Staying 21 CFR Part 11-compliant with Maurice and Compass for iCE

Introduction

Maurice® lets you analyze therapeutic molecules using whole column imaged cIEF (icIEF) or CE-SDS separation quickly and easily, making it ideal for biotherapeutic characterization and release. That also means that when you're using Maurice in a GMP environment, you need to be compliant with the FDA Title 21 Code of Federal Regulations (CFR) Part 11 to ensure the authenticity and integrity of electronic data. Procedural controls, like training notification and SOPs need to be in place, as well as technical controls in the software to maintain data security. Compass for iCE, the software package Maurice uses to acquire, manage and analyze data, has all the tools required for 21 CFR compliance so you'll have no concern analyzing biotherapeutics on Maurice in a regulated environment.

In this application note, we'll hone in on the 21 CFR Part 11 tools integrated into Compass for iCE for batch execution and data processing, plus audit trails and electronic signatures. For more details on exactly how Compass for iCE supports 21 CFR Part 11 compliance check out the Compass for iCE 21 CFR Compliance Checklist.

Compass for iCE Data Workflow

Maurice lets you perform whole-column imaged capillary IEF using absorbance and native fluorescence detection; as well as CE-SDS separation using absorbance detection. Imaged cIEF generates data in pixels compared to traditional CE or HPLC methods with fixed detection windows that generate data using time-based points. Compass for iCE uses pI standards in the sample mix to convert the x-axis to pI units which can then be analyzed with Compass for iCE or exported to a third-party software like Chromeleon™ or Empower™. CE-SDS uses a fixed detection window so data is generated as time-based points and can also be analyzed with Compass for iCE or exported. The software gives you all the tools needed for compliance throughout the whole process.

Getting Started

To use Compass for iCE CFR features, you'll first need a user log in. User accounts are set up in the Compass Authorization Server by a site administrator designated by your institute that manages user accounts and assigns user privileges for each user. Administrator accounts are part of the Windows local administrators group to ensure full compliance and control the setup and system access configuration for all users. *Chapter 14: Compass Access Control and 21 CFR Part 11 Compliance* in the Maurice User Guide provides Authorization Server installation instructions, including how to use LDAP to connect the Compass Authorization Server to your own network's domain controller.

Administrators can access Groups and User Authentication and Authorization via the Compass Authorization Server homepage (**Figure 1**).

The site administrator can view existing groups and permissions by clicking Groups on the Authorization Server homepage. The admin can also click Add or Change next to Groups to change permissions in a specific group or create a new group (**Figure 2**). There are four default user levels/groups, each with different allowed privileges (**Table 1**).

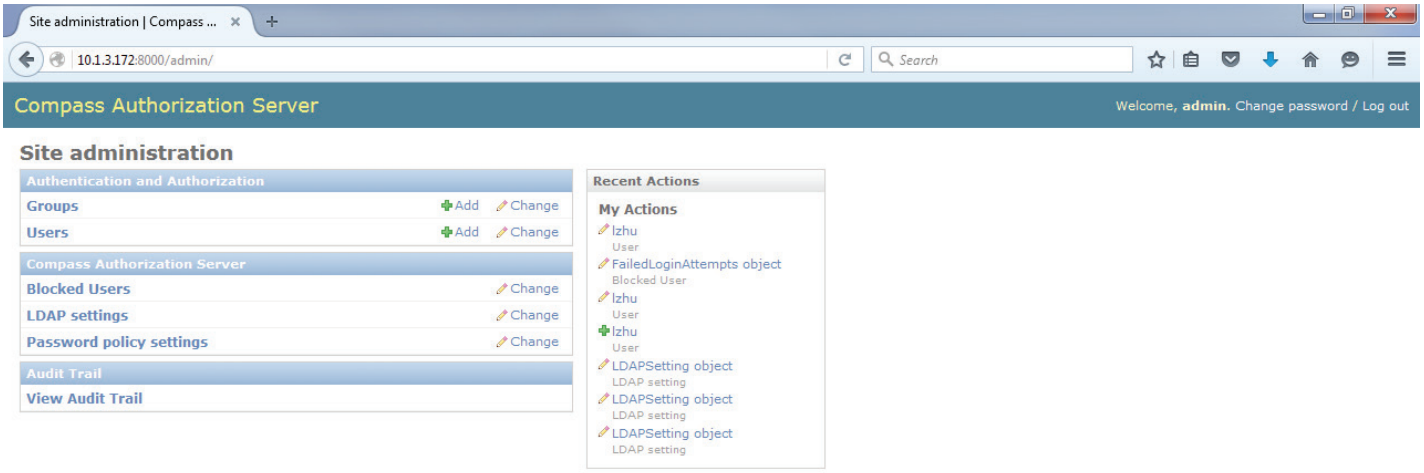


FIGURE 1. Compass Authorization Server homepage where administrators can access User and Groups Authentication and Authorization.

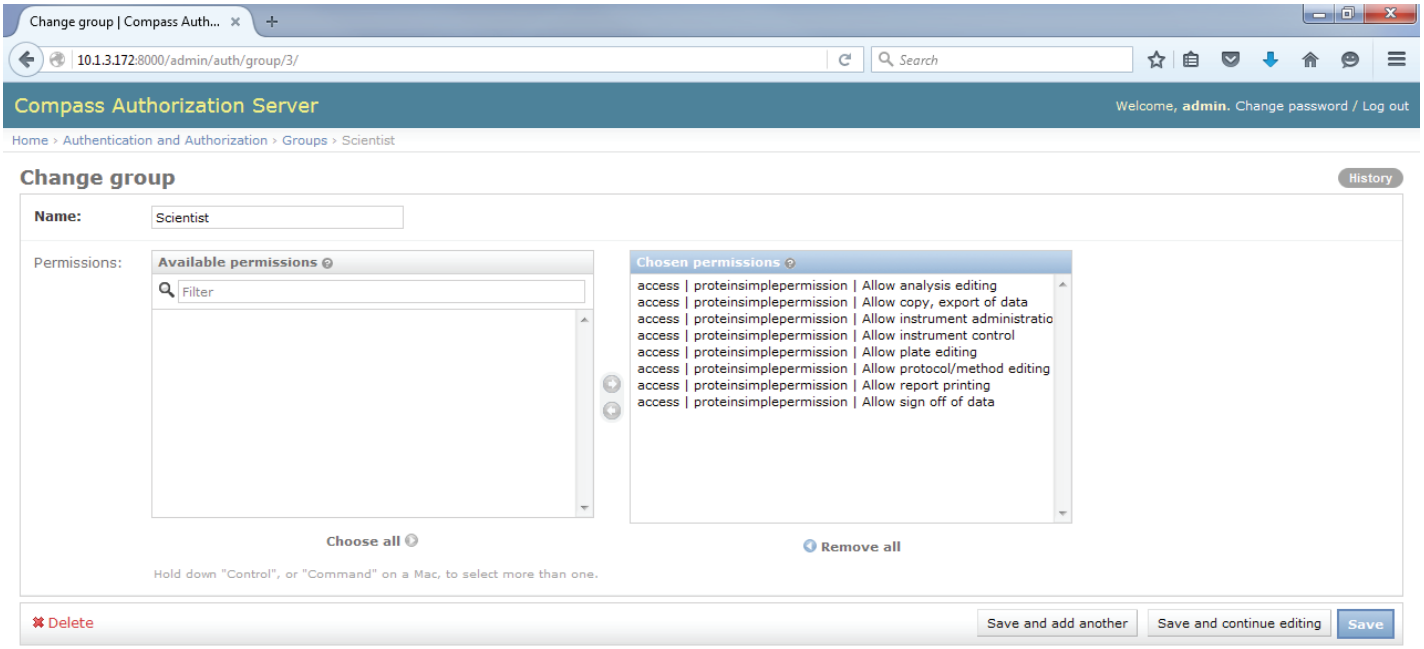


FIGURE 2. The site administrator can create new groups or modify permissions for existing groups by clicking Groups.

PRIVILEGE	ADMINISTRATOR	OPERATOR	REVIEWER	SCIENTIST
Analysis editing	X		X	X
Copy, export of data	X	X	X	X
Instrument administration	X			
Instrument control	X	X		X
Plate/injection editing	X	X		X
Protocol/method editing	X			X
Report printing	X			X
Data sign-off	X		X	

TABLE 1. Permissions and default user group privileges in Compass for iCE CFR-compliant mode.

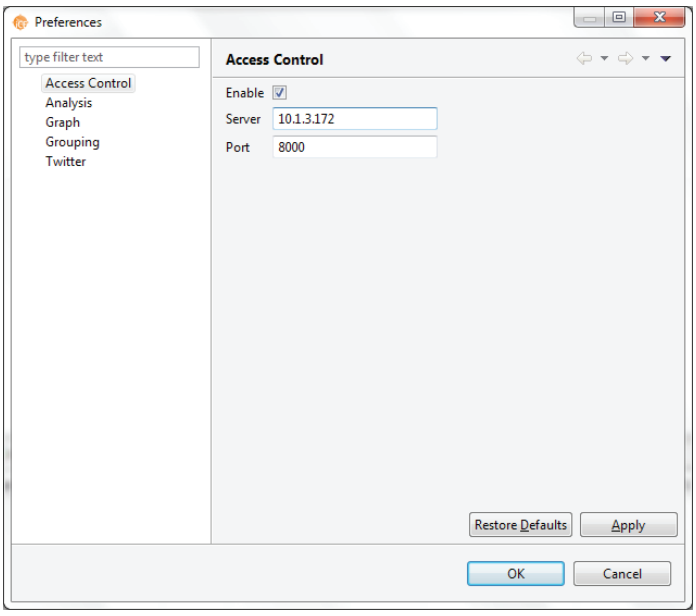


FIGURE 3. Turning Access Control on in Compass for iCE.

Clicking **Users** on the Authorization Server homepage lets the site administer view all current users. Selecting **Add** or **Change** next to Users allows the administrator to either add or change user preferences for an existing user. Users can be assigned to a group with multiple pre-defined permissions. New users will be assigned a unique Username and Password and be assigned to a specific group and/or given specific user permissions. Controls in the Compass Authorization Server ensure the uniqueness of each username, and password expiration is defined by your IT policy. Permissions not assigned to a user will be disabled. Compass for iCE needs to be relaunched if user permissions are changed on the server.

The administrator can also create other users with server permissions by giving them Superuser status in the Permissions section of their profile. For full access, the administrator will still have to be assigned to a group to have Compass for iCE permissions. All administrators will need to maintain their own admin and user account credentials. If an account is edited, for example if an admin account password is changed, ProteinSimple won't be able to give you access.

Once you have a user account, Access Control in Compass for iCE needs to be turned on (**Figure 3**). To do this, select **Preferences** in the **Edit** menu and then select **Access Control** in the left sidebar. Then, just check the **Enable** box. Access Control needs to be enabled in the software loaded on the computer you're using to run Maurice and/or analyze the data.

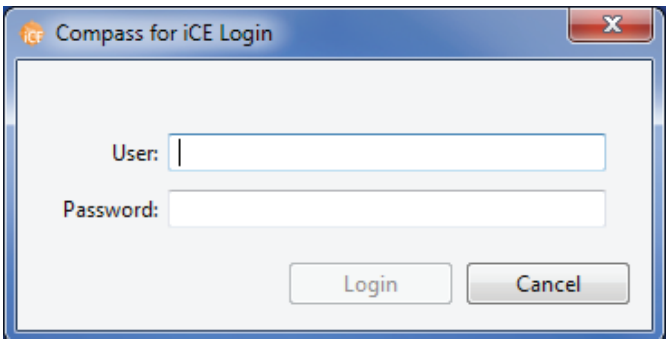


FIGURE 4. Compass for iCE login.

Running a Batch in CFR-compliant Mode

LOGGING IN

When Access Control is turned on, Compass for iCE will require you to log in with your username and password every time the software is launched (**Figure 4**). You'll get three tries before the system locks you out, but the site administrator can unlock your account if this happens. Once you've logged in, Compass for iCE will display your unique user information in the status bar at the bottom of the main window. You can lock the software to prevent access by other users whenever you need to step away at any point by clicking **Lock** in the status bar. Compass for iCE will automatically lock you out after 20 minutes of inactivity.

BATCH CONTROLS

Batches created in Compass for iCE CFR-compliant mode are saved as controlled files and can only be opened if Access Control is enabled. Any changes you make to a controlled batch, like adding injections or methods, will be tracked in the file History. Whenever you save the batch, a dialog box displays where you'll enter a mandatory comment. The file History will then display the date and time of the change, user information, action made and comment (**Figure 5**).

Maurice also lets you pause mid-run to modify the batch or open the door and add more samples. Any batch modifications made for new samples are logged in the

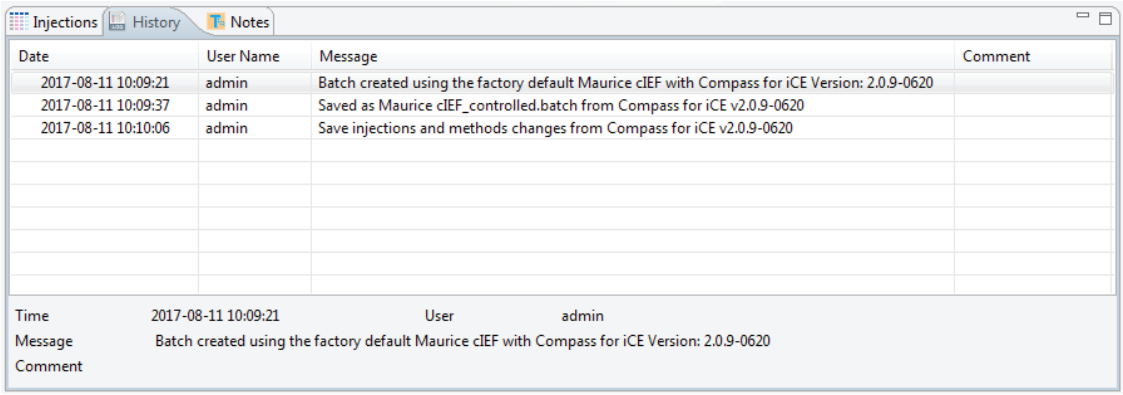


FIGURE 5. File History log of changes made to a controlled batch.

file History, and the instrument pause is logged in the file History and the Audit Trail.

Previously run controlled batches can be used again but can't be overwritten. If you want to make changes to the batch, save it under a different batch file name after you've made changes.

ELECTRONIC SIGNATURES

Files can be electronically signed to approve or acknowledge files. To sign a file, select **e-Signature** from the **File** menu and manually type in the meaning of the signature, like Approved or Verified, into the comments section of the dialog box that pops up (**Figure 6**). Then click **e-Sign** to save the signature in the file History (**Figure 7**).

All e-Signatures must include the meaning of the signature, and all include the unique user ID of the user signing the file. Signatures are time stamped automatically with the date and time.

Data Processing

Once the run is complete, no raw data processing is needed — your data is ready for analysis. All run files generated when Access Control enabled are controlled files, and any steps taken when analyzing the data are logged in the file History as well. Access Control must be enabled to analyze a controlled file. If for some reason you need to analyze the data with Access Control disabled, for example if you want to use manual peak integration, just create a separate uncontrolled file by going to the **File** menu and selecting **Export** and then **Uncontrolled**. That creates a duplicate run file will with the file name "filename_uncontrolled".

Converting and Exporting Data for Third-party Software

Data can be analyzed in Compass for iCE, but you can also export it into third-party software like ChromPerfect® (Justice Laboratory Software), Chromeleon™ (Thermo Fisher Scientific, Inc.) or Empower (Waters Corporation). You can choose your export parameters by selecting

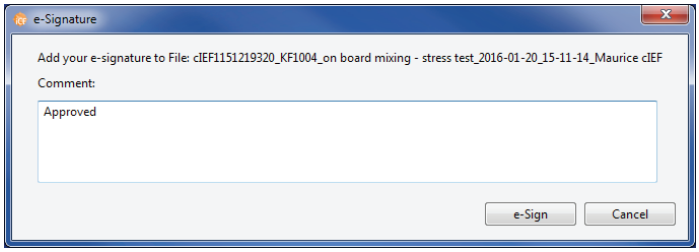


FIGURE 6. e-Signature dialog box with meaning for signature stated.

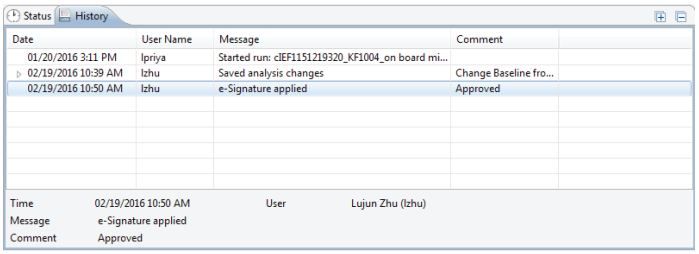


FIGURE 7. File History showing an e-Signature approving a file.

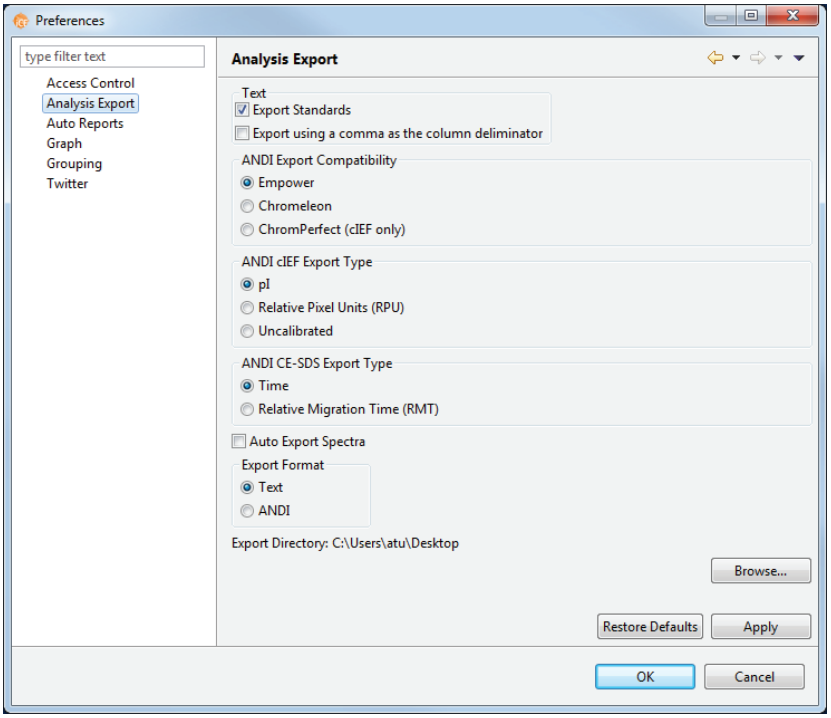


FIGURE 8. Parameters for exporting data to a third-party software.

Preferences in the **Edit** menu and then selecting **Analysis Export** (**Figure 8**) in the left sidebar. Select your preferences and then click **Apply**. You can also set things up so your run will automatically export as either a text or ANDI file at the end of the run by checking the **Auto Export Spectra** box.

To manually export spectra, select **Export Spectra** in the File menu, then choose .andi or .txt format and enter your e-signature when prompted (**Figure 9**). This export will be saved in the file History and the Audit Trail. ANDI files export the data with secure sample-specific information, but the amount of sample-specific information that gets transferred depends on the third-party software of choice. At the minimum, ANDI files will transfer the following: Injection Date/Time, System Configuration and Operator.

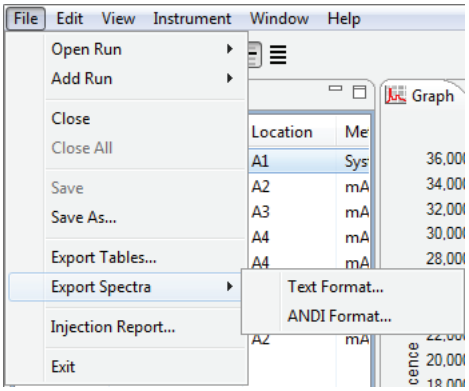


FIGURE 9. Exporting spectra in either text or ANDI format.

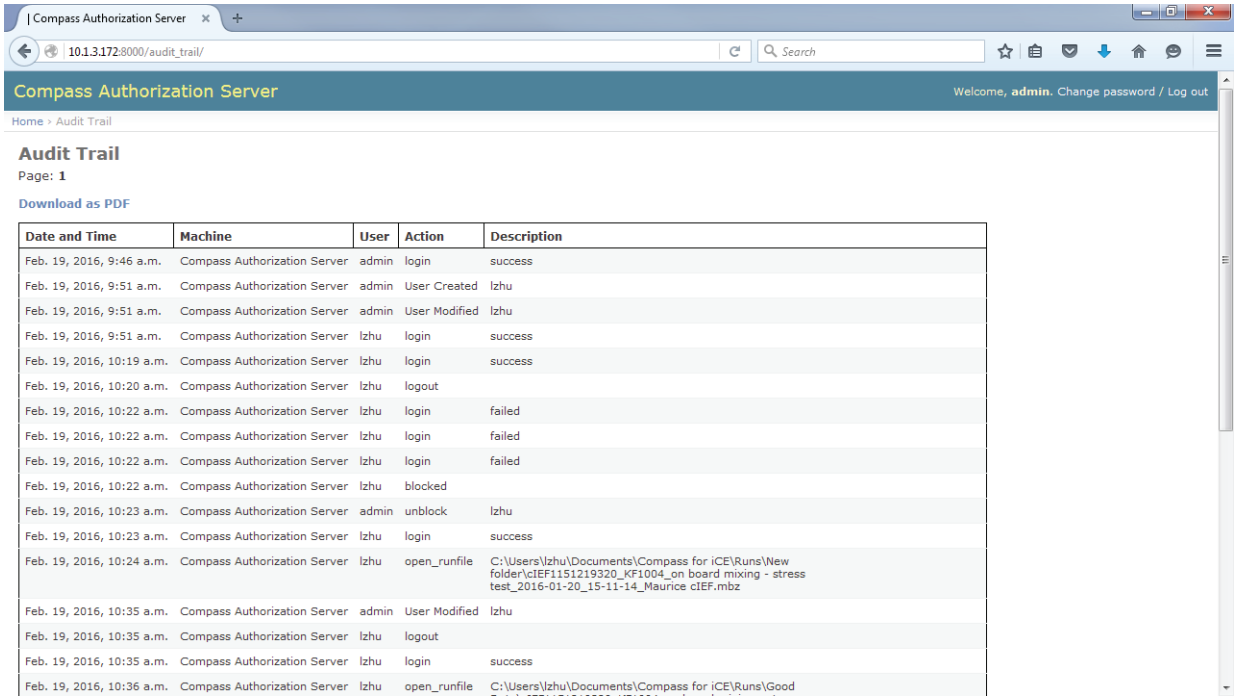
Importing ANDI files to Third-party Software

You can import the exported ANDI file into third-party software too, just follow the instructions in your selected third-party software. The ANDI file import along with the audit trail is defined by your third-party software and your institute's IT security protocol.

Audit Trail and Reports

Compass for iCE generates an audit trail for inspections and audits. Each audit trail includes these action categories:

- Instrument – Records changes to the system configuration. Examples include cartridge cleanup, pausing the instrument mid-batch and instrument upgrades.



Date and Time	Machine	User	Action	Description
Feb. 19, 2016, 9:46 a.m.	Compass Authorization Server	admin	login	success
Feb. 19, 2016, 9:51 a.m.	Compass Authorization Server	admin	User Created	lzhu
Feb. 19, 2016, 9:51 a.m.	Compass Authorization Server	admin	User Modified	lzhu
Feb. 19, 2016, 9:51 a.m.	Compass Authorization Server	lzhu	login	success
Feb. 19, 2016, 10:19 a.m.	Compass Authorization Server	lzhu	login	success
Feb. 19, 2016, 10:20 a.m.	Compass Authorization Server	lzhu	logout	
Feb. 19, 2016, 10:22 a.m.	Compass Authorization Server	lzhu	login	failed
Feb. 19, 2016, 10:22 a.m.	Compass Authorization Server	lzhu	login	failed
Feb. 19, 2016, 10:22 a.m.	Compass Authorization Server	lzhu	login	failed
Feb. 19, 2016, 10:22 a.m.	Compass Authorization Server	lzhu	blocked	
Feb. 19, 2016, 10:23 a.m.	Compass Authorization Server	admin	unblock	lzhu
Feb. 19, 2016, 10:23 a.m.	Compass Authorization Server	lzhu	login	success
Feb. 19, 2016, 10:24 a.m.	Compass Authorization Server	lzhu	open_runfile	C:\Users\lzhu\Documents\Compass for iCE\Runs\New folder\cIEF1151219320_KF1004_on board mixing - stress test_2016-01-20_15-11-14_Maurice cIEF.mbz
Feb. 19, 2016, 10:35 a.m.	Compass Authorization Server	admin	User Modified	lzhu
Feb. 19, 2016, 10:35 a.m.	Compass Authorization Server	lzhu	logout	
Feb. 19, 2016, 10:35 a.m.	Compass Authorization Server	lzhu	login	success
Feb. 19, 2016, 10:36 a.m.	Compass Authorization Server	lzhu	open_runfile	C:\Users\lzhu\Documents\Compass for iCE\Runs\Good

FIGURE 10. An audit trail generated in the Compass Authorization Server.

- File – Records creation of or changes to files. Examples include generating a batch report or exporting spectra in andi or text format.
- Security – Records changes in user administration. Examples include user created, user modified, user deleted and change password.

All the following actions will be logged into the audit trail:

- Login
- Logout
- Start run
- Stop run
- Pause run
- Continue run
- Delete run
- Cartridge cleanup
- Self test
- Open runfile
- Save runfile
- Open batchfile
- Save batchfile
- Instrument upgrade
- Change control settings
- Generate batch report
- Generate injection report
- Export spectra andi format
- Export spectra text format
- Export tables
- User created
- User modified
- User deleted
- Group created
- Group modified
- Group deleted
- Change password
- Sign off
- Edit LDAP settings
- Edit password policy
- Install
- Upgrade
- Blocked
- Unblocked

Audit trails log these actions for all users, is a secure log that can't be altered or disabled, and is date and time stamped. All users can view an audit trail by going to the Compass Authorization Server homepage and selecting **View Audit Trail** (**Figure 10**). Audit trails can then be downloaded by clicking **Download as PDF**.

Compass for iCE also generates batch, injection and instrument reports that can be viewed and downloaded in PDF format. For instructions on downloading these reports, check out the Maurice User Guide (**Table 2**).

REPORT	CIEF BATCHES	CE-SDS BATCHES
Batch Reports	Chapter 5: cIEF Batches	Chapter 6: CE-SDS Batches
Injection Reports	Chapter 9: Run Status	
Instrument Reports	Chapter 10: Controlling Maurice, Maurice C. and Maurice S.	

TABLE 2. Where to find instructions on downloading each report in the Maurice User Guide.

Archiving Raw Data

GMP regulations require data, including raw data, be kept for as long as the batch record is kept. Options for archiving records are generally user-defined based on the IT capabilities at your institute. This can include adding instructions for manually archiving data on a secure network drive in the SOP method, or creating a push code that'll automatically backup .mbz files from the local computer to a secure network folder.

Compass for iCE software uses the SHA1 hash algorithm to generate a unique hash code for all .mbz files. All files are encrypted with a digital key that, along with the hash code, ensures file integrity during secure data archiving. All current and future Compass for iCE software releases are backwards-compatible with data generated in earlier versions so secure archived data can be read and processed.

Conclusion

Compass for iCE software gives you many tools to ensure data authenticity and integrity, including but not limited to restricted access, secure computer-generated time stamped audit trails and e-signatures. The software also gives you 21 CFR Part 11-compliant data export and import into third-party software like Chromeleon and Empower. And while full compliance requires procedural controls like SOPs and training, the 21 CFR Part 11 compliant features in Compass for iCE along with rapid analysis and platform methods makes Maurice the go-to system for analyzing biologics in a regulated environment.

proteinsimple
a bio-techne brand

Toll-free: (888) 607-9692
Tel: (408) 510-5500
info@proteinsimple.com
proteinsimple.com

98-4008-00 Rev A