Way.m4a”.

At this point in time, the User could double-click on the file “01 Born This Way.m4a” and, in this particular case, iTunes would open up and start playing the track.

## Summary

The purpose of this guide is to provide you with the knowledge necessary to realize the full benefits of the mySD Encrypt Service. Now that you have become acquainted with this functionality, the next steps are to start protecting your valuable information!



# **Supplemental Guide**

## **Using the mySD Encrypt Service**

