Press Release

Society of Collision Repair Specialists • P.O. Box 909, Prosser, WA 99350 • (877) 841-0660 • Fax (877) 851-0660

FOR IMMEDIATE RELEASE
For Further Information
Contact Aaron Schulenburg, SCRS Executive Director
Phone: (302) 423-3537 or e-mail: aaron@scrs.com

Protecting Your EMS Data

Prosser, *Washington*, *July 15*, *2015* — Data is powerful, and everyone wants their hands on it. We see large corporations in the headlines all too often for "data breach" issues, or for utilizing consumer data for business gain; but those stories are more relative to companies that store and have access to millions of consumer records that contain customer credit card information. Sensitivity around customer privacy and protection of consumer and business data is a growing concern across the country and around the world. While you most likely are not storing customer credit card information, you do have some key information that needs to be protected. Aside from an obligation to your consumer to protect their data, your agreements with other businesses may also contractually obligate you to protect specific data elements as well. An example of language found in a DRP agreement may state:

> *The collision repair business (hereinafter "Repairer") acknowledges it may learn or have access to confidential, proprietary, or private information (hereinafter "Information") of the insurer, the insurer's vendors, and vehicle owners. This Information specifically includes, but is not limited to, customer names, addresses, phone numbers, social security numbers, vehicle accident and repair history, vehicle images, date of loss, and vehicle identification numbers. The Repairer warrants that it will use such Information for the limited purpose of repairing vehicles. The Repairer further warrants it will keep strictly confidential any such Information that the Repairer may learn. A third party performing as a subcontractor for the Repairer to accomplish duties subject to this Agreement may be given access to pertinent Information if that third party has agreed in writing with the Repairer to use such Information solely for the purpose of repairing vehicles and otherwise to keep such Information strictly confidential. The Repairer agrees it will not sell or share nor permit its third party vendors to sell or share Information.*

During the April 2015 Society of Collision Repair Specialists' (SCRS) board meeting in Atlanta, Georgia, the organization reported on a member issue, where the repair facility faced suspension from a particular DRP due to complaints from a consumer whose loss was identified on a VIN reporting database. The reporting company responded in writing that while they couldn't release the names of their sources for vehicle loss information, neither the collision repair facility nor the Information Provider (IP) was a source of the data. This was enough to reaffirm the carrier's concerns over the repair facility's roll in releasing data, but it further reinforced the need for collision repair business owners to have protocol in place to maintain control of information and data generated by their business. Aside from the potential loss of business that can occur from leaked consumer data, there are potential

liability concerns as well, and it is imperative to know if your professional insurance policies cover any accidental sharing of sensitive data.

One of the most gaping holes that exist for data leakage is the transmission of EMS data. This data standard was originally created by the Collision Industry Electronic Commerce Association (CIECA) to facilitate the transmission of data between the body shop estimating program and body shop management system to allow repairers to choose the technology platform of their choice. Today this standard is used by nearly every information and technology provider in the collision repair space to exchange data between estimating applications and third party applications that may include claims management, rental management, parts supply programs, aggregators, audit engines and beyond. Many of these programs collect data via a “data pump” or “client” installed locally on your server or hard drive. In many cases, these are programs or vendors that you intended to collect the information in order to conduct your business. If you are bound by agreements such as the example language above, you have hopefully established the necessary written agreements regarding their scope of use and role in the process.

Unfortunately, there are other scenarios where data pumps can be loaded on your computer without your consent or knowledge. They could be potentially installed by outside sales representatives visiting your business, be a part of a software or online program that you use in your business albeit unaware of the data collection properties, or in some cases outside call centers may call in and ask your staff to request remote access to you server to correct a connection issue on a program. These examples have all happened, and while they may be legitimate in many cases, it is important to know what pumps are on your system, and that the information is only going to the sources you intend it to go to.

So how do you know what third party applications are accessing your EMS data? Unless you are very savvy when it comes to information technology and have very tight controls on your computer network(s), you probably don’t know which applications are accessing your information; and it’s not easy to tell either. Because many of these third party applications employ “sweepers” (applications that watch for the EMS file to appear in a directory and then copy it and transfer it to another application) it’s very difficult to identify when a file is being “swept” since it happens in less than a second, in the background operations, and does not leave a trace.

The only way to really determine what applications are accessing your EMS files is through deduction and smart management of your data output. You have to eliminate unknown variables by limiting data transfer to only those applications that you know you want to have access to those files. The best way to do this is to start from scratch at the source. That means reconfiguring your EMS out paths in your estimating systems. Essentially, you have to break all of your connections, and then build them back. In doing so you can create unique paths for each application that uses EMS. Then you will know exactly which applications are using EMS files, and if you need to terminate the use of an application, you can easily disable that specific directory. Those applications that are using EMS unknowingly will now be disabled since you have changed the directory that they source from. It is important to note that some data pumps could potentially have automated scans built into their code to locate EMS file directories. If this is the case, moving the directory may still not fully eliminate unwanted data collection, but serves as a good precautionary measure.

These changes not only need to be made in the source application (your estimating system), but also in the destination application (example: your shop management applications.) Below we have provided instructions from each of three estimating providers on how to change the output path at the source.

WARNING: Before proceeding, you want to make sure you contact those companies that you know should be receiving your EMS files and get instructions to modify the EMS settings in their destination application to ensure your service is not disrupted.

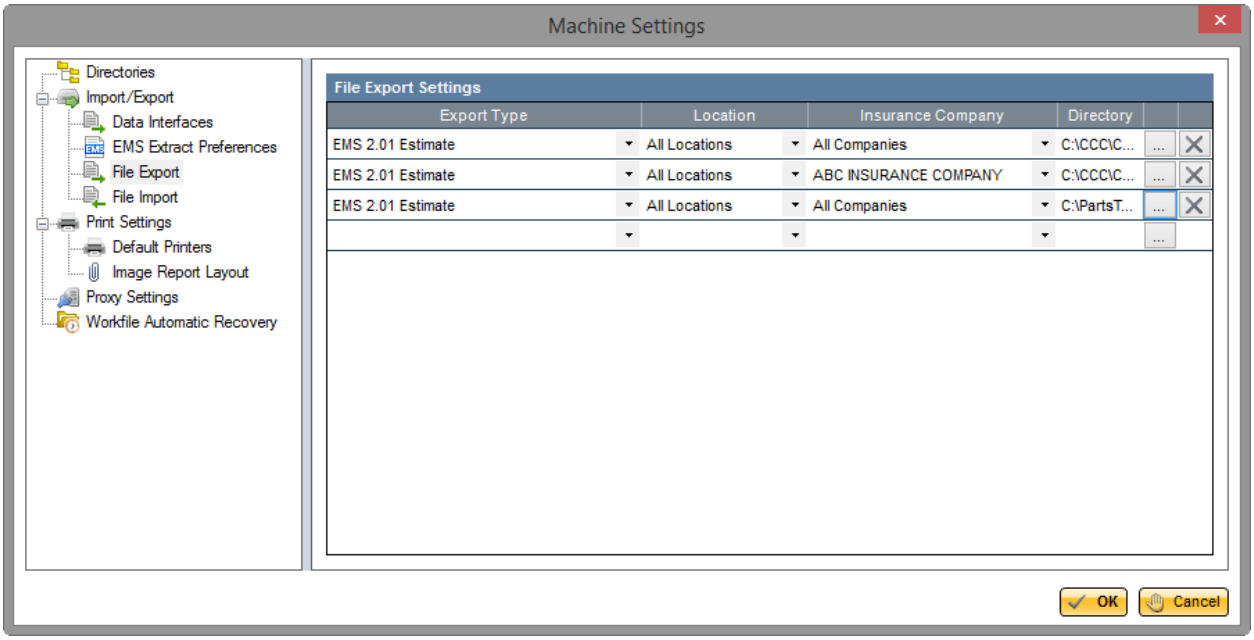
CCC Information Services – CCC ONE™ Estimating

CCC ONE not only provides the ability to specify multiple output directories, but for each of those output directories the system also provides the option to filter the output by insurance company. This way if you use an application required by an insurer you can limit the data exported to just that specific insurance company.

Configuration Steps:

Important: CCC ONE EMS configuration is specific to each computer in your network – i.e. there is no global setting. CCC recommends limiting the configuration of EMS to a few computers that are most often used. If CCC ONE is not open on the computer(s) that has EMS enabled, then EMS will not be exported. Configuring EMS on two or three active workstations (i.e. estimators) helps to ensure at least one will be open at all times and exporting files. Be sure to remove EMS export paths from computers that will no longer be used to export.

1. From CCC ONE (on each computer) select Configure > Machine Settings > File Export



2. Remove existing export directories by selecting the X on the far right.
3. Create new export directories for each application:
    a. Select the drop down in the “Export Type” column and select EMS 2.01 Estimate

b. Select the business location that is applicable to the user
c. Select a specific insurance company if applicable
d. Select the directory for the destination application. Note: in a network environment this directory should be in a shared location (i.e. file server) that the destination application has access to. We recommend creating a folder name that represents the destination application name.

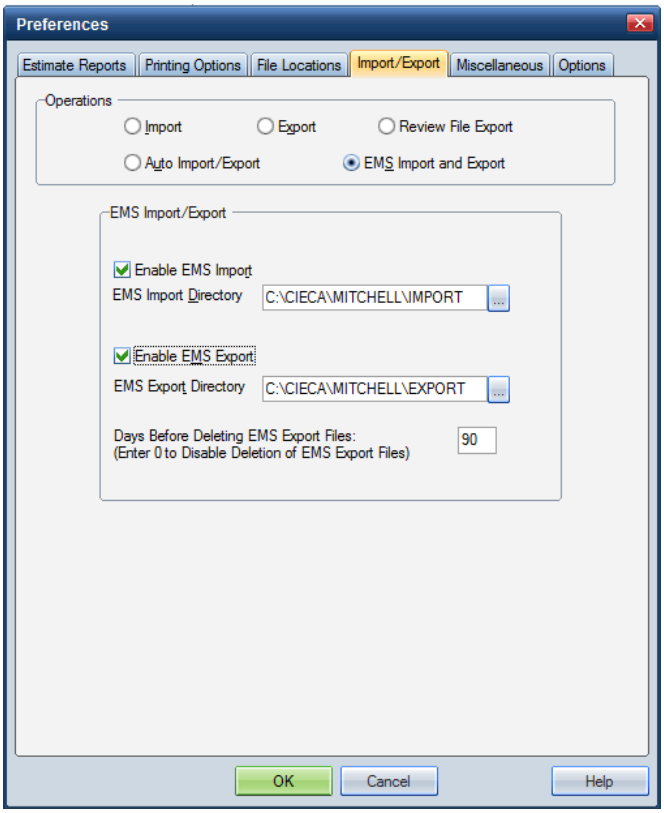
4. Click “OK” to save changes. Repeat for each applicable computer.

Mitchell – Ultramate™ Estimating

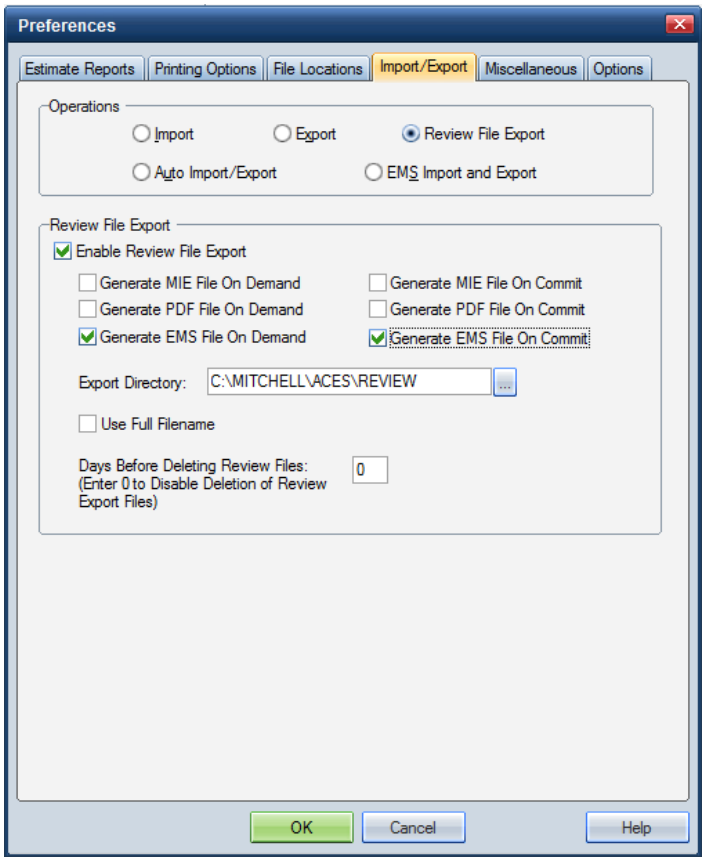
When Mitchell Estimating is installed for repair facilities (installation type = body shop), the EMS feature is automatically enabled. This is because the majority of shops that use estimating software also use shop management systems. The EMS is the common, open standard format, by which the estimate data is transferred over to the shop management system.

The default location for where these files are stored is C:\CIECA\MITCHELL\EXPORT.

The software application user has the ability to turn off/on the EMS file generation feature, as well as define where the files will be stored.



Additional EMS files (copies) can be generated and stored in separate locations by configuring the Review File Export feature. This feature is not activated by default and requires the software application user to configure the feature before use.



The default location for where these files are stored is C:\ MITCHELL\ACES\REVIEW.

Here again, the software application user has the ability to turn off/on the Review File Export feature, as well as define where the files will be stored.

Other EMS File Uses

State Farm / PartsTrader

EMS files are sent to PartsTrader for State Farm estimates only. These are only those estimates that originate from a State Farm assignment sent to the Repair Facility. These EMS files are in the EMS format but do not adhere to the CIECA standard (v2.6). They are intended for PartsTrader only and will only work for that interface. These EMS files are stored in a separate location pre-defined by the software and PartsTrader looks for EMS files only in this predefined location. The software application user does not have the ability to modify the generation or location of these files.

EMS files for PartsTrader are not automatically generated under any other condition. If a repair Facility chooses to use the PartsTrader feature for non-State Farm estimates, they must select the PartsTrader icon for the EMS files to be generated. Again, these EMS files are not CIECA standard and are stored in the predefined location as described above.

AudaExplore, a Solera company – Audatex Estimating™

Audatex Estimating users can obtain more information on how to adjust CIECA Import and Export settings by visiting our customer self-help portal at http://my.audaexplore.com. By entering the search term "CIECA" and clicking on the "CIECA Import Export" document, detailed instructions on how to adjust the settings are readily available. Users should take extra care in the adjustment of the CIECA EMS Import/Export directory settings as these can affect other systems relying on CIECA files, especially shop management systems.

Set Up an Import Path

The import feature in Audatex Estimating is used to import CIECA files from another system that handle estimates. The location of these CIECA files for import is required before setting up the import path(s).

1. Log in to Audatex Estimating.

2. Click Setup on the left side navigation.

3. Click on the Profile Name that the estimate will be imported to. Note: When setting up an importing directory under a particular profile, those estimates will import to that profile only. A unique import folder must be used to import files into a different profile.

4. Click Options on the left side navigation.

5. Click Import from under Options.

6. Click the Browse button next to the desired path and browse to the folder location of the CIECA files.

7. Select Always Import and / or Always Delete After Import when these settings are desired.

- Always Import will import the CIECA files automatically when Audatex Estimating is opened.
- Always Delete After Import will delete the CIECA files from the path after they have been imported into Audatex Estimating.

8. Click Profile List on the left side navigation to save settings.

9. Repeat Steps 3-8 for other profiles where CIECA file import features will be used.

Set Up an Export Path

1. Click Setup on the left side navigation.

2. Click on the Profile Name of the main profile that is displayed in blue letters.

3. Click Options.

4. Click Export.

5. Click the Browse... button to the right of Path 1 or Path 2.

6. Browse to the folder you would like to export the CIECA data to.

7. Click OK.

8. Select which CIECA Format will be used. Select Always Export on Close and / or Always Export on Estimate Exit when these settings are desired.

- Always Export on Close will export the CIECA data whenever the Close dialog is used.
- Always Export on Estimate Exit will export the CIECA data whenever an estimate is exited to the Work List.

9. Click Profile List on the left side navigation to save settings.

Import CIECA Files

1. Click the Import Files link on the left side navigation.

2. Select the check box(es) next to the claim(s) to be imported.

3. Click the Import button.

4. Click Ok.

5. Click Close.

Export CIECA Files

1. Select the check box(es) next to the estimate(s) to be exported on the Work List.

2. Click the Export Files link on the left side navigation.

3. Select the check

4. Click Ok.

Once the EMS export path is configured to the new directory, it is important that you contact all service providers that rely on the EMS data, in order to properly establish EMS import rules for those programs to ensure there is not a discontinuation of service. Each program may have a unique process, just as each IP has variation in their export steps.

SCRS encourages collision repair businesses to be exceptionally cautious with the data you generate as a business, and to take all necessary steps to secure and protect that information. It is important that you create and follow standard operating procedures that limit the potential for data loss or leaks.

If your business is interested in joining the largest national trade association dedicated to representing the collision repair professional, please contact our offices at info@scrs.com. For more information about SCRS, visit our website at www.scrs.com.