

Integritest[®] 4N Integrity Test Instrument Network and Administrator Manual

MILLIPORE

Contents

Introduction	7
Preface	
Networking Features.....	8
Network Configurations	9
Chapter 1 Networking an Instrument	9
Wireless Network.....	10
Integritest 4N Instrument Central Instrument Management Tool.....	10
Password Policy	11
Chapter 2 Network Security	11
Account Lockout	13
Audit Policy	14
Security Options	15
Virus Protection	17
Why is Virus Protection of the Integritest 4N Instrument Not Required?	17
Why can Antivirus Software not be installed on the Integritest 4N?	17
Options for Antivirus Protection of the Integritest 4N Instrument.....	18
Report Options	19
Chapter 3 Report and Printer Options	19
Specifying Operator Input Requirements	19
Printer Options	21
Installing Addressable Network Printers.....	21
Setting Default Printer.....	21
Understanding Report Transfers	23
Chapter 4 Setting Up Network Options	23
Selecting Remote Backup Options	24
Selecting Report Transfer Options	25
Auditing from Backup Files	29

Chapter 5 Auditing an Instrument and Central IMT Software	29
Extracting Audit Files.....	30
Auditing Files.....	35
XML Overview	41
Chapter 6 XML Filter Test Reports.....	41
Configuration Table Sub Elements	44
TestResults Sub Elements.....	44
TestResultsRow Table Element Sub elements.....	47
CalResults Table Element Sub elements	48
Signatures Table Element Sub elements.....	48
Chapter 7 Troubleshooting.....	49
Verifying External Resource Connection	49
Using ping and ipconfig	49
Log File Entries	49
Unavailability of a Printer.....	50
Add Printer Dialog Window Disappears	50
Event Log Overwrites	50
Central IMT Software.....	50

Introduction

The Millipore Integritest 4N Automatic Filter Integrity Tester is designed to conduct on-site bubble point, diffusion, HydroCorr™ tests and additional tests on a wide range of membrane filter systems. Designed for continuous operation, the Integritest 4N Instrument conducts filter integrity tests on the upstream side of the filter system, ensuring sterility of downstream connections, while simultaneously tracking data and test results. Both hydrophobic and hydrophilic membrane filters can be tested with the instrument, and testing is not limited to Millipore products.

The Integritest 4N Instrument is equipped with a customized Microsoft® software and Windows XP® Embedded operating system that has been validated for use with the instrument.

The Integritest 4N Instrument software is designed to increase productivity by taking advantage of isolated and integrated network infrastructures. The primary productivity gains are printing to a standard paper size network printer, saving test reports to a central data repository and, with an optional Central Instrument Management Tool (IMT) software, remotely administering Integritest 4N Instruments from a networked personal computer (PC). The isolated network includes the Integritest 4N Instruments, printers, and electronic file repositories only.

The instrument complies with the technical controls of 21 CFR Part 11 for electronic records and electronic signatures. Test reports can be signed electronically by the operator and a supervisor. All changes to user, test, and instrument configuration are logged with the date, time, and name of the individual making the change. It is the responsibility of the end user to maintain compliance with applicable data security policies and regulations, including 21 CFR Part 11.

It is recommended that the user be familiar with Windows XP administration before attempting to perform administrative duties on the instrument. Administrative changes may only be made by a SuperUser. For a detailed description of all Instrument User Roles, please see the Integritest 4 Automatic Integrity Test Instrument XIT4S0001 and XIT4N0001 Operators Manual. This publication is to be used as a reference for the instrument hardware and the Millipore software.

Networking Features

There are four basic networking features available on the instrument:

Remote Printing

The Integritest 4N Instrument can print test reports by sending data to an external printer that is configured on the network.

Backup

Data can be sent to another network location for backup and audit purposes.

Report Transfer

Completed filter test reports can be sent to the central repository and then be removed from the instrument. Checksum files are sent with reports to verify validity of reports.

Electronic Signatures

Signatures may be added to transferred reports that include user name, date, time, and reason for signature validation. Multiple signatures may be configured, and reports will not transfer to the central repository unless the appropriate signatures have been provided.

Chapter 1

Networking an Instrument

Network Configurations

One or more Integritest 4N Instruments can be connected to an external printer and/or back-up devices, such as a PC or networked attached storage (NAS). Consult a network administrator for DHCP and DNS configuration in a typical network. Integritest 4N Instruments are DHCP enabled by default.




Two network configurations are available, one with the Central IMT and one without the Central IMT software.

Cabled Network

A cabled network requires the following components:

- Print server or networked printer or
- NAS or PC
- Appropriate lines and devices as listed per the device manufacturer's specifications

To set up a cabled network, one or more hubs are required. Plug all lines into the hub and a network connection should be established. Follow the steps below to test the connection of each external resource: report repository, backup repository, and printers.

1. Log in as an administrator.
2. Select the  **Instrument Management Tool**.
3. Select **Manage System Options** and press the  icon.
4. Press the  icon once to access the **External Resource Setup**.

5. To test the connection of the report repository to the instrument, select the **Report Repository** tab and press the **Test Connection** button to view any errors.
6. To test the connection of the backup repository, press the **Backup Repository** tab and press the **Test Connection** button to view any errors.
7. To test the connection of the printer, press the **Printers** tab and select desired printer. Under the **Printer** menu, select **Properties** to see if the printer is connected to the instrument.

Wireless Network

A wireless network requires the following additional components or equivalents:

- One wireless ethernet bridge for each Integritest 4N Instrument
- Wireless access point

Configure the access point and wireless ethernet bridge on a separate PC per the manufacturer's guidelines. **Note: All wireless ethernet bridges must be compatible with their respective access points.** Once the ethernet bridge and the access point are configured, connect the access point to the printer and server. The wireless bridge connects to the Integritest 4N Instrument. The connection can be tested as previously outlined above.

Integritest 4N Instrument Central Instrument Management Tool

The Integritest 4N Instrument Central Instrument Management Tool (IMT) is designed to provide centralized administration of filter testing instruments on a network. The Central IMT software is used by administrators to manage instruments users, tests, reports, and other system options.

The network functionality of the Integritest 4N Instrument, with or without the Central IMT software is independent of the physical connectivity or availability of shared resources. Resource sharing is based on standard Windows sharing software (files, printers). Connectivity is based on TCP/IP.

Authentication (gaining access to shared resources) uses standard protocols as the Integritest 4N Instruments use the Windows XP embedded operating system.

Installation procedures and network configuration information for the Central IMT software can be found in the *Integritest 4N Integrity Test Instrument Central Instrument Management Tool Installation and Operators Manual*.

Password Policy

The items discussed in this chapter only apply to local users. For domain users, domain security policies are applied automatically.

The Integritest 4N Instrument provides configurable settings for password security to meet the requirements of 21 CFR Part 11. The default settings were chosen to enable easy access during instrument setup. The settings below can be customized to meet the needs of process requirements. All other settings are Windows XP Embedded system defaults, and should be left as such.

1. Login as a SuperUser.
2. Under the **Start** menu, access the **Control Panel**.
3. Open **Administrative Tools**.
4. Open **Local Security Policy**.
5. Open the **Account Policies** folder.
6. Open the **Password Policy** folder to make changes to any password settings.

Setting	Description	Default
Enforce password history	Determines the number of unique new passwords a user must use before an old password can be reused. It can be set between 0 and 24; if set to 0, enforce password history is disabled.	0 passwords remembered
Maximum password age	Determines how many days a password can be used before the user is required to change it. Can be set between 0 and 999; if set to 0, passwords never expire.	0
Minimum password age	Determines how many days a user must keep their new password before they can change it. This setting is designed to work with the 'Enforce password history' setting so that users cannot quickly reset their password 24 times and then change their password back to the old password. It can be set between 0 and 999; if set to 0, users can change their password immediately after changing it.	0 days

Setting	Description	Default
Minimum password length	Determines how short passwords can be. This setting can be set between 0 and 14 characters. If it is set to 0, then users are allowed to have blank passwords.	4 characters
Passwords must meet complexity requirements	<ul style="list-style-type: none"> • Determines whether or not password complexity is enforced. <p>When this setting is enabled user passwords will have the following requirements:</p> <ul style="list-style-type: none"> • The password is at least six characters long. • The password contains characters from three of the following categories: <ul style="list-style-type: none"> English uppercase characters (A - Z) English lowercase characters (a - z) base 10 digits (0 - 9); non-alphanumeric (e.g.: !, \$, #, or %) Unicode characters (e.g.: ä, ö, ü, ß, ç, ô). • The password does not contain three or more characters from the user's account name. If the account name is less than three characters long then this check is not performed. When checking against the user's full name, these characters are treated as delimiters that separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, pound-signs and tabs. For each token that is three or more characters long, that token is searched for in the password, and if it is present, the password change is rejected. For example, the name "Erin M. Hagens" would be split into three tokens: "Erin," "M," and "Hagens." Since the second token is only one character long it would be ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. All of these checks are not case sensitive. 	Disabled

Setting	Description	Default
Store password using reversible encryption for all users in the domain	Determines whether or not passwords are stored on the system using reversible encryption.	Disabled

Account Lockout

The Integritest 4N Instrument provides configurable settings for account lockouts to meet the requirements of 21 CFR Part 11. The default settings were chosen to enable easy access during instrument setup. Settings can be customized to meet the needs of process requirements.

1. Login as a SuperUser.
2. Under the **Start** menu, access the **Control Panel**.
3. Open **Administrative Tools**.
4. Open **Local Security Policy**.
5. Open the **Account Policies** folder.
6. Open the **Account Lockout** folder to change any Account Lockout settings.

Setting	Description	Default
Account Lockout Duration	Determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The range is 1 to 99,999 minutes. A value of 0 results in the account being locked out until an administrator explicitly unlocks it by setting the value to 0. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.	Not applicable
Account Lockout Threshold	Determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. Failed logon attempts values can be set between 1 and 999, or can be set to 0 to specify that the account will never be locked out.	0 Invalid login attempts

Setting	Description	Default
Reset Account Lockout Counter	Determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0. The range is 1 to 99,999 minutes. If an account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.	None

Audit Policy

The Integritest 4N Instrument provides configurable settings for audit policy to meet the requirements of 21 CFR Part 11. The default settings were chosen to enable easy access during instrument setup. Settings can be customized to meet the needs of process requirements.

1. Login as a SuperUser.
2. Under the **Start** menu, access the **Control Panel**.
3. Open **Administrative Tools**.
4. Open **Local Policies**.
5. Open the **Audit Policy** folder to change Audit Policy Settings.

Setting	Description	Default
Audit Account Logon Events	This policy setting determines whether or not to audit successes and audit failures. Success audits generate an audit entry when an account logon attempt succeeds. Failure audits generate an audit entry when an account logon attempt fails.	Success Failure
Audit Account Management	Determines whether to audit account management events: <ul style="list-style-type: none"> • When a user account or group is created, changed, or deleted. • When a user account is renamed, disabled, or enabled. • A password is set or changed. If this policy setting is defined, audit successes, audit failures, or not audit the event type at all can be specified. Success audits generate an audit entry when any account management event succeeds. Failure audits generate an audit entry when any account management event fails.	Success Failure

Setting	Description	Default
Audit Policy Change	<p>Determines whether to audit every incidence of a change to user rights assignment policies, audit policies, or trust policies.</p> <p>If this policy setting is defined, specify whether to audit successes, failures, or not audit the event type at all. Success audits generate an audit entry when a change to user rights assignment policies, audit policies, or trust policies is successful. Failure audits generate an audit entry when a change to user rights assignment policies, audit policies, or trust policies fails.</p>	Success Failure
Audit Privilege Use	<p>Determines whether to audit each instance of a user exercising a user right.</p> <p>If this policy setting is defined, specify whether to audit successes, failures, or not audit the event type at all. Success audits generate an audit entry when the exercise of a user right succeeds. Failure audits generate an audit entry when the exercise of a user right fails.</p>	Success Failure
Audit System Events	<p>Determines whether to audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.</p> <p>If this policy setting is defined, specify whether to audit successes or failures. Success audits generate an audit entry when a system event is executed successfully. Failure audits generate an audit entry when a system event is attempted unsuccessfully.</p>	Success Failure

Security Options

The Integritest 4N Instrument provides configurable settings for security options to meet the requirements of 21 CFR Part 11. The default settings were chosen to enable easy access during instrument setup. Settings can be customized to meet the needs of process requirements.

1. Login as a SuperUser.

2. Under the **Start** menu, access the **Control Panel**.
3. Open **Administrative Tools**.
4. Open **Local Policies**.
5. Open the **Security Options** folder to change Security Settings.

Setting	Description	Default
Administrator Account Status	<p>Determines whether the Administrator account is enabled or disabled under normal operation.</p> <ul style="list-style-type: none"> • If an attempt is made to reenble the Administrator account after it has been disabled, and if the current Administrator password does not meet the password requirements, the account cannot be reenbled. In this case, an alternative member of the Administrators group must set the password on the Administrators account by using the Local Users and Groups user interface. • Disabling the Administrator account can become a maintenance issue under certain circumstances. For example, in a domain environment, if the secure channel that constitutes the user's join status fails for any reason, and there is no other local Administrator account, the Integritest 4N System must be restarted in safe mode to fix the problem. 	Enabled
Interactive Logon: Do Not Display User Name	Allows user name to be preset so that only the password must be entered. For requirements of the electronic signature elements of 21 CFR Part 11, both user name and password must be entered by the operator to generate a valid electronic signature. When electronic signatures are not used, it may be beneficial to allow the instrument to populate the most recently used user name and require only the password.	Enabled
Guest Account Status	Account that would enable an unregistered user to operate the instrument.	Disabled

Virus Protection

Millipore has received requests to protect the Integritest 4N Instrument with antivirus software. It is Millipore's position that the Integritest 4N Instrument does not need antivirus software for protection nor does it provide a network virus security threat. As such the Integritest 4N Instrument was not designed to accommodate Antivirus software.

Why is Virus Protection of the Integritest 4N Instrument Not Required?

The Integritest 4N Instrument only runs the software it is intended to run. It is not intended to access the Internet, which is the primary source of software viruses. Further, the software modules that are required for such access do not exist because the designer of the system did not include them when he chose the components of the embedded operating system. For example, there is no Internet browser and no capability for email. Thus, the risk of virus infection is greatly minimized. When the Integritest 4N Instrument is connected to a corporate network, it only communicates with well-defined network equipment but not with the outside world.

TCP ports that give access to the system and through which viruses typically spread inside a network are closed on the Integritest 4N Instrument. Only ports required to transfer software updates and perform system calibration are open and require a special tool to be accessed.

Infection of the corporate network originating from the Integritest 4N Instrument is extremely unlikely. For any viruses to arrive on the Integritest 4N Instrument they would have to travel through the network first.

Why can Antivirus Software not be installed on the Integritest 4N Instrument?

Operating System

The operating system of the Integritest 4N Instrument includes Windows XP Embedded operating system. This is a reduced version of the Windows XP operating system. The software designer selects those components of Windows XP operating system that are required to run the system, while leaving out those that are not required. This results in a custom version of the operating system that is well-defined and extremely stable. Commercially available antivirus software requires modules of the operating system that are not present on the Integritest 4N Instrument. Thus, a user cannot simply install an antivirus package and expect it to work.

System Performance

Since, by its nature, antivirus software intercepts the operating system's functions to protect the system, it can have unpredictable effects on the performance of the system. For example, antivirus software intercepts all disk activity to check files that are read or written to the harddisk. This task takes a certain, but undefined, amount of time, which can cause measurements to be delayed.

Secondly, antivirus software reduces the available processor power to some extent in order to execute. While the Integritest 4N Instrument was fully validated in the configuration in which it is sold, Millipore would not be able to guarantee that it performs correctly when the processor is asynchronously interrupted for antivirus tasks that were not present in the

originally validated system.

Currently, the most popular anti-virus software manufacturers do not support the use of their software on Windows XP embedded operating system. As stated above, this is primarily due to the component structure of the embedded operating system, which does not guarantee that the required modules are present.

What Options Exists for Antivirus Protection of the Integritest 4N Instrument?

Firewall

To ensure that viruses cannot reach the Integritest 4N Instrument, a user may install a firewall router between the instrument and the corporate network. Multiple Integritest 4N Instrument systems may be connected on the protected side of the firewall.

The firewall can be programmed to block all unwanted access to the systems. By only allowing specific hosts to access the instruments on the restricted ports, the risk of contracting a virus via the corporate network is greatly reduced.

The use of a firewall is the best option to ensure separation between the Integritest 4N Instruments and the corporate network.

Remote Scanning

The files on the Integritest 4N Instrument can be scanned remotely from a server or a different PC. This task can easily be automated in most Antivirus packages so that a scan is run daily or weekly at pre-set times. If possible, it is recommended that remote scanning is performed while the Integritest 4N Instrument is not being used for filter testing to minimize the risk of affecting the performance of the application software.

Report Options

Test reports are the official record of filter integrity test performance. It is important to set the report options before any tests are run. The administrator should determine these parameters, following any relevant standard operating procedures.

Specifying Operator Input Requirements

The instrument allows an administrator to customize the input required of operators before each test to facilitate consistency with standard operating procedures. Log in as an administrator with SuperUser privileges, but do not select SuperUser mode.

1. From the **Tools Menu** select  **Instrument Management Tool** to access the **Local Instrument Management Tool**.

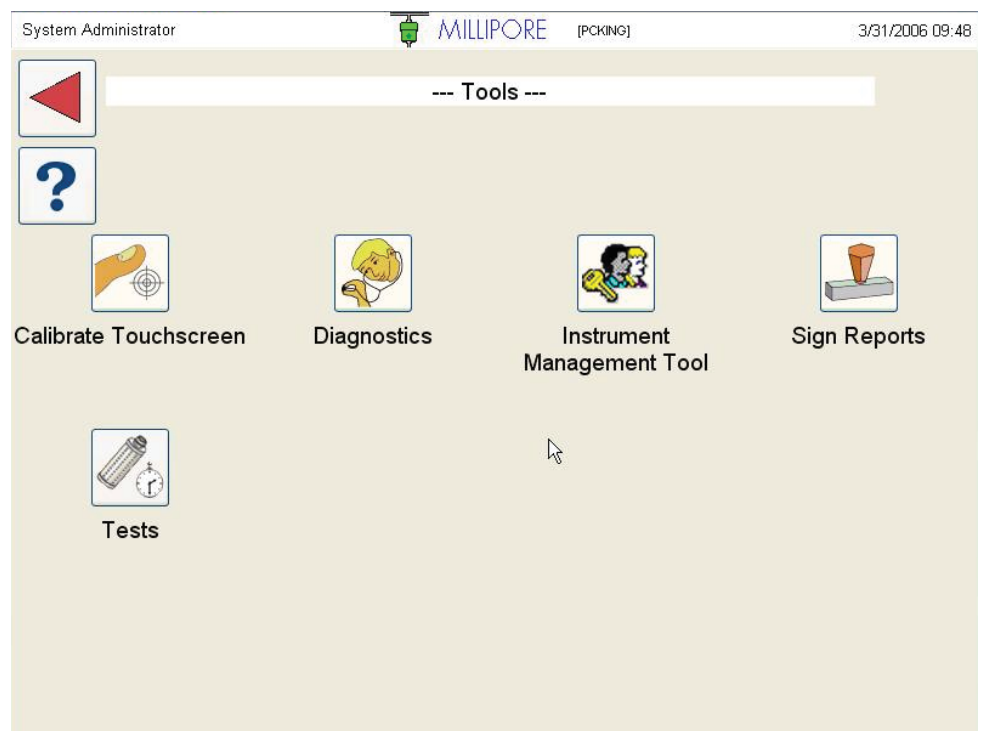



Figure 5: Tools menu



Figure 6: Local Instrument Management Tool

2. Select **Manage System Options** and press the  icon three times to access **System Setup**.
3. **Comment Req**
Select “Yes” or “No” under Comment Req if a comment should be forced to start a test.
4. **Signatures**
Check this box to specify zero, one, or two signature blocks on reports. For a test report to be signed off, a valid User ID must be created.
 - If 0 signatures are selected, the check box for Requires Supervisor will be grayed out on screen, and no signatures will be necessary for test report transfer.
 - If 1 signature is selected, the instrument will require one user to enter a UserID, password and reason for signing. Once this is done, the test report is considered complete, and the report can be transferred.
 - If 2 signatures are selected, one user must enter the required information. Once that is completed, a second signature box becomes available, and a second user must enter their information. A different user must provide the second signature, with a different UserID and password.


5. **Requires Supervisor**

Check this box under Electronic Signatures to necessitate a supervisor signing the report. This option is only enabled for two signatures and will be grayed out on-screen if less than two are selected.

6. **Autoprint**

Check this box to automatically print reports upon test completion.

7. Select the  icon to save changes.

8. A system restart window will pop up. Click OK, and press  the twice to return to the **Tools** screen.



Printer Options

Installing Addressable Network Printers

Network printer drivers may be installed onto the Integritest 4N Instrument by Millipore Technical Services.

Setting Default Printer

By default, the instrument is configured to use the internal printer. A SuperUser may install an external or network printer and set that printer as the default. Follow these steps to set a default printer.

1. Log on as a SuperUser and select  **Instrument Management Tool** from the **Tools Menu**. Select **Manage System Options**, press the  icon twice and select the Printers tab under **External Resource Setup**.

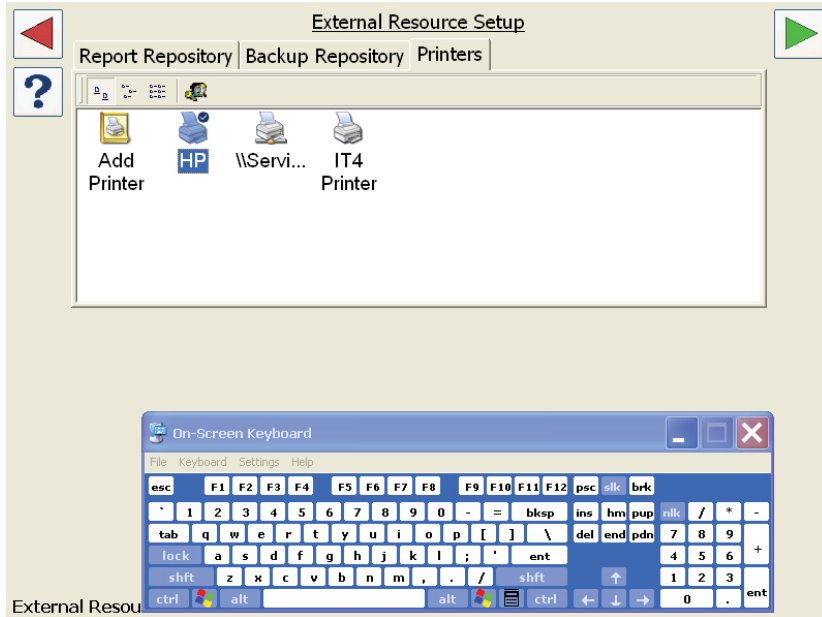




Figure 7: Printers/External resource setup

This window contains all configured printers, and allows printers to be installed and set as default.

2. To set a printer as the default, press the specific printer icon and select the  icon on the on-screen keyboard to access the Printer Menu. Select **Set as Default Printer** from the **Printer** menu. The default printer will have a check mark on its icon.

Note: If the External Resource Setup window has covered the Add Printer option, access the Add Printer window by using the onscreen keyboard and ALT TAB. TAB as necessary to select the Add Printer window, and then press the ALT key once more.

3. After any printer parameters are changed, the Integritest 4N Instrument must be rebooted for changes to be implemented.
4. Press the  three times to return to the **Tools** menu.

Chapter 4

Setting Up Network Options

For users of the Central IMT software, refer to this chapter for definitions and descriptions only, not for instrument settings. Instructions for creating these settings are located in the Central IMT software Operators Manual. Settings done in the instrument will be overwritten by those defined in the Central IMT software during the course of an update.

Understanding Report Transfers

Each file transferred by the instrument is based on the name of the instrument and the test serial number.

File Type	Extension	Sample File Name
PDF report	PDF	TEST-W11111-20030419093019.PDF
PDF checksum	PDFSUM	TEST-W11111-20030419093019.PDFSUM
XML report	XML	TEST-W11111-20030419093019.XML
XML check-sum	XMLSUM	TEST-W11111-20030419093019.XMLSUM

As the instrument transfers each report, it also creates and transfers a checksum file to accompany each report. Every report in the central repository will have an accompanying checksum file, which is used to verify that the report has not been edited (see **Chapter 5 Auditing an Instrument**).

If no checksum file was sent, the transfer was interrupted and the report file is not considered a valid test record. At the next transfer, the instrument will retransmit the report and checksum file for any test results that are in its database but do not have a checksum file in the central repository.

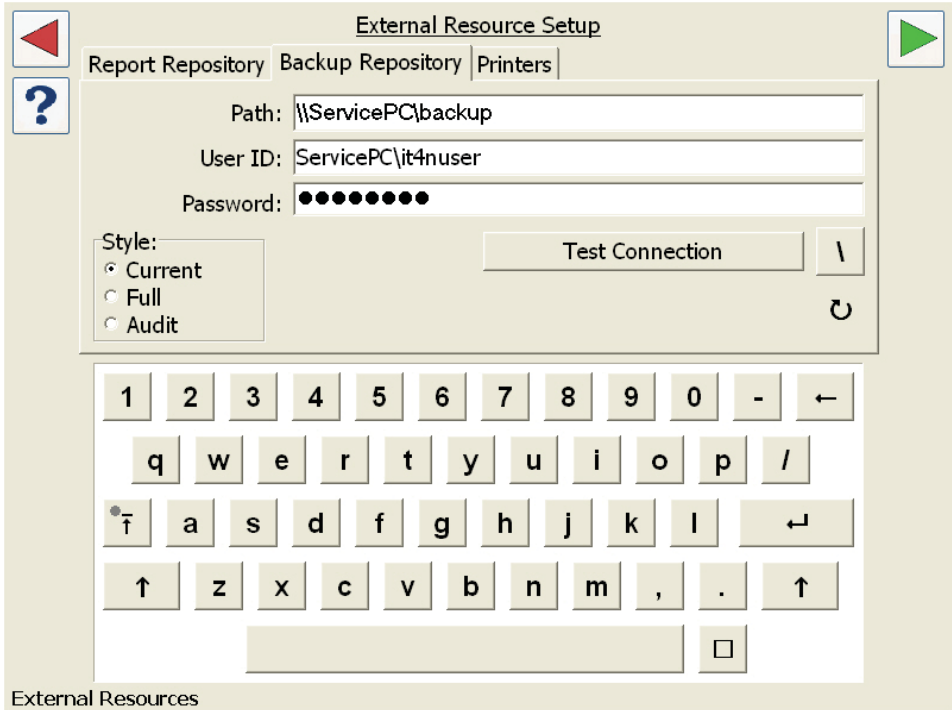
This feature can be used to retransfer any reports that are still in the database, even if those reports were transmitted successfully. If the original transferred report was lost, deleted or changed accidentally, then delete the checksum file from the central repository. The report will be recreated and sent during the next transfer.

Selecting Remote Backup Options

The Integritest 4N Instrument can be configured to send backup data to a specified Backup Location on the network. Backups are performed by administrators to save a record of the state of the instrument and may be automatically performed weekly. Performing regular backups allows for the complete recovery of test data and records in the event of a catastrophic failure. Restores require the services of a Millipore Technician.

The remote backup options are displayed in the **Backup Repository** tab. Follow the steps below to configure the remote backup options.

1. Press  **Instrument Management Tool** on the **Tools Menu**, select **Manage System Options**, and press the  icon twice.
2. Select the **Backup Repository** tab.



External Resource Setup

Report Repository | Backup Repository | Printers

Path: \\ServicePC\backup

User ID: ServicePC\it4nuser

Password: ●●●●●●●●

Style:

- Current
- Full
- Audit

Test Connection

External Resources

Figure 9: Backup Repository

3. The **Path** field contains the path to the **Backup Location** on the network.
4. Enter a valid **User ID**.
5. The **Style** options are only available if **Path**, **User ID** and **Password** fields are filled. The following table shows the types of backup files saved during backups.


Database files	integra.mdb	Server database
	Itclient.mdb	Client database
	Signature.mdb	Signature database
Log files	*.log	Instrument logs
Event files	*.evt	Operating System Logs
Unzip key for auditing	XceedZip.dll	See Auditing an Instrument
Auditing utility	auditor.exe	See Auditing an Instrument
	auditview.exe	See Auditing an Instrument
	languagestrings.mdb	See Auditing an Instrument

The following table shows the files created for each backup type.

Current (Current Data Only)	Full (Complete Backup)	Audit (Complete Backup & Audit Files)
Itclient.mdb	Itclient.mdb	Itclient.mdb
integra.mdb	integra.mdb	integra.mdb
Signature.mdb	Signature.mdb	Signature.mdb
	*.log	*.log
	*.options	*.options
		*.evt
		XceedZip.dll
		auditor.exe
		auditview.exe
		languagestrings.mdb



The **Audit** (Complete Backup & Audit Files) backup type is the only one that allows an auditor to unzip and view the contents of the backup files to be viewed on other computers. Data that is backed up using the Current Data Only or Complete Backup options is unmodifiable and used only in the event of performing a system restore.

The **Current Data Only**, **Complete Backup**, and **Complete Backup & Audit Files** headings correspond to the backup type options displayed to the user when performing a local backup.

6. Choose a **Style**.
7. Click the  icon to save and continue.

Selecting Report Transfer Options

The instrument can be configured to transfer completed test reports to a remote location called the central repository for later retrieval and review. The steps below describe how to configure the report transfer options; instructions for transferring reports can be found in the Integritest 4 Automatic Filter Integrity Test Instrument Operators Manual.

1. Log in as an administrator and press  **Instrument Management Tool** on the **Tools Menu**, select **Manage System Options**, and press the  icon twice.
2. Select the **Report Repository** tab.
3. The **Path** field contains the path to the central repository for reports.
4. Enter **User ID**. The logged in **User ID** must have access to the specified repository.

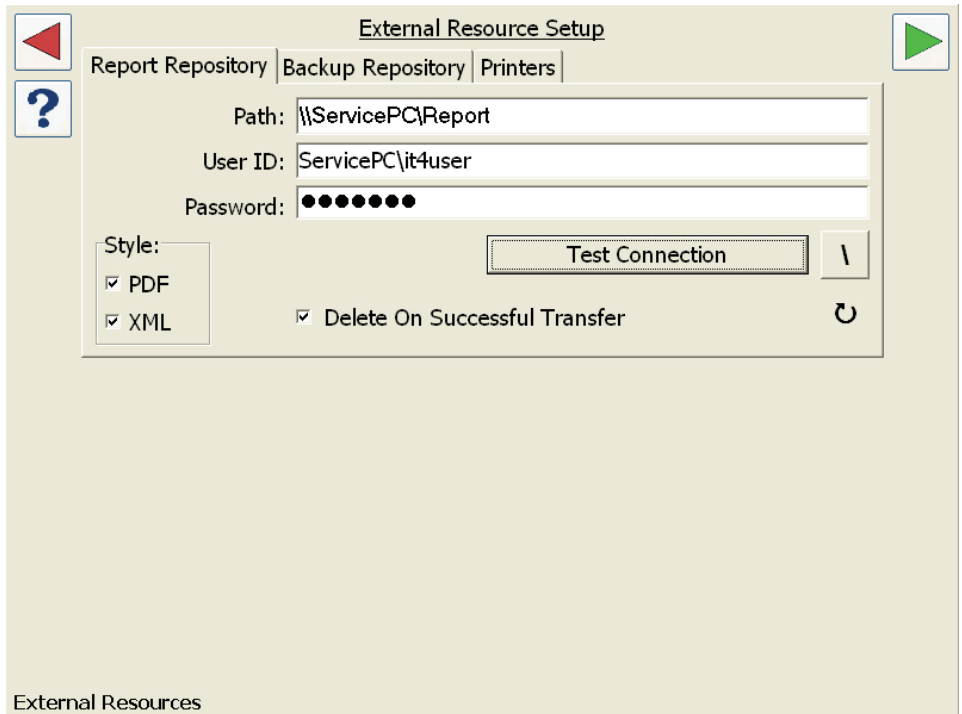


Figure 8: External resource setup

5. Choose a report **Style**.




Two report styles are available for transferred reports: **PDF (portable document file)** and **XML (extensible markup language)**. In the **Style** box, select **PDF**, **XML** or both by placing a check mark next to the desired style(s).

- The PDF report file generated by the instrument is a formatted report that can be reviewed with Adobe® Reader®.
- The XML report file contains all of the test data. This file can be viewed in a text editor, but is unformatted. If printing or analysis of the XML report is required, it is recommended that the latest version of Microsoft Internet Explorer be employed to view file code.

Note: The serial number of the test is found in the file name.

If only one report style is selected, all of the report files will be in the Central Repository folder. If both **PDF** and **XML** styles are selected, the **XML** file is considered the primary record file and the **PDF** file is placed in a Central Repository subdirectory named **PDF**.

6. To automatically remove data from the instrument after it has been transferred and processed, place a check mark in the **Delete on Successful Transfer** field. Selecting this option removes the test data from the instrument when the following two conditions apply.
 - The test report and its associated checksum file were transferred successfully to the central repository.
 - The report has been reviewed, processed, and removed from the central repository, leaving only its checksum file to be detected by the instrument during the next transfer. This option is only recommended if the network is secure and standard operating procedures governing the management of electronic test records exist. If the **Delete on Successful Transfer** field is left unchecked, all test results will be kept in the Instrument's database. Eventually, when the database becomes full, the Instrument will inform the user that the disk is full and no more tests may be stored. This ensures data integrity by not allowing an overwrite of the data.

7. Follow the steps below to test the connection of each external resource: report repository, backup repository, and printers.
 - Log in as an administrator.
 - Select the  **Instrument Management Tool**.
 - Select **Manage System Options** and press the  icon.
 - Press the  icon once to access the **External Resource Setup**.
 - To test the connection of the report repository to the instrument, select the **Report Repository** tab and press the **Test Connection** button to view any errors.
 - To test the connection of the backup repository, press the **Backup Repository** tab and press the **Test Connection** button to view any errors.
 - To test the connection of the printer, press the **Printers** tab and select desired printer. Under the **Printer** menu, select **Properties** to see if the printer is connected to the instrument.

- To check the instrument's network connection, connect the instrument to a PC with a known IP address and crossover cable to the same location as the Integritest 4N Instrument. If the PC is able to connect to the network but the Integritest 4N Instrument cannot, there may be an error within the Integritest 4N Instrument network.

Chapter 5

Auditing an Instrument and Central IMT Software

For users of the Central IMT software, there are additional audit files maintained on the service PC. These are located in C:\Program Files\Millipore\IT4NMaster\Audit.

Auditing from Backup Files

An audit may be performed to check the record of all tasks that have been performed on the instrument. An auditor may remotely view backup files on another computer on the Integrist 4N Instrument network. These files must be unzipped to be viewed.

Security logs (Securitylog<date>.evt) are readable using the Windows® Event Viewer and allow the SuperUser to search for Windows events related to audits, logins, and user changes.

Application logs (Applicationlog<date>.evt) are readable using the Windows Event Viewer and contain information about significant application events such as:

- Application Exception
- AutoUpdate Restart
- Compaction of a database
- Error changing password by a user
- Exacta Server information
- Flight Recorder does not exist
- Flight Recorder found
- Login attempt by a user
- Logout by a user
- Password Change by a user
- Run AutoUpdate
- Running as SuperUser

- Shutdown by a user
- Space check of Flight Recorder
- Startup of user interface
- System file checksum failed
- Test Data Removed
- Test Started
- Unable to save data to Flight Recorder.
- User interface shutdown

Maintenance changes (MaintChanges-<date>.txt) are located in the Audit subdirectory and can be used to audit changes to tests and system configuration, and audit updates (AuditUpdate-<date>.txt) can be viewed to monitor software version updates.

Other files are principally of interest to Millipore support.



Figure 10: Zipped audit file

The filename references the date and time of creation. In this case, the year is 2003 and the date is September 15th. The time is referenced last in 24 hour format (in this case 12:23:53 PM). The last digit (4) is indicative of the type of backup that was performed (see the following table). This is helpful for identification purposes if there is more than one backup file in a folder.

Last Digit of Zip filename	Backup Type
0	Complete Backup (Full)
1	Current Data Only (Current)
4	Audit

Extracting Audit Files

1. In the desired target directory, create a new folder that will be used as an audit workspace. In this example, the folder has been titled “Audit Workspace”.
2. Access the appropriate zip files from another computer on the Integritest 4N Instrument network using Windows XP Explorer (or another suitable decompression tool). Make sure that the option **Details** is enabled under the **View** drop down menu.

- Determine which files are password protected by examining whether “Yes” or “No” is listed under the heading “Has a Password”. Extract and transfer (either drag and drop or copy and paste) all unprotected files (XceedZip.dll, LanguageStrings.mdb, Auditor.exe, AuditView.exe) to a folder location where the auditing will take place (Audit Workspace in the example).

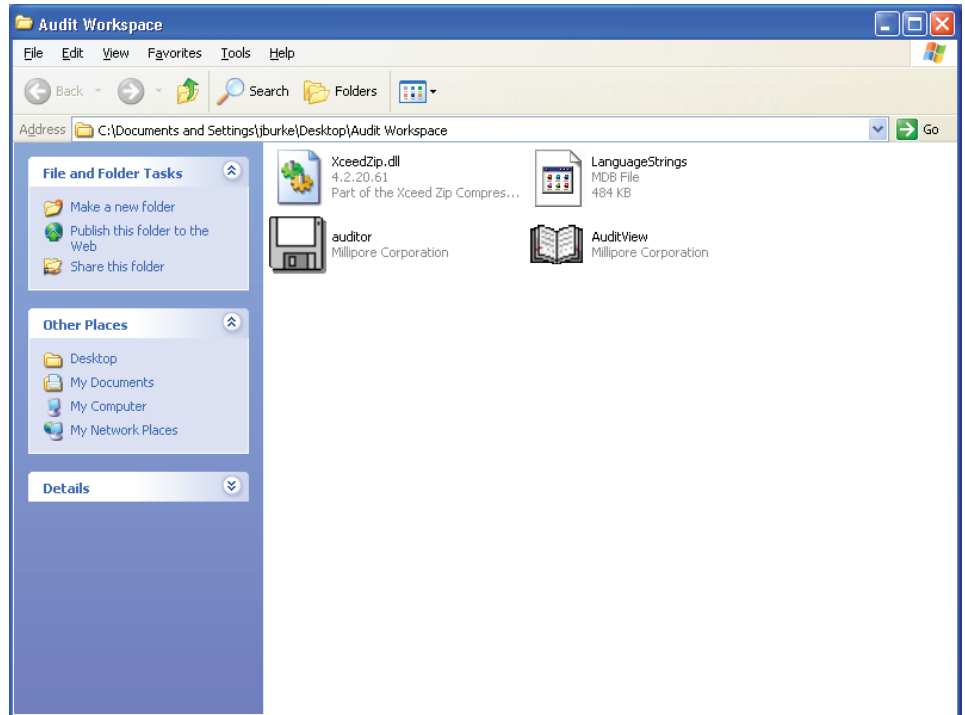


Figure 11: Auditing Workspace

- Open auditor.exe. Click the auditor.exe icon to open the Auditor window.

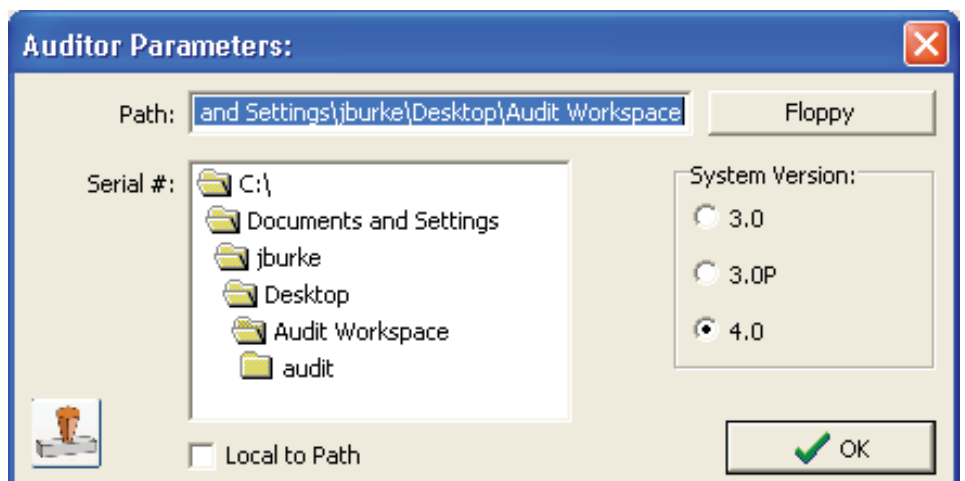


Figure 12: Auditing Parameters with local to path unchecked

- On the right side under **System Version**, select the appropriate version of the software. Auditor.exe defaults to the most current version, 4.0. Navigate to the folder with the serial number that corresponds to the files being audited, or enter it manually. If the folder icons are not visible (and the path is shown as a manually enterable field) uncheck the **Local to Path** box.

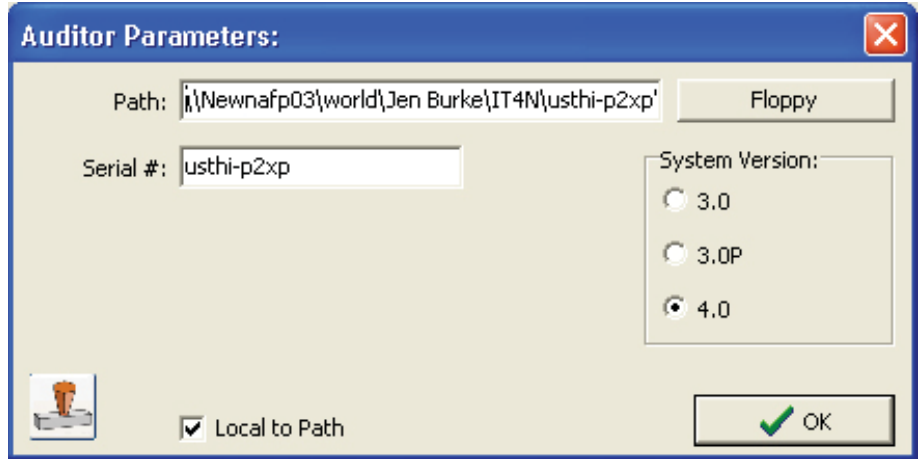


Figure 13: Auditing parameters manually entered serial number

- Click **OK**.
- A screen will prompt the user to select a folder to load all files to. Select the desired folder, and then click **OK**.

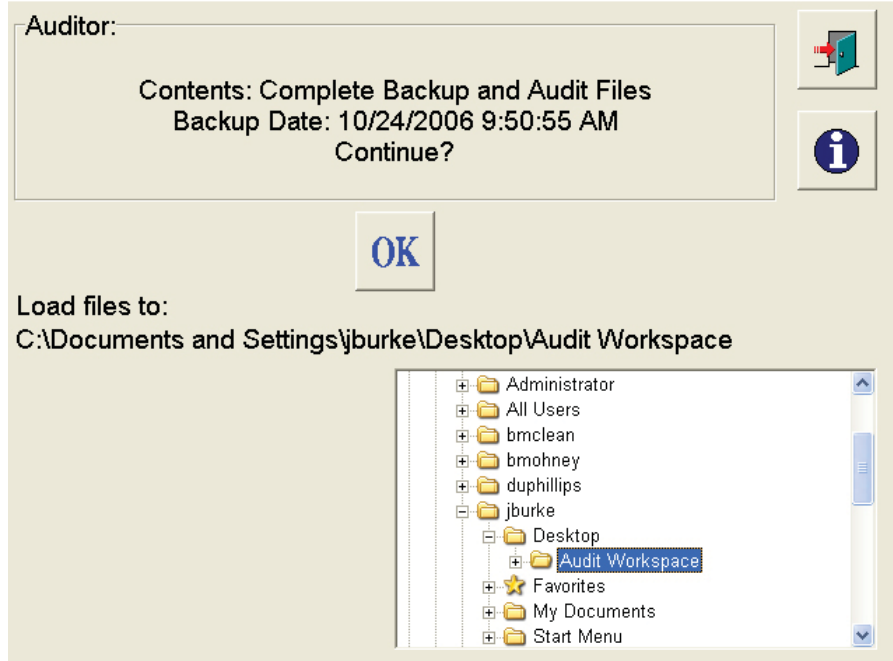


Figure 14: Load files screen

8. A list of files available for backup will be visible. Select the desired back up file (note: the only files that may be audited end in the numeral 4). If only one zip file is available, skip Step 8.

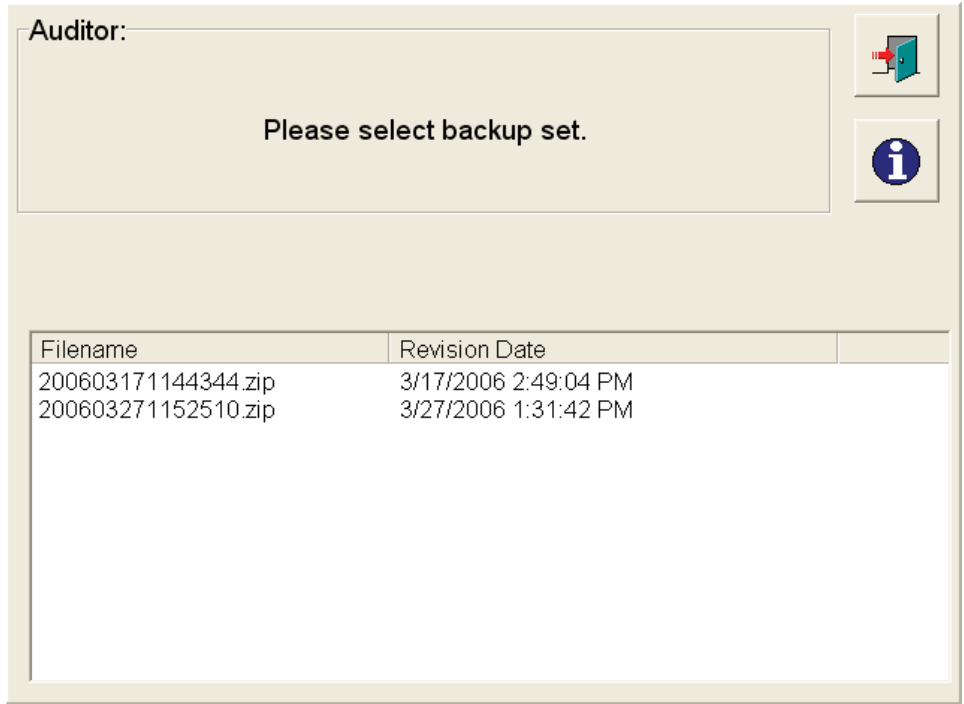


Figure 15: Backup selection

9. The next screen prompts the user to select a destination for all audited files to be loaded to. The example here selects a folder previously created in Step 1 called "Audit Workspace". Navigate to the desired folder, and then click **OK**.

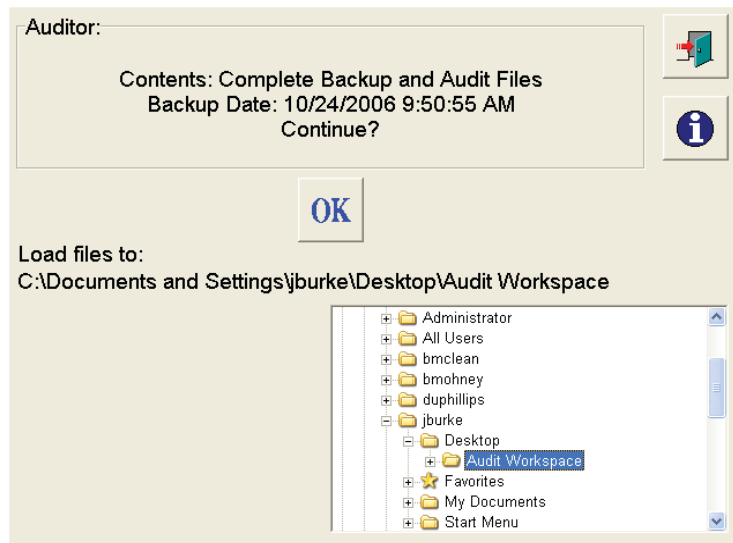


Figure 16: Select destination

10. Click **OK**, and the extracted files will be viewable.

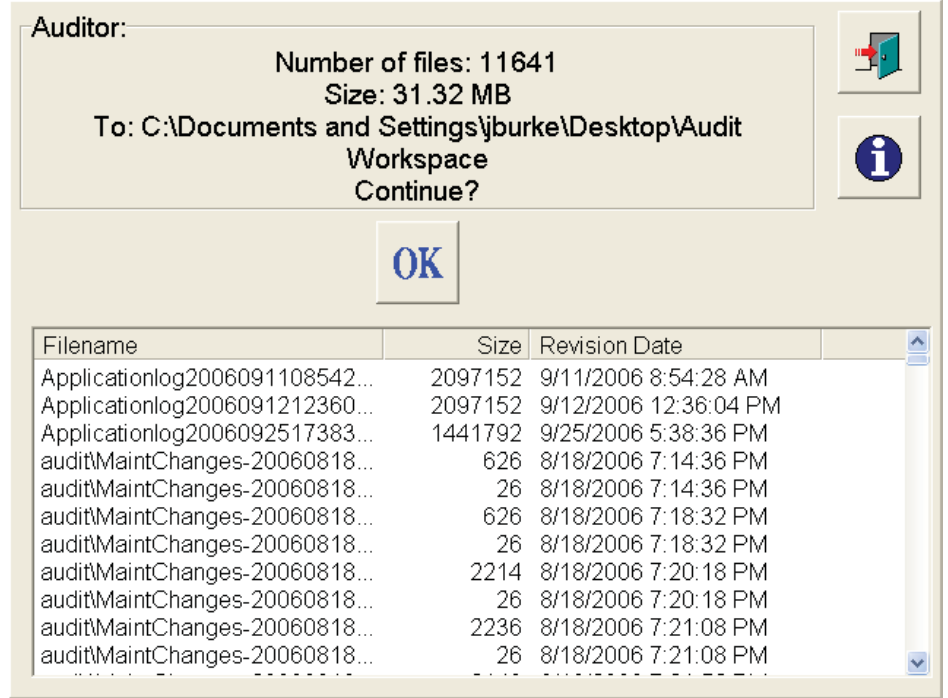


Figure 17: Auditor file listings

11. Click **OK** to continue with extraction. When the Auditor is finished extracting the files, select the **Close** button. The files may now be opened for review. The audit viewer is a supplied tool to simplify the viewing, but the extracted file types may also be opened with the following tools:

File	Associated Tool
.log	Notepad, Microsoft Word, or other text editing tool
.evt	Event Viewer (Microsoft Windows NT [®] or later Administrative Tool)
.mdb	Microsoft Access [™] database software, Microsoft Excel [®] spreadsheet software, or equivalent database viewer capable of reading Microsoft Access files

Auditing Files

1. In the Audit Workspace folder, open the program called Audit Viewer (auditview.exe).

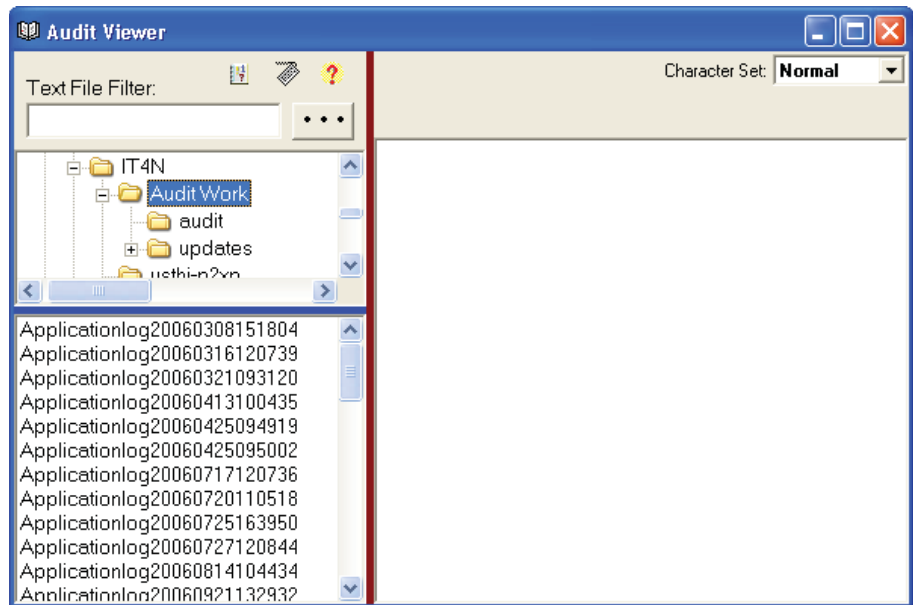


Figure 18: Audit viewer

2. To view files, navigate to the Audit Workspace folder by scrolling manually. Files may also be filtered by a keyword that may be entered in the **Text File Filter** field pictured below.

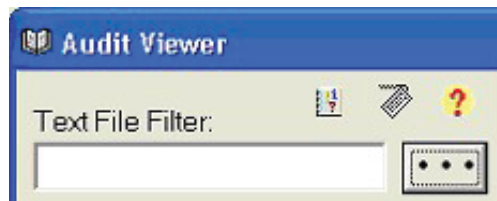


Figure 19: Text file filter field

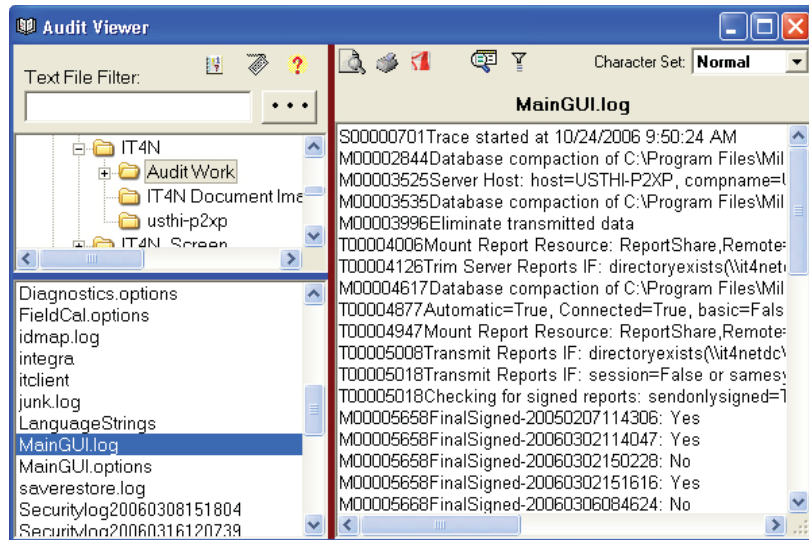



Figure 20: Audit viewer

- After the desired file has been selected, the search results can be narrowed by clicking the filter  icon, and entering a key word. The software automatically filters the selected file to include only the data containing the key word entered in the filter field.

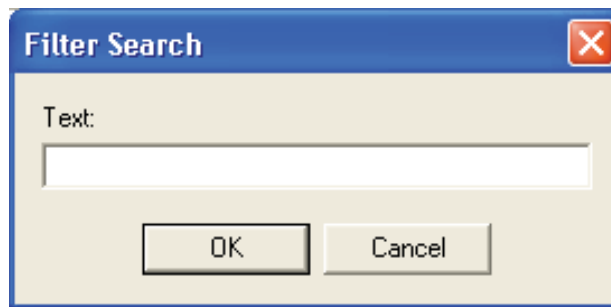



Figure 21: Filter search field

- The  icon acts as a search function. By selecting this icon and entering a word or phrase, the software will find all pertinent information in the selected log file.

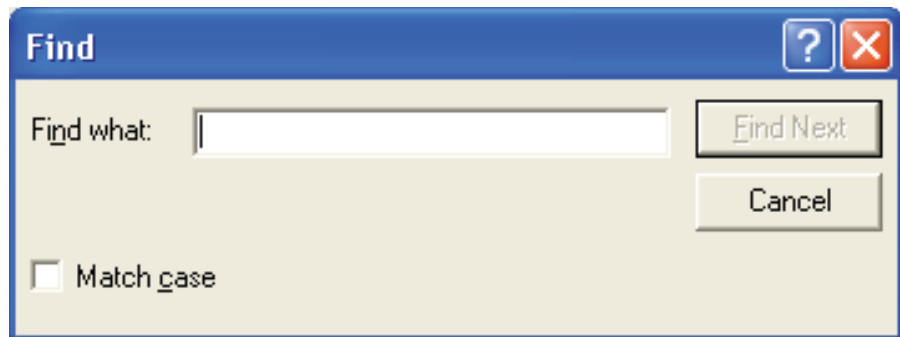




Figure 22: Find field

- To print an audited file, select the  icon and the printable version of the audit log will be sent to the printer; to preview the file before printing, click on the  icon to the left

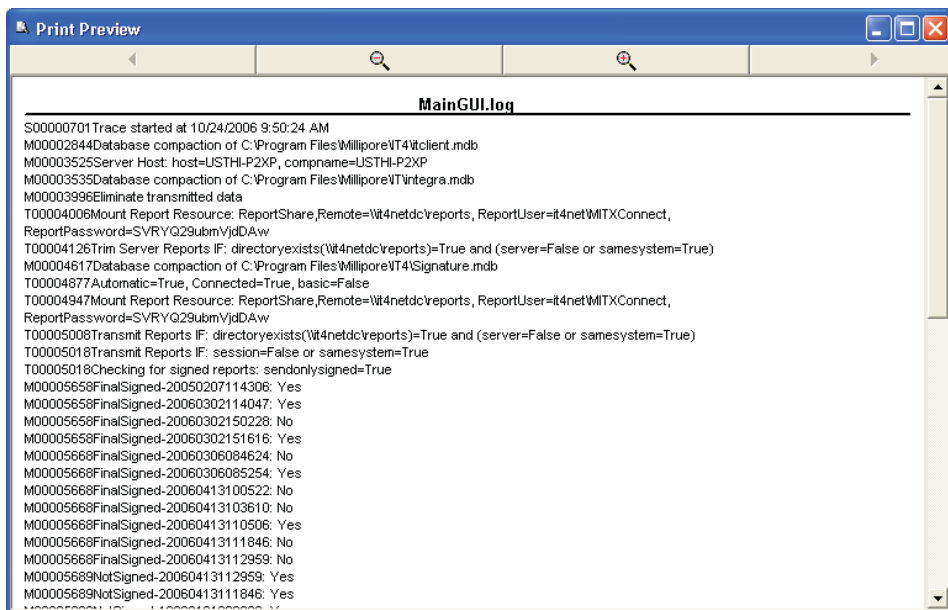


Figure 23: Print preview

- If the file is an event log, the Windows Event Viewer window will display the selected file. If the file is a database, a database viewer will display the selected file.

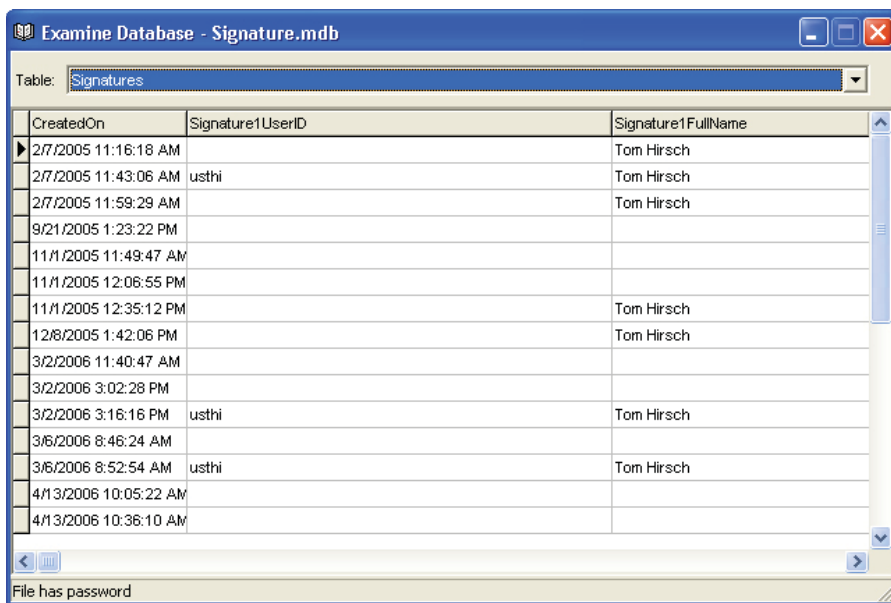


Figure 24: Sample Database

- To check validity of saved files that are paired with a checksum, select the file. The date and timestamp will be displayed in red if the file has been tampered with or altered in any fashion. A red date and timestamp may indicate an error in setting date and time of the computer. To correct errors in setting date and time, please refer to **Chapter 7 Troubleshooting**. Green date and timestamps indicate no problems.

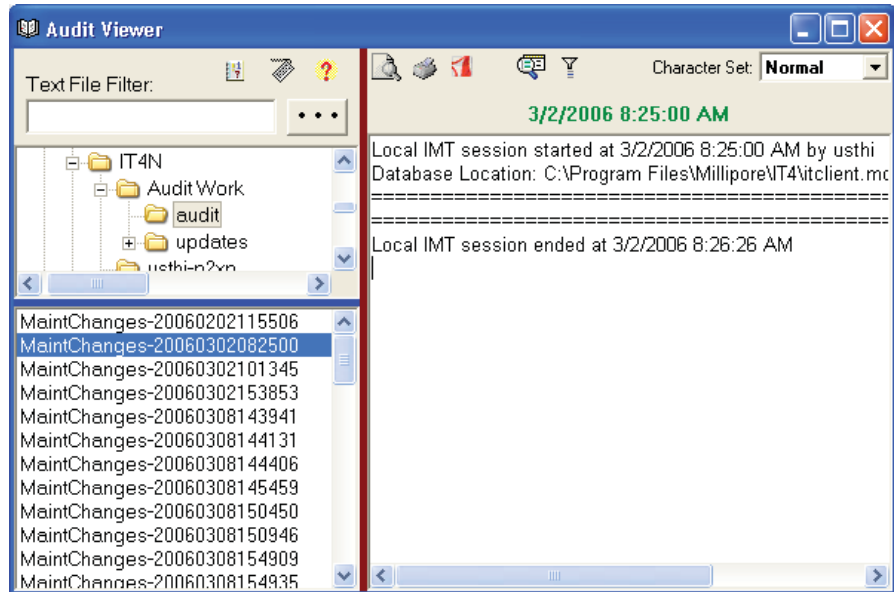


Figure 25: Valid Checksum

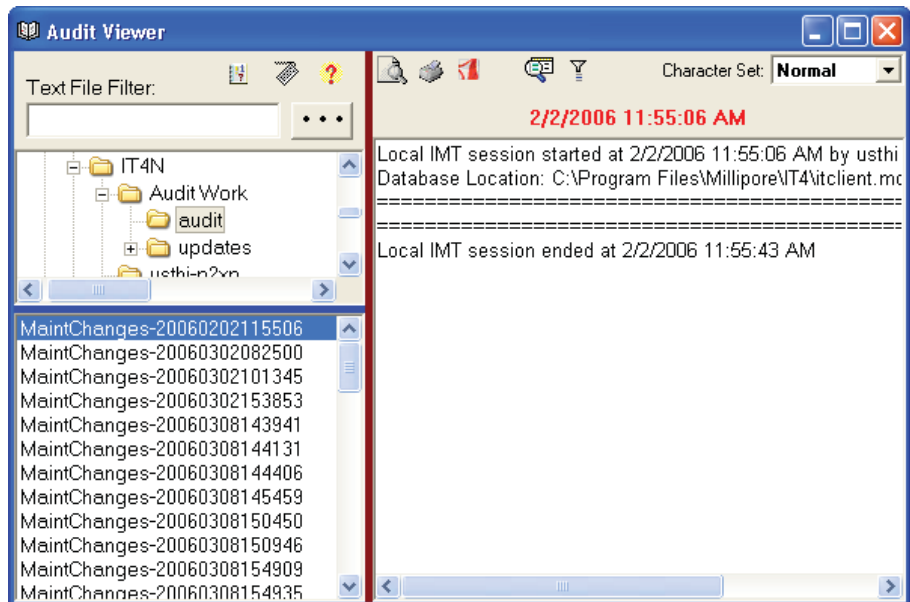


Figure 26: Invalid Checksum

Verifying Checksum Data

The Audit Viewer will automatically verify the checksum of those files that have them. Part of the checksum involves the file creation date. Different file systems associated with Windows use different methods to remember this time, such as local time or GMT. The relationship between the local time and GMT is critical for the checksum to be created or checked. If the time zone is set incorrectly, false positives on checksum errors may occur. Set all auditing computer time zones properly to avoid this problem.

Chapter 6

XML Filter Test Reports

XML Overview

The Integritest 4N Instrument can be programmed to export an XML version of filter test report data to a specified network location called a data repository. These XML files are useful for trending test data, integrating automatically into batch records or creating custom test reports. The following is a detailed explanation of a sample XML file data structure and the definitions of elements contained in the file. All pressure values are listed in psi.

```

<?xml version="1.0"?>
<ClientData>
  <FileRow>
    <Configuration>
      <FileRow>
        <ConfigurationID>13</ConfigurationID>
        <ModifiedBy>system</ModifiedBy>
        <ModifiedOn>10/6/2003 10:32:08 AM</ModifiedOn>
        ...
        <ITXVersion>4.00</ITXVersion>
      </FileRow>
    </Configuration>
    <TestResults>
      <FileRow>
        <CreatedOn>4/13/2006 11:05:06 AM</CreatedOn>
        <FilterID>ABCD1234</FilterID>
        <FilterRev>0</FilterRev>
        ...
        <PressureUnits>3301</PressureUnits>
      </FileRow>
    </TestResults>
    <TestResultsRow>
      <FileRow>
        <RowID>97</RowID>
        <CreatedOn>4/13/2006 11:05:06 AM</CreatedOn>
        <Value1>2.25408333333333</Value1>
        <Value2>19.9987</Value2>
        ...
        <Value7>0</Value7>
        <Value8>0</Value8>
      </FileRow>
      <FileRow>
        <RowID>98</RowID>
        ...
      </FileRow>
    ...
  </TestResultsRow>
  <CalResults>
    <FileRow>
      <ConfigurationID>54</ConfigurationID>
      ...
    </FileRow>
  </CalResults>
  <Signatures>
    <FileRow>
      <CreatedOn>4/13/2006 11:05:06 AM</CreatedOn>
      <Signature1UserID>usthi</Signature1UserID>
      ...
      <Signature2Check>1380685005</Signature2Check>
      <NumSigsReq>2</NumSigsReq>
    </FileRow>
  </Signatures>
</FileRow>
</ClientData>

```

Where:

XML Key (elements are the building blocks of XML and start with “<” and with an “>” followed by the element name):

- **XML Declaration:** specifies the version of XML being used
- **Root Element:** the tags that hold the XML document (<ClientData>)
- **Table Element:** have start and end tags and represent tables of data (<Signatures>)
- **Row Element:** have start and end tags and represent rows of data (<FileRow>)
- **Elements:** (aka paired elements) have start and end tags, data is between the tags themselves (<ConfigurationID>)
- **Character Data:** information between elements (13)

The above example omits much of the actual data for the sake of compactness. Please refer to an actual XML file if more information is necessary. Most element names are self-explanatory.

There are several table elements in the filter test report file.

Table Element	Element Description	Details
<Configuration>	Configuration information	Most of this data is not used; however, the elements used will be defined.
<TestResults>	Combination of test inputs and results	Only one row element exists. Many of the elements come from the test definitions and are described in the Managing Filter Tests section of the Integritest 4 Operators Manual.
<TestResultsRow>	Values obtained during the test.	Multiple row elements can exist and have different formats depending on the test and the phase of the test.
<CalResults>	Not applicable to this instrument.	Not described.
<Signatures>	Electronic signature information.	One one row element exists.

Configuration Table Sub Elements

Element	Element Description	Data Format
<UserField1Mandatory>	Required input field 1	True or False
<UserField2Mandatory>	Required input field 2	True or False
<InstrumentSerialNumber>	Serial number of the instrument	Text
All others	N/A	N/A

Values for most of the TestResults sub elements come from test definition and will not be defined below. For more specific explanations of test definition fields, consult the Integritytest 4 Operators Manual.

TestResults Sub Elements

Table Element	Element Description	Data Format
<CreatedOn>	Key	Date and time
<TestTypeID>	Test type: 1 = Bubble Point 2 = Enhanced BubblePoint 3 = Diffusion 4 = HydroCorr 7 = Enhanced BubblePoint (asymnetric membranes) 8 = BubblePoint (asymmetric membranes) 9 = Diffusion (variable prepressurization) 10 = Pressure Hold	Number
<MaximumBP>	If ((Bubble Point test or Enhanced Bubble Point test) and AcceleratedBpFlag=True) or (Bubble Point (asymmetrical membranes) test or Enhanced Bubble Point (asymmetrical membranes) test then Final Test Pressure else Maximum Bubble Point	Number
<AcceleratedBpFlag>	Accelerated test if (IT2LikeFlag = True and Diffusion Test) or (AcceleratedBpFlag = True and (not Bubble Point (asymmetric membranes) test and not Enhanced Bubble Point (asymmetric membranes) test) Hydrophobic/Utility if HydrophobicFilter = True	True or False
<IT2LikeFlag>		True or False

Table Element	Element Description	Data Format
<ManualSizingFlag>	If True then Preset gas volume else Calculate gas volume	Text
<CreatedBy>	Operator ID	Text
<UserDefinedField1>	Operator input to batch	Text
<UserDefinedField2>	Operator input to lot	Text
<UserDefinedLabel1>	Label for batch	Text
<UserDefinedLabel2>	Label for lot	Text
<RunNotes>	Operator comment input	Text
<TestPassed>	0 = Fail 1 = Pass 2 = No result 1 = Pass unless an enhanced test where TestPassed = 1 and SizeAtTemperature = 1	Number

Table Element	Element Description	Data Format
<TestStatus>	0 = OK 1 = General failure 2 = Failed precondition check 3 = Failed post condition check 4 = Parameter low range 5 = Parameter high range 6 = RPC failure 7 = RPC service not available 8 = Test execution general failure 9 = Test procedure not found 10 = Test version not found 11 = Test already running 12 = No test available 13 = Requested test not available 14 = Requested test data not available 15 = Test already Exists 16 = Leak detected 17 = Max time exceeded 18 = Max loss exceeded 19 = Out of calibration 20 = User aborted test 21 = Filter not found 22 = HC inputs not found 23 = Setup inputs not found 24 = Client log error 25 = Database unavailable 26 = User not found 27 = Incorrect password 28 = Server DB failure 29 = Test execution failure 30 = Hardware warming up 31 = Temperature probe error	Number

Table Element	Element Description	Data Format
<TestStatus> (cont.)	32 = Temperature change rate 33 = Replay OK Note: Some values do not apply to this implementation.	Number
<PressureUnits>	Interface setting: 3300 = PSI 3301 = Millibar 3303 = kPa	Number
<NResultsRows>	Number of TestResultsRow elements	Number
<SystemSize>	Measured Volume	Number
<SizeAtTemperature>	Size at temperature	Number
<Flowrate>	Flowrate	Number
<FlowRateAtTemperature>	Flowrate at temperature	Number
<FlowrateAtConst>	Flowrate at constant pressure	Number
<FlowrateAt20Min>	Flowrate at 20 minutes	Number
<ActualTestTemperature>	Temperature used	Number
<ActualTestPressure>	0 = no result	Number

TestResultsRow Table Element Sub elements

Element	Element Description	Data Format
<RowID>	Index	Number
<CreatedOn>	Key	Date and time
<Value1>	See Table Below	Number
<Value2>	See Table Below	Number
<Value3>	See Table Below	Number
<Value4>	See Table Below	Number
<Value5>	See Table Below	Number
<Value6>	See Table Below	Number
<Value7>	See Table Below	Number
<Value8>	See Table Below	Number

The contents of the values depend on the test type and phase of the test.

Element	Diffusion within Enhanced Bubble Point	Bubble Point	Diffusion or HydroCorr
<Value1>	-2000 = Code to Split Diffusion and Bubble Point Data	Pressure at which flowrate was calculated	Time (minutes)
<Value2>	N/A	Flowrate	Pressure at which flowrate was calculated
<Value3>	N/A	Temperature at which flowrate was calculated	Temperature at which flowrate was calculated
<Value4>	N/A	N/A	Flowrate
<Value5>	Time (minutes)	N/A	N/A
<Value6>	Pressure at which flowrate was calculated	N/A	N/A
<Value7>	Temperature at which flowrate was calculated	N/A	N/A
<Value8>	Flowrate	N/A	N/A

CalResults Table Element Sub elements




Element	Element Description	Data Format
All	N/A	N/A

Signatures Table Element Sub elements

Element	Element Description	Data Format
<CreatedOn>	Key	Date and time
<Signature1UserID>	User ID for first signature	Text
<Signature1FullName>	Full name for first signature	Text
<SignedAt1>	GMT time of first signature	Date and time
<Comment1>	Comment associated with first signature	Text
<Signature1Check>	Internal check for first signature	Number
<Signature2UserID>	User ID for second signature	Text
<Signature2FullName>	Full name for second signature	Text
<SignedAt2>	GMT time of second signature	Date and Time
<Comment2>	Comment associated with sccond signature	Text
<Signature2Check>	Internal check for second signature	Number
<NumSigsReq>	Number of required signatures	Number

Verifying External Resource Connection

Follow the steps below to test the connection of each external resource: report repository, backup repository, and printers.

1. Log in as an administrator.
2. Select the  **Instrument Management Tool**.
3. Select **Manage System Options** and press the  icon.
4. Press the  icon once to access the **External Resource Setup**.
5. To test the connection of the report repository to the instrument, select the **Report Repository** tab and press the **Test Connection** button to view any errors.
6. To test the connection of the backup repository, press the **Backup Repository** tab and press the **Test Connection** button to view any errors.
7. To test the connection of the printer, press the **Printers** tab and select desired printer. Under the **Printer** menu, select **Properties** to see if the printer is connected to the instrument.

Using ping and ipconfig

A network specialist can login as a SuperUser to manually troubleshoot any problem with the network and Integritest 4N Instrument using standard Windows tools such as ping and ipconfig.

Log File Entries

The SuperUser can access the log file entries via Notepad or Audit Viewer for additional information regarding network connections errors.

Unavailability of a Printer

Printer unavailability may be caused by an offline machine, empty ink cartridge or paper tray or other, similar problems, and may not be reported immediately if a print document is in the print queue. Delays in printing should be checked via the local IMT screen, where the printer queue will report an Error status if a printer is unavailable. Correct the error as directed, and the document will print.

Verifying Checksum Data

The Audit Viewer will automatically verify the checksum of those files that have them. Part of the checksum involves the file creation date. Different file systems associated with Windows use different methods to remember this time, such as local time or GMT. The relationship between the local time and GMT is critical for the checksum to be created or checked. If the time zone is set incorrectly, false positives on checksum errors may occur. Set all auditing computer time zones properly to avoid this problem.

Add Printer Dialog Window Disappears

During **Add Printer**, the **Add Printer** dialog box may disappear when the **External Resource Setup** window is accidentally accessed. The **alt** and **tab** keys on the onscreen keyboard may be used to cycle through the open windows and bring the user back to the **Add Printer** dialog box. Select the **alt** key and then the **tab** key as many times as needed to highlight the **Add Printer** icon, and then use the **alt** key to bring the window to the front.

Event Log Overwrites

The Windows event logs for Security, System, and Application are normally set to overwrite as needed. The Security log and the Application log are saved and emptied during a backup in the audit mode. The System log is not significant for 21 CFR Part 11, and is used to troubleshoot system hardware or software problems. Overwrite as needed is selected to avoid unwanted messages from the system that may appear if the logs were to fill up. It is recommended that occasional audit backups are performed to capture this information.

Central IMT Software

With the Central IMT software, issues can occur due to access or security concerns in the network. Review permission settings in groups and shared resources(printers etc.). Ensure Role server settings in Service PC and instruments are consistent.

Technical Assistance

For more information, contact the Millipore office nearest you. In the U.S., call **1-800-MILLIPORE** (1-800-645-5476). Outside the U.S., see your Millipore catalogue for the phone number of the office nearest you or go to our web site at www.millipore.com for up-to-date worldwide contact information. You can also visit the tech service page on our web site at www.millipore.com.

MILLIPORE

Millipore and Integritest are registered trademarks of Millipore Corporation. HydroCorr is a trademark of Millipore Corporation. Microsoft, Access, Excel, Windows, Windows NT and Windows XP are trademarks of Microsoft Corporation. Adobe and Reader are trademarks of Adobe Systems Incorporated.

0101797PU Rev B. 06/2007 © 2007 Millipore Corporation. All rights reserved.