Documentation

Description

AuditTrail is designed to streamline CSEC audit routing by removing the need to print and route paper audits. With its standardized routing matrixes and instant email notification, it very effectively reduces routing time, eliminates lost audits, and increases visibility.

With features like the ability to add comments to each hit, add comments to the audit as a whole, simple rejection capability, and signature security, AuditTrail is the most efficient method of audit management.

The program was originally developed in MS Access 2000 in 2006 at (then AIMD Whidbey Island.) Since then it's undergone extensive updates as Access versions have changed, features have been added, and to keep current with NMCI requirements.

A new installation will run for 60 days before requiring registration. Only administrators will see the registration screen. To register, simply click the Send Registration Request button and an email will be sent with your installation ID. You will receive your registration code by return email. You'll simply copy /paste (ctrl-c/ctrl-v) your code into the box and click Apply Registration Code. This only needs to be done once and will not be affected by future upgrades. AuditTrail will cease to function after 60 days if not registered.

As of 1 August 2016, SANDIGITAL has acquired all of Bluejacket Software. As a result, an annual subscription fee will now be required before a registration key will be sent. An ITPR will likely be needed to get authorization for payment. See www.sandigital.tech/bjs for details. Bluejacket Software will continue to exist as a subsidiary of SANDIGITAL. The website www.sandigital.tech is where updates will be posted as well as this documentation. See the Support section for details.

Features

Features of AuditTrail include:

- Paperless audits (Can still be printed if needed)
- Electronic tracking
- Instant audit location
- Instant monitoring of NAMP routing deadlines
- Permanent archival and instant retrieval
- Email notifications during routing

Benefits

- No more tracking down lost audits
- Easy retrieval of previous audits to compare progress
- Verifiable signatures
- Overall reduced routing time
- Awarded “Best Practice” recognition by AMI inspectors on multiple inspections

Initial Installation

Once you've downloaded the AuditTrail package, unzip it to a location on your network share where all intended users will have access. Typically, this location is somewhere under the QA folder but it's entirely at your discretion as long as everybody that needs to use it has the permissions on that folder set to ’MODIFY’ (or Full) permissions. Please contact the IT Department for assistance with this requirement.

The installation bundle will look like this:

```
|-AuditTrail

      |-App

         |-icons.ico   <= The icon used to create shortcuts

         |-data

            |-ATFE2_be.mdb  <= This is where your data will be stored

          |-fe

            |-ATFE2.accdb  <= This is the application itself

              |-changelog.txt <= Document showing what's changed since the last update

            |-atfe2.bmp <=A custom splash screen

            |-settings.ini <=A settings file created by AuditTrail during its install routine
```

Any other files that appear in these folders are not required and can be removed. For example, in some cases Access feels the need to compact and repair a database as part of its normal housekeeping. Sometimes that process gets interrupted and so backup files don't get removed as expected.

Initial Configuration

To configure your installation initially, you'll need to double click on the ATFE2.accdb file location in the fe folder as shown above. Depending on your workstation's security settings, you may be confronted with various warning dialogs. Please confirm that you wish to open/run any file that AuditTrail shows you.

Note: *If at any time you need to re-run this configuration setup, simply RENAME the **settings.ini** file located in the fe directory. The next time AuditTrail is started from the network share, it will see that the settings file is not there and assume a new installation is required. No data loss will occur if you follow this procedure.*

The database will orient itself and become aware that this is the initial install and ask you for configuration information:

1) What is the name of this command (i.e. FRC North West)?

1. **1.** This locale information will appear on any printed audits and will also be added to any bug reports that get sent to the developers. This will be important as the team will likely need more information to correctly fix the bug. Please enter anything valid but not classified.

2) Will this be installed on local user's machines?

1. **1.** In some cases, there are policies in place that can prevent users from installing this program on their local machines. This is also a common occurrence for commands underway. If you are aware that your installation is constrained by this policy then please answer No to this question. If you are not sure, you can answer Yes (or accept the default) and if you find this problem later, you can easily change it in the settings.ini file described in the settings.ini section in appendix b.

3) Local installation location?

1. **1.** Accepting the default location is typically the proper thing to do. If you find that you get Access Denied errors when installing then the default location is not writable (likely from policy as described in question 2). In that case you'll have to modify the settings.ini file to point to a path that IS writable and reinstall.
2. This location informs AuditTrail where to look for its files on your local hard drive. If it finds that it was NOT started from that location it will attempt to install to that location. This is the mechanism used when installing from the server. AuditTrail is aware of the directory it started from and a simple comparison to this path lets AuditTrail know to install or start up.

4) What email address do you want misrouted email notifications sent to?

1. **1.** If someone in the chain of command receives notice that they have audits to work on but they are not the correct person, the email address entered here will show up on the bottom of the **email notification** so they will know who to forward the email to for correction. Typically, this email address would be the QAS or QA LPO or perhaps the QA Secretary. It's typically meant for the person that routes audits most of the time. Again, if it's wrong here, it can later be changed by modifying the **settings.ini** file as described in appendix b.

5) Enter the NMCI user name for the person responsible for administration of AuditTrail.

1. **1.** This person will have **full rights** to access any part of the system including **user management**, etc. This should be restricted to the QAS, QA LPO etc.
2. **2.** AuditTrail recognizes who is logged into the machine by examining the CAC card. Therefore, this needs to be in the format firstname.lastname as that's how your card shows it. Said differently, it should be the first part of your email address just before the @ symbol.

6) Do you wish to (re)install AuditTrail on your workstation?

1. **1.** If you selected NO for question 2, you won't see this dialog. You are now able to install the system on your local machine and begin using AuditTrail.

Updating an existing installation

Updating to the latest version of AuditTrail is a matter of only a few steps.

1) Ensure all users are logged out and disable the database. See the Administrative Overview section for details.

2) Make a backup copy of your AuditTrail folder and all of its contents as shown above.

   1. Note, after the initial installation was completed, there will be at least two new files in the fe folder. Please ensure ALL files get backed up in case something goes wrong.
      a. settings.ini – contains your site specific configuration
      b. mortem.dmp – contains data used for bug reports but can safely be deleted

3) Take the new ATFE2.accdb and the changelog.txt files and overwrite the ones in the fe folder.

4) Start AuditTrail the way you normally would and the upgrades will be performed automatically.

5) Re-enable the database for all users – See the Administrative Overview section for details.

In some cases, a manual installation may be required. It is possible that the automated installer will fail due to Group Policy or other changes. In this case, you will receive an error code 5 in your crash report.

The install and update routine uses the same code so you may have to do a manual update as well.

The installer and updater routines simply create an AuditTrail folder (spelling is very important) and copies files down from the AuditTrail/app/fe folder from your share drive and then creates a shortcut on your desktop. In many cases, there will be more files in the fe folder than are needed to run AuditTrail. They can be safely deleted as they are always cruft left over from MS Access. The four files that are crucial for operation are ATFE2.accdb, ATFE2.bmp, changelog.txt and settings.ini. So essentially, if you find yourself in a position where a manual install is required you can go through the following 6 steps to get a working copy on your machine:

1) Create a folder in the %appdata% folder called AuditTrail (Spelling is very important)

2) Browse to the AuditTrail/App/fe folder on the share drive

3) Copy ATFE2.accdb (access database), atfe2.bmp, changeling.txt, and settings.ini

4) Paste them into the newly created AuditTrail folder on the C: drive

5) Double click the ATFE2.accdb file to start AuditTrail. It will automatically create a shortcut on your desktop for future use.

6) Start AuditTrail from the desktop shortcut

Administrative overview

During the initial installation, the system asked for the NMCI user name of the person chiefly responsible for administration of the database. This person will have full access to the database.

The admin user will be able to perform the following functions:

1) Import audits

2) Manage all routing matrices

   1. Add
   2. Delete
   3. Modify
   4. Modify routing stops

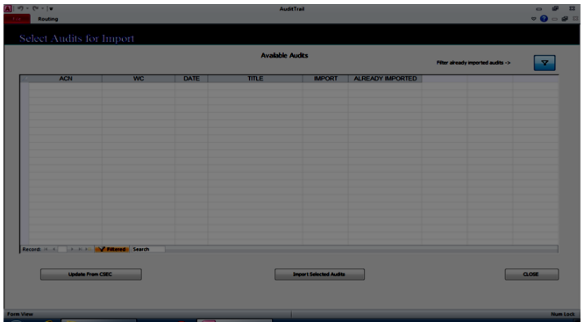
3) User rights management

4) Options selections

5) Edit an audit in route

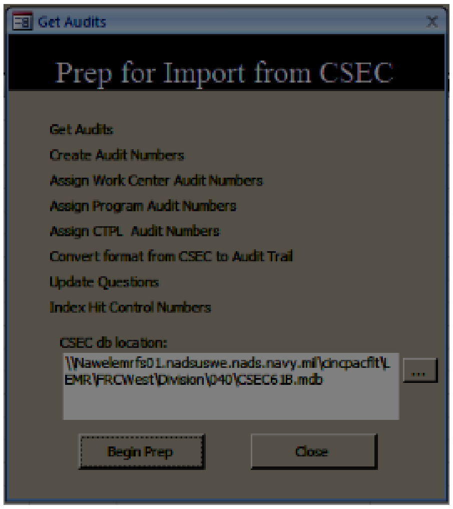
Importing Audits

To start the import of audits, click on Tools | Import Audits (you'll find the Tools menu under the Add-Ins ribbon)



The columns shown above are ACN = Audit Control Number. Each audit gets a number similar to a JCN. WC is the primary work center involved in the audit. Date and Title are self-explanatory. In some cases you might want to route an audit from CSEC while there are audits not quite finished. With the IMPORT check box, you can determine which audits you want to import and route. The ALREADY IMPORTED column is for housekeeping. If you toggle the filter shown by the funnel, then you'll see which audits have already been imported from CSEC. This is used as a filter to prevent importing the audit twice.

From here, you'll connect to CSEC by clicking on the Update from CSEC button.   You'll be presented with the following dialog:



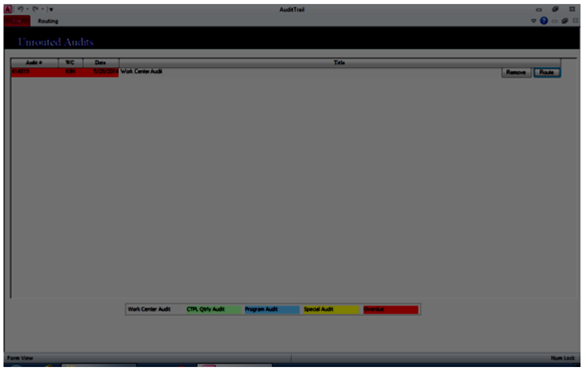
Prep for Import from CSEC

Get Audits
Create Audit Numbers
Assign Work Center Audit Numbers
Assign Program Audit Numbers
Assign CTPL Audit Numbers
Convert format from CSEC to Audit Trail
Update Questions
Index Hit Control Numbers

CSEC db location: \\Nawelemrfs01.nadsuswe.nads.navy.mil\cincpacflt\LEMR\FRCWest\Division\040\CSEC61B.mdb

This dialog will allow you to connect to CSEC and prepare the audits for import. The CSEC db location window shows the last CSEC that was used. Click the ellipsis button to select a new location.

After connecting to CSEC, you will be brought back to the Select Audits for Import screen, this time showing the new audits that were found in the CSEC database. Place check marks in the IMPORT column for all the audits you want to import and route. Click the Import button and the audits will be imported and placed in an UNROUTED bin. To get there, click the CLOSE button and you will be brought to the UNROUTED screen seen here:



Unrouted Audits

Audit #	WC	Date	Title
414019	60H	5/28/2014	Work Center Audit

Work Center Audit | CTPL Qtrly Audit | Program Audit | Special Audit | Overdue

 Above, you will see similar information you've already seen. Two exceptions, though, include the Remove button and the Route button. The Remove button will simply dump the audit out of AuditTrail. The Route button will begin routing the audit as needed.

Routing Audits

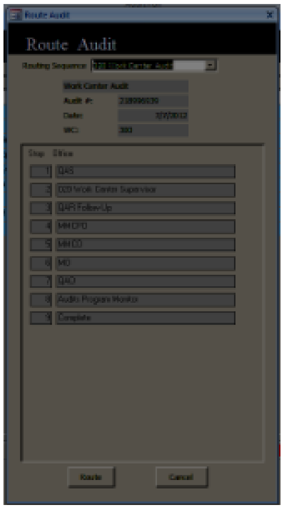
Audits are routed in one of two general ways – Standard Routing, and Flex Routing. AuditTrail knows which format to use based on the data imported from CSEC.

Standard Routing

Work center audit routing (and in some cases a simple program audit routing) is assumed to be vertical - from the work center up through the chain of command as needed.

Work center audits and the following program areas will give you that routing screen:

500, 800, 1000, 1500, 1600, 2800, 2900, 3100, 3400, 3900, 4000, 4600, 4900, 5200, 5300, 5400, 5700, 5900



Route Audit

Routing Sequence: [illegible] Work Center Audit

Work Center Audit

Audit #: [illegible]

Date: [illegible]

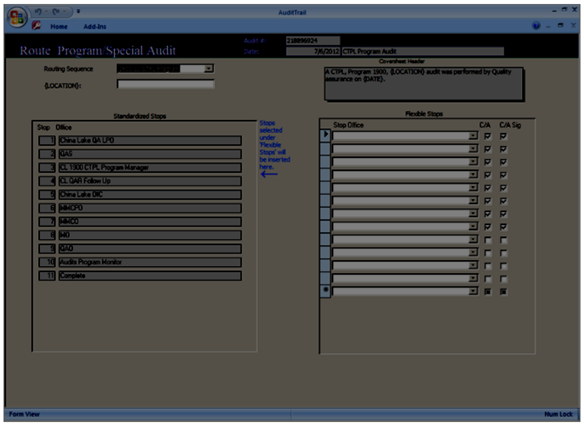
WC: [illegible]

Stop	Office
1	QAS
2	020 Work Center Supervisor
3	QAR Follow-Up
4	MM CPO
5	MM CO
6	MO
7	QAO
8	Audits Program Monitor
9	Complete

In the Route Audit dialog, you can select the appropriate routing matrix and click the Route button. AuditTrail will generate notification emails and place the audit in the first stop (In the above matrix, the notification will go to the QAS and the audit will arrive in his in-box in the main screen.)

Flex-Routing

The other method of routing is for program audits and audits that may impact multiple work centers. Programs such as CTPL (Area 1900) often hit several work centers in a single audit but often the work centers involved will vary between audits. Therefore, the initial part of the routing would be the same (i.e. QA stops) followed by the dynamic routing stops. Since creating a routing matrix for each possible combination of program areas and work centers is infeasible, Flex-Routing was created.



Route Program/Special Audit

Audit #: 218896924

Date: 7/6/2012 CTPL Program Audit

Routing Sequence: [illegible]

{LOCATION}:

Coversheet Header

A CTPL, Program 1900, {LOCATION} audit was performed by Quality assurance on {DATE}.

Standardized Stops

Stop	Office
1	China Lake QA LPO
2	QAS
3	CL 1900 CTPL Program Manager
4	CL QAR Follow Up
5	China Lake OIC
6	MMCPO
7	MMCO
8	MO
9	QAO
10	Audits Program Monitor
11	Complete

Stops selected under 'Flexible Stops' will be inserted here. ←

Flexible Stops

Stop Office	C/A	C/A Sig
	☑	☑
	☑	☑
	☑	☑
	☑	☑
	☑	☑
	☑	☑
	☑	☑
	☑	☑
	□	□
	□	□
	□	□
	□	□
	■	■

As you can see in the above screen shot, this audit triggered a Flex Route routing matrix. **If you don't see this routing screen, check that the "Use vertical routing for program audits" box is unchecked in the Options dialog on the General tab.**

Starting from the top, the Routing Sequence selector allows you to choose the appropriate matrix. The {Location} block allows you to type a location where the audit was performed (i.e. 600 Division) that will be inserted into the coversheet header. To the right of that is the Coversheet Header. It's entirely optional but is there to provide detail.

In this case "A CTPL, Program 1900, {LOCATION} audit was performed by Quality assurance on {DATE}. The two tokens, {LOCATION} and {DATE} will be replaced by what is typed into the {LOCATION} block to its left and the date of the audit respectively.

Next is the left column. This is the standardized routing matrix that was selected. The blue arrow in the middle indicates where stops will be inserted if they are entered on the right column labeled "Flexible Stops".

The first 3 stops are intended to be the same for every audit using this matrix (in this case CTPL) so that any audit routed with this matrix will always follow the first three steps but then move to the customized work centers as needed. The custom stops are entered on the right side of the screen and will be inserted automatically between stops 3 and 4 (where the blue arrow points).

For example, if the audit was for 600 division and work centers 610 and 69b were the two work centers involved then the custom stops would read 610 WCS followed by 69b WCS followed by 600 Division LPO, 600 Division LCPO, 600 Division Officer etc.

Special note, all of the stops listed in the matrix on the left starting at stop 4 will be added to the end of the matrix. Think of the stops on the right as being 'wedged' into the selected matrix between stops 3 and 4.

The right column, again the Flexible Stops column, is entirely optional but is there to allow stops to be inserted into the routing matrix for the given audit. The Stop Office column shows all available stops in the system. **The C/A column indicates whether the given stop should have the ability to modify the Corrective Action block**. In some cases, the work center supervisor would need CA whereas a branch LPO would not. **The C/A Sig block indicates whether that stop's signature appears as the Corrective Action Signature on printed audits.**

Special note, the Sig block is meant to determine which stop will have their signature selected on the coversheet has the final corrective action signature. Typically this would be the program manager. Selecting more than one Sig stop will cause the audit to look like it has several Corrective Action signatures when printed.

Once the matrix is created the way you'd like, click the Route button on the toolbar (under the Add-Ins ribbon.) AuditTrail will automatically renumber the stops so that the Flexible Stops get inserted in the proper order and every stop from stop four gets moved down below the flexible stops.

Un-routing Audits (Removing an audit from AuditTrail)

In some cases it might be desirable to un-route an audit, either because a mistake was discovered in the initial audit, or perhaps an audit was routed using the wrong matrix. To accomplish this, simply open the audit and reject it back to the first stop in the matrix. If it's already at the first stop a warning dialog will appear informing you that this will un-route the audit and ask you if that's what you intended. If it wasn't at the first stop already, simply open the audit again (from the first stop in-box) and reject it again.

After the audit it rejected and un-routed, it will then reside in the un-routed bin located in the UNROUTED screen. You can get to it by selecting Go | Un-routed from the In-boxes (Add-Ins ribbon). Here you have the choice of re-routing it or clicking Remove to purge it from AuditTrail altogether.

Matrix Management

The core feature of AuditTrail is allowing audits to be routed electronically. In order to do that, the system requires routing matrixes that describe which stops, and in which order each audit should use. A routing matrix models that behavior with individual stops.

To create a matrix, click on Tools | Matrix Management | Add Matrix. An Add Routing Matrix dialog will appear. Provide a name (Such as “040 Quarterly Tech Pub Audit”) a Routing Title (“QA Audit Routing Sheet”) and a header (“Work Center {WORKCENTER}{QUARTER} Tech Pub audit was performed …..”)

Please note the paragraph on that dialog box that describes how special tokens can be placed in the header and what they do.

Creating a matrix from scratch can be difficult. Instead, it's recommended that you either modify an existing matrix or copy one and change the title etc. Those dialogs are self-explanatory. Should you need help, please contact technical support.

Caution: *Modifying or deleting a **matrix** while audits are in route with that **matrix** will **not** cause harm. Deleting **stop**s, on the other hand will cause the audit to disappear when it reaches that **stop**. Aud its with invalid routing matrices can be found by going to the options screen below. They will also appear in a LOST AUDITS inbox on the main screen.*

Stops are individual offices where an audit will require a signature. Take care when modifying stops. **Do NOT delete them**. If you need to take one out of service, simply change the email address to @navy.mil and that will terminate any audit notifications.

The LEVEL indicates where that in-box should appear in the tree at the in-box screen. It serves no other purpose than to keep the in-boxes organized.

Please freely run the Empty Email report and to make sure there are no mistakes by clicking the buttons below the list.

User Management

User permissions should be given with care. Most users will not require any permissions at all since AuditTrail ships with a standard set of permissions. An explanation of the columns is below:

User Name: The NMCI username as logged into the system.

Options: Allows the user into the Options dialog. Only intended for administrators

Import: Allows the user to import from CSEC. Be careful to only allow access to those that need it

Matrix Manager: Allows the user to modify matrices.

Developer: Only the developers should use this.

Editor: USE WITH CAUTION. Allows the user to edit the entire audit including discrepancies. In most cases this should never be used but in the rare case that the normal audit work flow won't allow the needed changes, this provides a way. Be very careful as this bypasses all routing constraints and can be used to change any part of an audit at any time.

Developer Nag: Deprecated

Email Nag: A flag to prevent email warnings from occurring.

Options

There are a number of options that can affect how AuditTrail functions. Use caution when assigning users the Options permission as this can have a substantial negative impact on work flow.

On the General tab:

Enforce Signature Security (Default – Checked) – When signing an audit AuditTrail will compare the last portion of the signature against the CAC card logged into the machine. For example, if your NMCI user name is russel.t.bucket you can sign the audit as AT1(AW)Russel Bucket because the last chunk of your signature will match the last name on the CAC card. The signature entered will be what appears on the printed audit so it's preferable to use a formal signature. If this option is off, then no signature checking will be performed at all. This is not recommended as this opens an opportunity for forgery and can compromise data integrity.

Punt rejected audits to rejecter vice chain of command (Default unchecked) – When an audit gets rejected down the chain several steps, it might be desirable to allow the intermediate steps see the audit again as it transits back up the chain. Be aware that this will cause delays in getting the audit fully routed. In some cases it might be desirable to simply push the audit back to the rejecter instead, bypassing the intermediate steps. This is a global setting and not audit specific.

Use vertical routing for program audits (Default checked) – Many program audits will use a **Flex Route matrix** that will allow for a custom routing **matrix** for a given audit. Checking this box will override this feature and only allow "**Vertical**" routing.

Database Down for Maintenance – This will gracefully **force all users to log out** of the system. Use this when database upgrades are needed etc. This will also prevent users from being able to log in. See ERT below...

ERT: Estimated Return Time. If a time is entered here, when the database is taken off line a screen will alert the user at what time to expect the system to be available again.

Enable hit comments (Default checked) – This will enable comments on a per-hit basis.

Currently Logged In Users – This will show you who is currently logged in. In some cases the list will get out of sync with who's actually logged in. If a user logs out properly then the system will remove their name. If you see users logged in with an old LOGIN TIME it might be the case that the user is having trouble with their machine. A visit to that computer might reveal issues that the IT department may need to be aware of.

On the Email Options tab:

Send automated emails (Default checked) – When AuditTrail needs to send an **email notification** about audits it will first check this to see if it's authorized to do so. If unchecked, no emails will be sent.

Pop up email send window (Default checked) – AuditTrail generates a standardized **email notification** and send it to the next user in the **matrix**. If this box is checked, the email window will open allowing the current user to customize the email message as desired. If unchecked, an email will be sent silently. In both cases, Outlook will need to be open. If it's not, AuditTrail will ask the user to open it.

Email crash reports to the developers (Default checked) – If AuditTrail malfunctions it can 'phone home' to inform the developers. No sensitive data will be sent and if the Pop up (see above) is checked, it will allow you to verify what it's sending. It is HIGHLY recommended that this box remain checked.

On the Misc. tab:

List audits with invalid routing sequences – This function will scrub audits that are in route that have invalid routing matrices. Typically this should never happen. One possible reason this could happen is if a **stop** is deleted from the system before an audit has hit that point in its **matrix**. This should be checked on occasion just to be sure nothing has gone awry. It's also important to let the developers know this happened so that the reason can be resolved and the audit can be recovered. This is also the first place to look if an audit has gone 'missing in action'. As of version 10.1.4 this feature is now duplicated in a LOST AUIDTS inbox.

Login History Report – Useful to audit who's logging in to the system.

Purge Old Data – This will remove audits older than 24 months along with their associated data. This is needed to keep the data file down to a manageable size. If performance begins to degrade it's a good idea to print out archives and purge old data.

Send Debug Info – Creates a simulated malfunction and generates an email to the developers. This is only useful for testing communication capability with the support team.

Compact data file on next shutdown – This will attempt to automatically compact the backend after the last user logs out. If performance begins to degrade it's a good idea to do this.

Import Det Data – Allows a parent command to import data from dets or subordinate commands. Note: to avoid ACN duplication, the letters DET will be prepended to the ACN.

On the Non-Working Days tab:

This is a list of dates that should be excluded from the 10 day mandatory routing time frame as stated in the NAMP. Weekends are automatically excluded but holidays and special lib days are not.

Normal work flow

Overview

The normal work flow begins with an email notification indicating there is an audit awaiting work. The audit can be found in the In-boxes screen (the main screen as seen when first opening AuditTrail). From there, clicking the Go button for that audit will open the audit for review and corrective action as needed.

As of version 10.1.5 there are two new features of the inbox: A Stall column and a color switch. The Stall column indicates how many days an audit has been at its current stop and the color (or Gray) button allows the user to toggle color coding on or off for performance reasons.

Each hit in the audit can be viewed by clicking the forward/back buttons on the toolbar (in the Add-Ins ribbon) and if the current stop is listed as having Corrective Action authority, corrective action information can be entered/modified. If Corrective Action authority is not given for the current stop, the block is locked and cannot be modified to prevent unauthorized changes. When all hits on an audit have been corrected it can then be forwarded to the next stop in the matrix by clicking the Sign button and filling out the blocks in the signature dialog. Likewise, if the audit needs to be rejected to a previous stop, the same can be done by clicking the Reject button. The toolbar buttons are described below:

Audit Actions

Open Archives – Opens the archived audits attempting to locate the previous matching audit to allow for comparison with the current audit.

Show Audit – Opens the current audit in a print-preview mode.

– Opens a traditional **cover sheet** where audit wide comments will be shown along with signatures, dates, names etc. These comments should not be confused with hit comments described below.

Add Comment – This comment button will add comments to the *current hit,* not to be confused with **cover sheet** comments above.

QA Follow Through – This will schedule a follow up date for QA to re-examine the discrepancy. This will allow the audit to be signed and continue through its routing **matrix** in a timely fashion. An example of this would be something like a pub discrepancy where a new pub is on order and will be some time before it's received thus not allowing the hit to be completely corrected in a timely manner. Delaying the audit for this would likely exceed the time allotted by the NAMP to complete the routing matrix. This feature will allow outstanding hits to remain visible by QA without delaying the audit.

First-Previous-Next-Last – Moves to the corresponding hit in the given audit.

Sign- This will open the signature dialog allowing the appropriate member to sign the audit and forward it up the **matrix**. If the **admin**istrator has left the **Enforce Signature Security** option checked in the options then only the person logged in to the computer to sign the audit. This has the added benefit that if the last NMCI name matches the last word in the signature then AuditTrail will accept the signature. This allows the signer to use a proper signature but still be verifiable against the CAC card. For example, the NMCI user russel.t.bucket could sign an audit as AT1(AW)Russel Bucket because Bucket would match (case insensitive) the last part of the NMCI user name. The signature that is typed in this block will be what is printed on the audit so most commands prefer this feature.

Done- Will close the audit and return to the **Inboxes** screen.

QA Work flow

Scheduled QA Follow-Throughs

To prevent an audit from being delayed in transit, the stop that has the corrective action authority can schedule a QA Follow-Through for a later date and thus allowing the audit to continue through the routing matrix. The example given above is that a pub discrepancy may require ordering a new pub and thus the hit cannot be fully corrected until the pub arrives. The scheduled follow-through feature will allow QA to keep visibility on outstanding corrective actions and monitor completion.

The scheduled follow-throughs can be found on the In-boxes screen at the bottom of the tree. Just like creating a signature on an audit hit, the follow-through can be signed off or rescheduled if needed.

Archives

The archives of completed audits can be found on the In-boxes page at the bottom of the tree. These archives serve as a permanent record of past audits (or those that haven't been purged.) While the data cannot be changed, the audit can be opened and printed for comparison or historical analysis.

The button labeled Run Trend Analysis Report will generate a historical report based on selected work centers or program areas. The data can be printed or exported to Excel for further analysis.

Reports

There are several reports on the Reports menu (under the Add-Ins ribbon):

Single Audit- Prints a single audit by its ACN

Cover Sheet – Prints the audit's coversheet by ACN

– Prints a routing **matrix** or all matrices. Useful for auditing etc.

Routed Audits - Prints a list of audits currently in route. Useful to make sure nothing has gone missing etc.

Most Recent Audit Hits By Division – A simple comparison of hit count per division

(365 Day) Hit Count by NAMP Program Area – A count of hits in the last year by **CSEC** Area. Useful to quickly identify areas that need special attention.

– A count of hits in the last year by **CSEC** question. Useful to quickly identify hits that need special attention.

Appendix A: Support

While AuditTrail has been designed to be self-documenting and requiring little in the form of training and support, help is available by contacting:

Email – support@sandigital.tech

Phone – 480 427 0391

Web – www.sandigital.tech

New releases will be announced on the site and available for download and update with necessary instructions.

AuditTrail was originally authored by me, AT1(AW)Scott Reeves (Ret.) at Fleet Readiness Center Northwest with the help of Quality Assurance Secretary Judy Hutchings and the QA Officer CWO5 Benjamin. Bluejacket Software was created to continue management long after I left FRCNW.

Appendix B: settings.ini and mortem.dmp

When AuditTrail is initially configured it creates a settings.ini file in the fe folder. These settings affect how AuditTrail behaves and can be changed to manually override its configuration. Additionally, if the answers to the initial installation routine need to change, one can either delete the settings.ini or modify it as needed.

If the file is deleted then it will be necessary to start AuditTrail again from its shared location (on the network). When AuditTrail sees that the file is gone it will assume it's in its initial install mode and prompt for answers it needs to configure itself. It should be noted that ***FOLLOWING THIS PROCEDURE WILL NOT CAUSE ANY DATA LOSS.*** These settings do not in any way impact the security and stability of the database but rather inform AuditTrail how the specific installation needs to be configured in order to run properly at your facility.

There are several entries in a given settings.ini file and they are described here:

[AuditTrail] (Section heading)

FePath=”...” <= Where the Front End resided. This is the file end users will use.

ICON=”...” <= Location where the icon for the shortcut resides

BePath=”...” <= Location where the data is kept. This is the file you will need to take care to preserve.

CSECPath=”...” <= Last known location of the CSEC database

SiteID =”...” <=Your site's installation ID used for registration

**If you relocate AuditTrail you will need to change these paths accordingly or delete this file as stated above*

[Tools] This heading is for administrative control of the database.

Relink=No <=Changing this to Yes will force the frontend to relink to the backend. This is useful in cases where the system location has changed or if a disconnect is suspected.

[Options] (Section heading)

Tree=ALL Inboxes <=This is the in-box the user selected. Referenced on next load it will put the user back in the in-box it last used. In the case that there are no audits in that in-box, ALL Inboxes will be the default. Saves time when a large number of audits are in the system.

Share=No <= This will determine whether users will install AuditTrail on their systems or if they will all share the same copy on the server. According to Microsoft, having multiple users accessing the same front end can cause corruption. Best practices dictate that users have their own copy. However, policy prevents file copying onto local machines in some locations. This can be changed here if necessary.

Gray=No <=Optional. For better performance a user may elect to turn the color coding off on the main screen. This is set on a per user basis and can be changed at any time.

[Locale]

Locale=Development Lab <=Your facility name i.e. FRC Northwest

LocalInstallPath = "…" <=If shared mode is set to No (preferred) then this is the path on the local user's machine where AuditTrail will install itself. If all fails, then contact AuditTrail support (appendix a) for assistance.

[Email]

subject = AUTOMATED: Audit notification <=Email subject line for notifications. Change as needed.

message = You have received an Audit in your inbox. Please review it at your earliest convenience.   This is an automated message. If you feel you have received this message in error, please forward this email to email@yourfacility.navy.mil <=You can change this to read anything you like. This is a default template and is entirely discretionary.

Mortem.dmp

The mortem.dmp file is a log file that AuditTrail creates as the user works. In the event that there is a malfunction, AuditTrail will try to contact the developers with details about the malfunction and include this file. This information is needed by the developers as it gives a detailed step by step account of what was going on when the malfunction occurred.

As a side note, crash reports do not include any data from audits, hits, etc. It only includes meta-data that describes which buttons were clicked in which order etc so we can recreate the circumstances that led to the failure.

Every time AuditTrail starts it deletes this file and starts a new one. This way only the information from current session is in the file. You are free to delete it at any time you wish and is not necessary to include in any backups.

Related articles

- Manual Install Procedure
- Documentation