FraudWatch version 3.5

Installation Guide

FraudWatch 3.5 Installation Guide

Documentation version 3.5

May 9, 2007

PN: 092006FW3.5/AG

Copyright

SAP - Important Disclaimers

Coding samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Internet hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint where to find supplementary documentation. SAP does not warrant the availability and correctness of such supplementary documentation or the ability to serve for a particular purpose. SAP shall not be liable for any damages caused by the use of such documentation unless such damages have been caused by SAP's gross negligence or willful misconduct.

Accessibility

The information contained in the SAP Library documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP specifically disclaims any liability with respect to this document and no contractual obligations or commitments are formed either directly or indirectly by this document. This document is for internal use only and may not be circulated or distributed outside your organization without SAP's prior written authorization.

Table of Contents

1

1 FraudWatch System Requirements

This chapter gives a brief introduction to the FraudWatch software, and outlines its advantages. Topics in this section include:

The role of a FraudWatch administrator

In addition to installing FraudWatch, it is the role of the administrator to add and maintain your organization's users and security clearance, create templates and refine the parameters by which FraudWatch operates to detect exceptions, and perform the required backup procedures necessary for system and data integrity.

It is assumed that FraudWatch administrators are familiar with the Transaction Log (TLog), the POS operations and its effect on the TLog, SQL database administration, and should have a working knowledge of the FraudWatch database.

Hosting FraudWatch

SAP provides the following options: you can have your FraudWatch system hosted by the SAP service if your company does not have the resources to run FraudWatch on site, or you can install and host FraudWatch at your site if you have the required IT infrastructure or if your corporate policy prohibits the release of transaction data to an external party.

System requirements for SAP-hosted installations

To subscribe to the SAP-hosted FraudWatch service, you will minimally require a PC with the following specifications:

- Pentium Processor, 512 MB RAM

- 15" monitor capable of 1024x768 resolution
- Mouse (wheel mouse recommended)
- Modem or LAN connection to the Internet capable of 56 Kbps
- Microsoft Windows 2000 operating systems, Internet Explorer 6.0 service pack 1 with 128-bit encryption is required.

System requirements for hosting FraudWatch at your site

System requirements for hosting FraudWatch at your site will depend on your expected transaction volume. The various FraudWatch components do not require excessive resources, however if your business normally produces high transaction volumes you will need to select equipment which can process high volume database files. The following table lists the minimum hardware and software requirements for hosting an Enterprise FraudWatch system at your site.

Pre-installation requirements

You must ensure that the following requirements are satisfied before installing FraudWatch.

- The Database Server is linked to the Administrative server.
- You are signed on as the Administrator for the server on which you are installing FraudWatch. This ensures that you have the appropriate authority level to run all jobs required to successfully install FraudWatch.
- Check that the SQL Server Agent service is installed and that the SQL server is running.
- You must ensure that the setting which allows you to log in using mixed mode is activated.
- Full Text Search SQL service is required for FraudWatch fuzzy searches. If this service is not installed, the FraudWatch installer will not allow you to proceed.
- The Microsoft Search service must be installed. This can be installed when you install SQL Server in Service Manager.
- Ensure that the role in SQL Server is **DB_owner** and the username is **sa**.
- An authentication server must also be installed.
- Select an SSL certificate provider. Your provider will supply you with the instructions on how to apply it to your website.
- The Java Runtime Environment 1.4.2 must be installed on your system.
- The latest version of DBTools must be installed on your system if you are doing an version upgrade.
- Sprinta2000.jar must be installed in C:\Program Files\Java\j2re1.4.2_10\lib\ext. before the installer is run. Inet Software Sprinta2000 driver can be obtained from:http://www.inetsoftware.de/

FraudWatch Components

FraudWatch component in required order of installation	Hardware and software requirements	What this component does
1. Admin server	Hardware requirements ■ Pentium IV processor with 128 MB RAM ■ 500 MB free disk space Software requirements ■ Windows 2003 Server, Service Pack 4 ■ Microsoft SQL Server 2000, Service Pack 3	■ Middle tier server ■ Contains business logic, .dll files ■ Manages user security and access rights ■ Performs some processing
2. Web server	Hardware requirements ■ Pentium IV processor with 128 MB RAM ■ 40 MB free disk space Software requirements ■ Windows 2003 Server, Service Pack 4 ■ IIS 5.0 Server Service ■ Microsoft SQL Server 2000 client connectivity	■ Front-end server ■ Handles requests from client; serves HTML pages and custom presentations
3. Database server	Hardware requirement ■ Pentium IV processor with 512 MB RAM minimally — 2 G preferred ■ Based on a metric of 30,000 txns/day each having an average of three items per transaction and storing two years worth of data, the hard drive requirement is expected to be 50G (plus or minus 20%) when the recovery option is set to 'simple'. Software requirements ■ Windows 2003 Server, Service Pack 4 ■ Microsoft SQL Server, Service Pack 3 ■ Raid5 is recommended for large databases	■ Back-end server ■ Mostly used for storage ■ Performs some processing and exception marking
4. Data loading server	Hardware requirements ■ Pentium IV processor with minimum 128 MB RAM ■ Disk space requirement depends on the size of transaction logs. Minimum suggested size is 2G Software requirements ■ Windows 2003 Server, Service Pack 4	■ Parallel to Admin server but independent from presentation server ■ Uploads and parses transaction files ■ Processes STIFF format files
5. DBtools	This utility should also be installed to assist with future upgrades.	

Configuring Windows Application Server

Several Componets must be added to Windows Application server configuration for Fraudwatch to run.

1. Click **Start/Control Panal/Add Remove Programs/Add Remove Windows Components/**
2. Check/Add the following components:
    - Information Services (IIS)
    - Message Queing
    - Network Services
3. Go to IIS Manager
    a) Step 1
        - Go to **Wed Service Exception**, highlight '**Active Server Pages'**
        - Click '**Allow'** button.
        - Click on **Fraudwatch**,
        - Select **Properties**
        - Go to '**Home Directory Tab'**
        - Click **Configuration**,
        - Select '**Enable Parent Path'** checkbox.
    b) Step 2
        - Go to **Wed Service Exception**, highlight '**Server Side Includes'**
        - Click '**Allow'** button.
        - Go to **Application Pools** and find the **Fraudwatch path**
        - Right click on the '**Application Pool**'.
        - Select "**Properties**..." from the pop-up menu
        - Go to the "**Identity**" tab.
        - Change the "**Select a security account for this application pool**:" to "**Predefined**"
        - Select "**Local System**" from the list
        - Click **OK**.

Note: Step 3 is only valid for IIS 6.0. IIS 6.0 has added new security protocols and the default differs from the previous versions. The web service exception is only valid in IIS 6.0. IIS 6.0 is only available on the windows Server 2003 Operating System (for the moment) Other Operating Systems such as Windows 2000 and Windows XP use IIS 5.0.

Configuring Java Runtime Environment 1.4.2

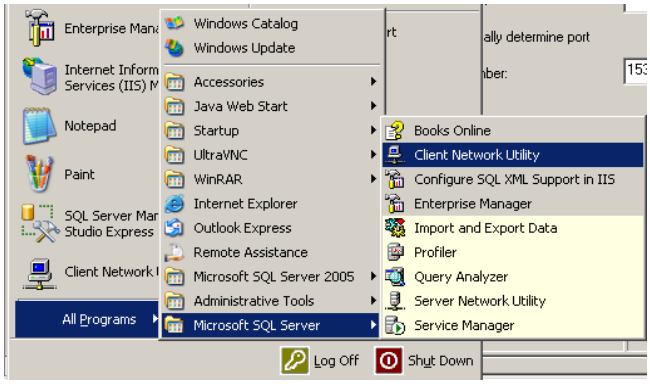
Install the Sun JRE 1.4.2 on the system if it isn't already present.

1. Copy the file bcprov-jdk14-xxx.jar to the JRE installation directory\lib\ext.
    - A typical JRE install location would look like C:\Program Files\Java\j2re1.4.2_10
    - You can obtain the latest bcprov-jdk14-xxx.jar from http://BouncyCastle.org.
    - Be sure you download the version intended for use with Java 1.4
    - The installation has been bench tested successfully with bcprov-jdk14-133.jar

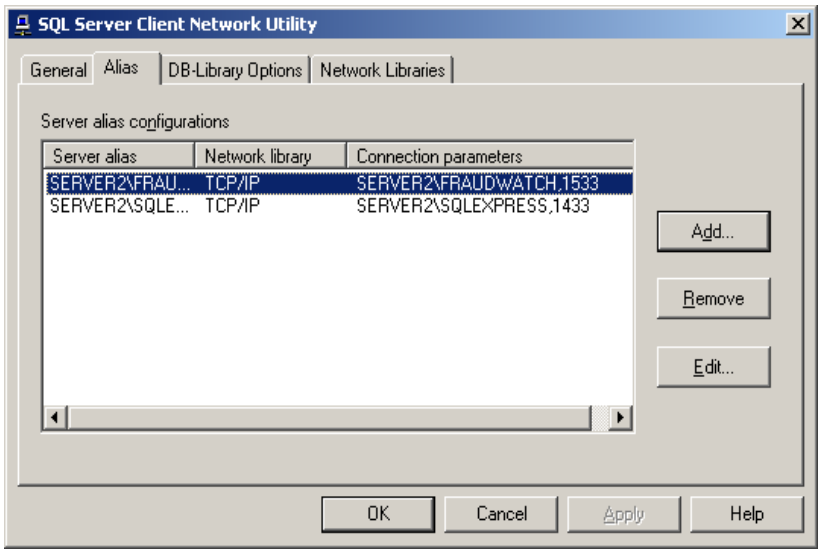
2. Copy these files to the JRE installation directory\lib\ext.
   - msutil.jar
   - mssql.jar
   - msbase.jar

Installing SQL Server or New Alias

1. Do a complete install of SQL Server
2. If SQL Server is already installed create a new instance.
3. Select **All Programs/Microsoft SQL Server/Client Network Utility.**

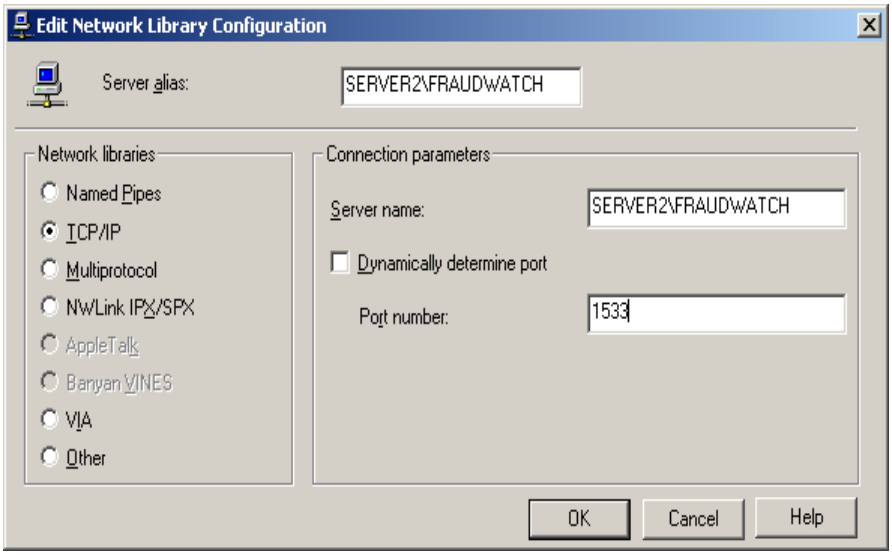


4. The SQL Server Client Network Utility window will open.



5. From the Alias Tab Click the **Add** button.

6. The Edit Network Library configuration window will appear.

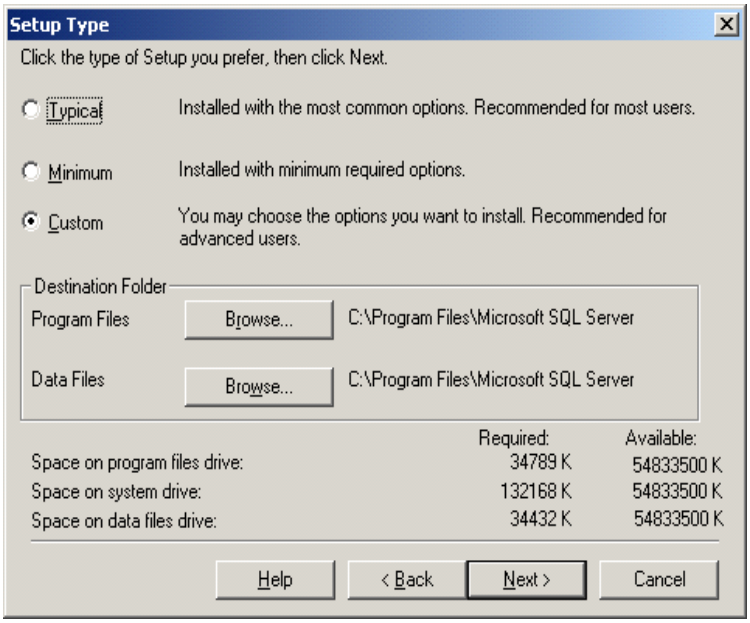


7. Enter server Alias and Server Name (must be the same).
8. Uncheck **Dynamically Determine Port.**
9. Enter new **Port Number.**
10. Click **OK**.

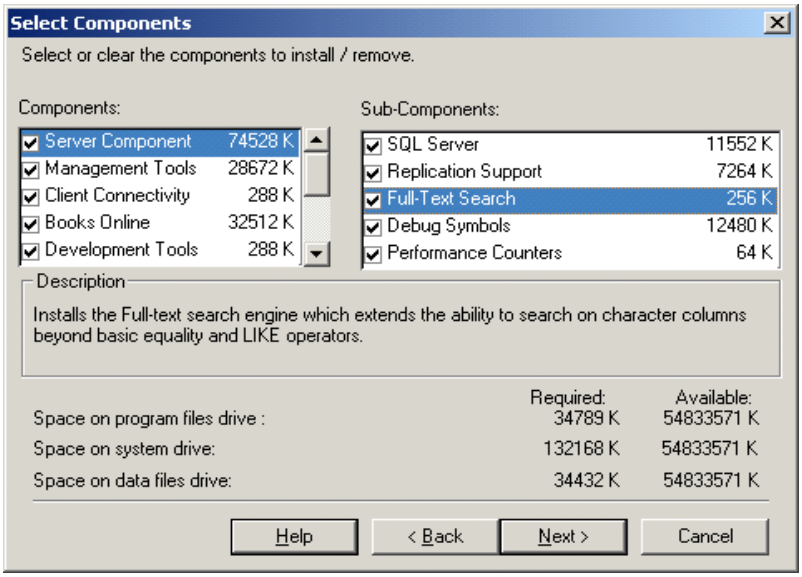
Configuring SQL Server

SQL Server setup must be customized before Fraudwatch 3.5 will run.

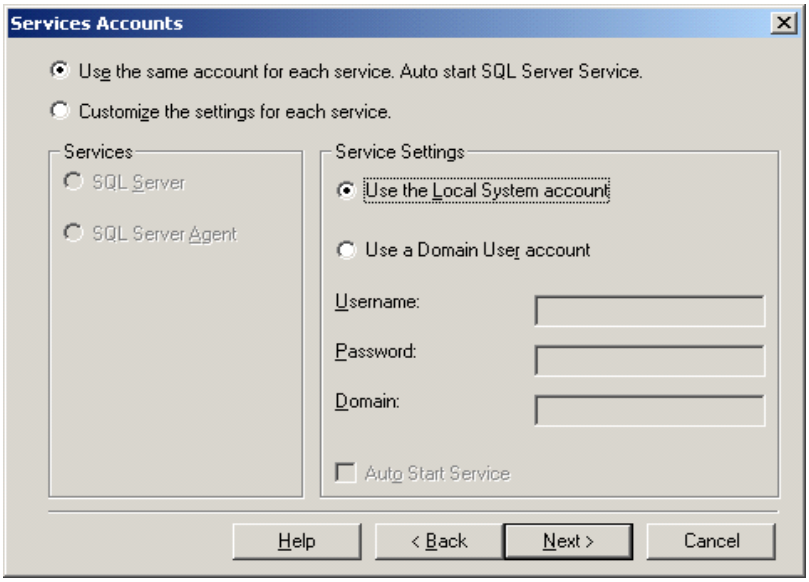
1. Choose **Custom** setup



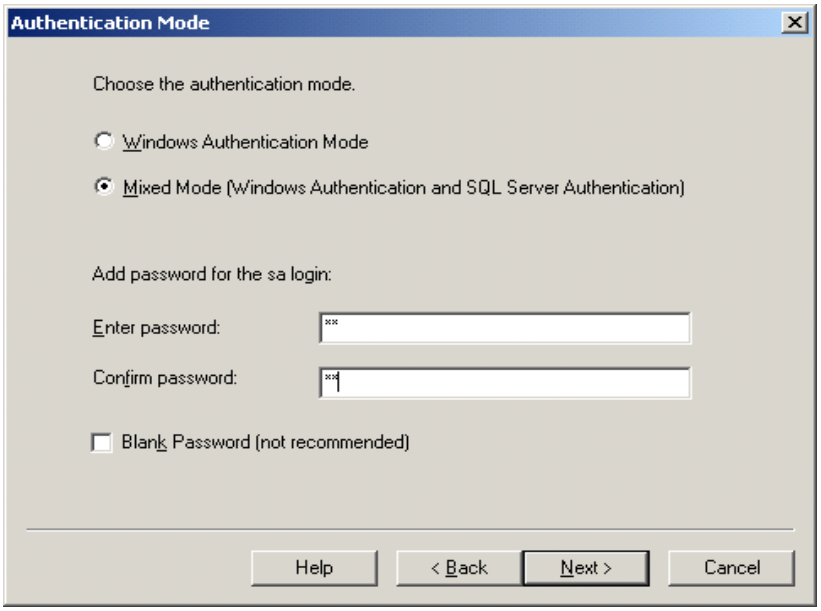
2. Make sure **Full-Text Search** is enabled



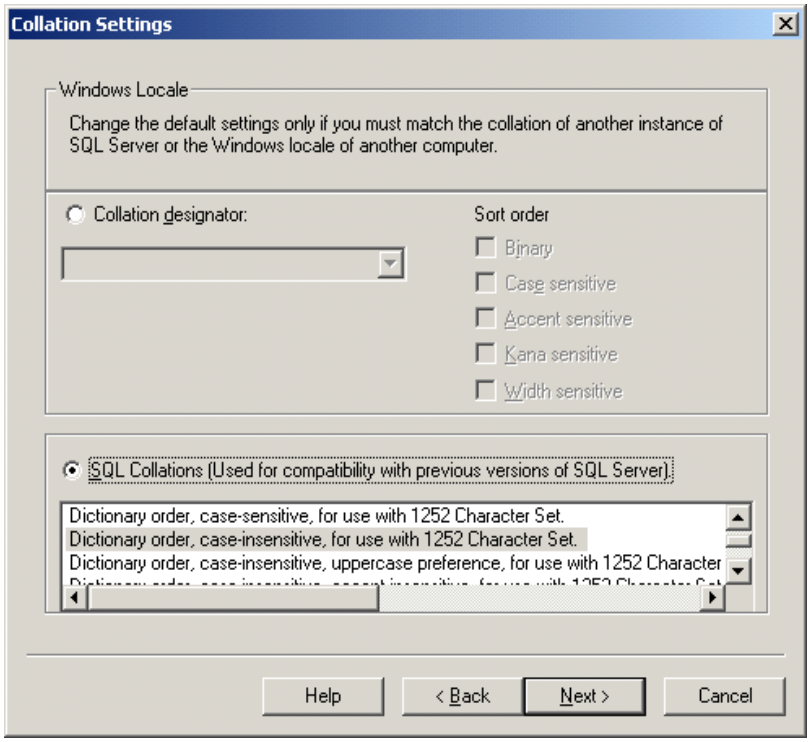
3. Setup the **Service Accounts** as follows:



4. Use the **Mixed Mode** for authentication.

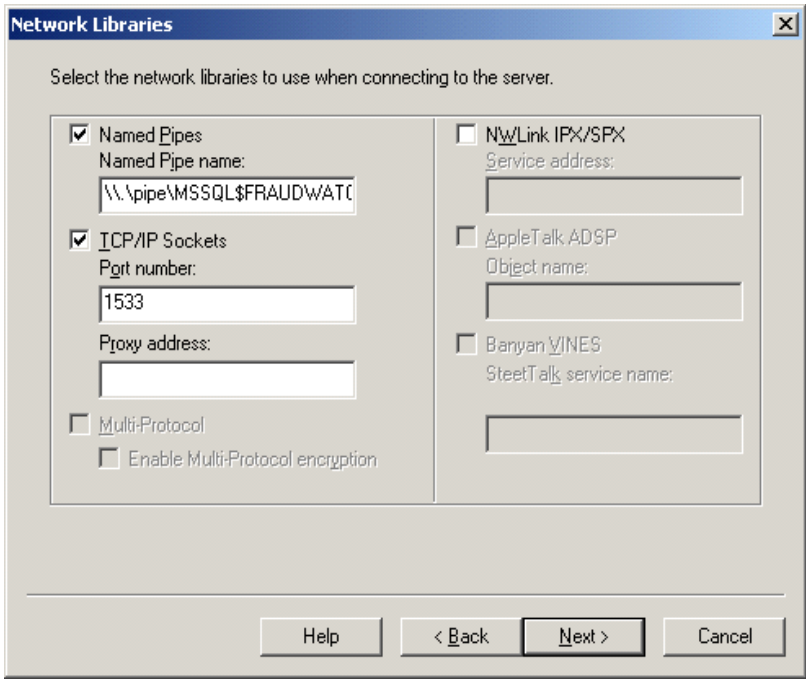


5. Chose **Dictionary Order, case-insensitive, for use with 1252 Character Set** as the collation.



6. Select a port for TCP/IP.

Note: FraudWatch does not support dynamic port assignment (port number 0)



Licensing and Registering Software

All pre-installed software required to host Fraudwatch 3.5 is to be installed and licienced by Client.

Getting Help

For FraudWatch support call 416-490-8199 or email questions to triversity@sap.com.

FraudWatch Installation

2

This section covers all the reports available in the FraudWatch system. Topics in this section include:

FraudWatch Installation

Required Information For Installing FraudWatch

Collecting Information for Checklist

7. Administrative and Client Data Base

   The default port is 1433 for a database that does not have an SQL instance.

   If there is an SQL instance, you can locate the port number in the SQL Server Enterprise Manager.

   a) Click **Start>Programs>Microsoft SQL Server>Enterprise Manager**.

   b) Double-click on **Server Network Utility**.

   c) Record instance name

   d) Right-click on **TCP/IP** in the Enable protocols window

   e) Record Port

8. Internet Data Base

   a) Click **Start>Cntrol Panel>Administrative tools**.

   b) Double-click on **Server Name**.

   c) Right-click on FraudWatch 3.5

   d) Right-click on **Properties**

   e) Record Web IP Address

   f) Record TCP Port

   g) Record SSL Port

9. All Additional information can be obtained from your IT Department

Complete the following Information Checklist before installing FraudWatch

Table 1: Information Checklist

Required Information	Details
Select Required Features Complete - Installs All Custom - Allows selected features	Fraudwatch Administrative Database:_____ Fraudwatch Client Database:_____ Fraudwatch Service:_____ Fraudwatch Data Load:_____ Fraudwatch Website:_____ Restore Exceptions:_____ Fraudwatch Documentation_____
Destination Directory	Installed on: __:\SAP\Fraudwatch_194
Administrative Database	Server Name:_____ SQL Port Number:_____
Database Server	Database Server Name:_____ Windows Authentication:_____ SQL Authentication:_____ Database Admin Login ID:_____ Database Admin Password:_____
Client Database	Client Database Name:_____ Port Number:_____ Hierarchy Level:__5___
Working Directory	Directory Location: __:\SAP\Fraudwatch_194\working
FTP Upload Directory	Directory Location: __:\SAP\Fraudwatch_194\working
Keystone Creation	New:_____ Existing:_____
Directory for TWSecurity	Directory Name:___:\WINDOWS\system32\TWSecurity.jar
Internet Services	Web Site IP Address:_____ IIS Server Name:_____ IIS Service Port Number:_____ SMTP Host Server Name:_____ SSL Port Number:_____

Installing FraudWatch

There are two instances when you may be required to run the FraudWatch installation process: you have newly subscribed to the FraudWatch service and are installing FraudWatch on your computer for the first time or you are currently running a version of FraudWatch and need to install an upgrade.

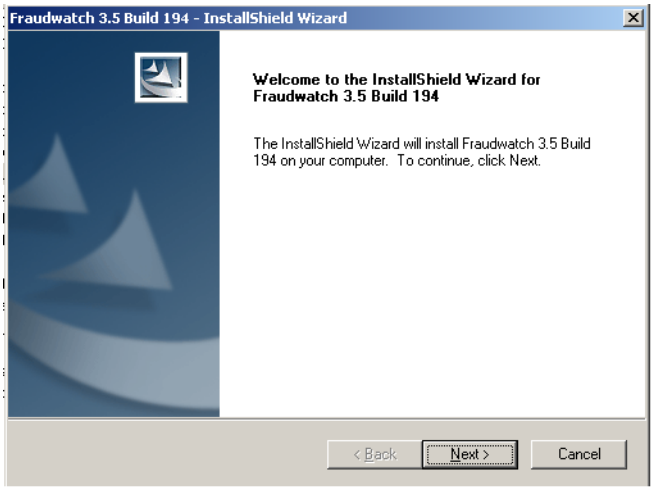
The following sections describe the required steps to install FraudWatch on your system for the first time. To perform an initial FraudWatch installation, you will receive an installation CD containing the following files: media.inf, setup.jar, FraudwatchInstaller.exe, version.ini.

A complete installation involves the following main steps:

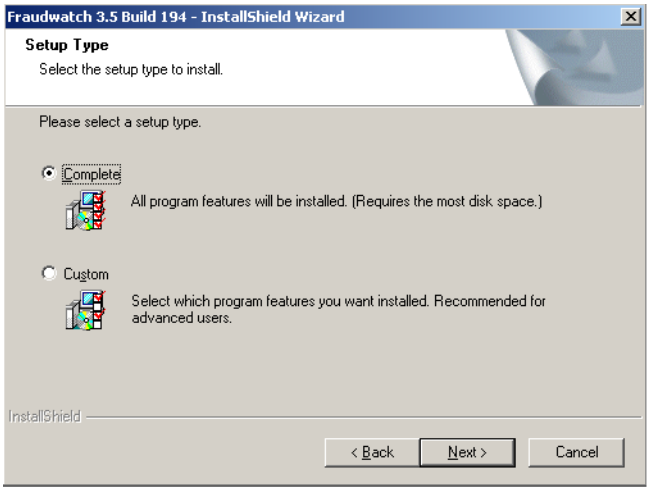
- Install the FraudWatch software from the CD
- Check that the Web server is operating properly
- Load data and check the data load log. For instructions on checking the data load log, see.
- Configure and run the first job to ensure the process is set up according to your requirements. For instructions on creating, configuring and running jobs, see.

To Install FraudWatch at your Site (Complete Install):

1. Insert the installation CD into your PC and run the *FraudwatchInstaller.exe* file from the CD. This executes the InstallShield Wizard that installs FraudWatch. The InstallShield presents various windows in which you will need to enter details about your system from the Information Check List to properly set up and map the FraudWatch components.



2. Click **Next** to continue the installation process.
3. Click the radio button adjacent to the **Setup Type** that you want to install.

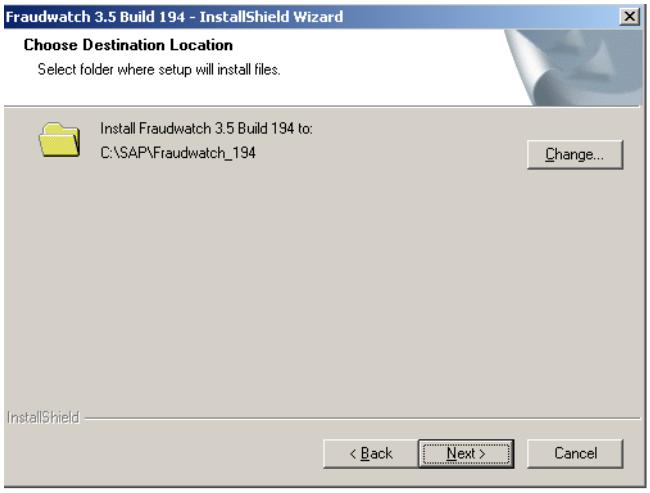


- The *Complete* installation installs all of the FraudWatch components on your system.
- If you have selected a **Custom** installation, you will need to specify the FraudWatch components to install at this time.

Note: The Custom installation options are for expert users who are familiar with all of the details of the FraudWatch system.

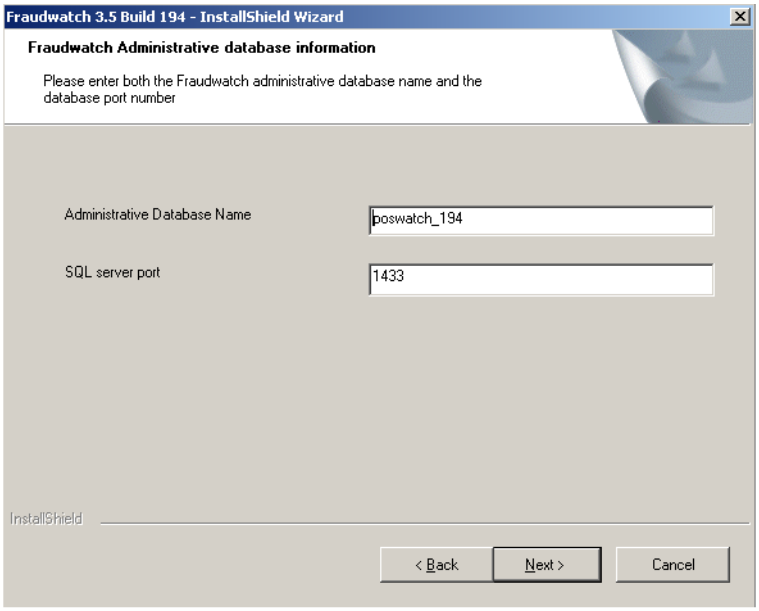
---

4. Click **Next** to continue the installation process.
5. Choose the **Destination** where Fraudwatch is to be installed.



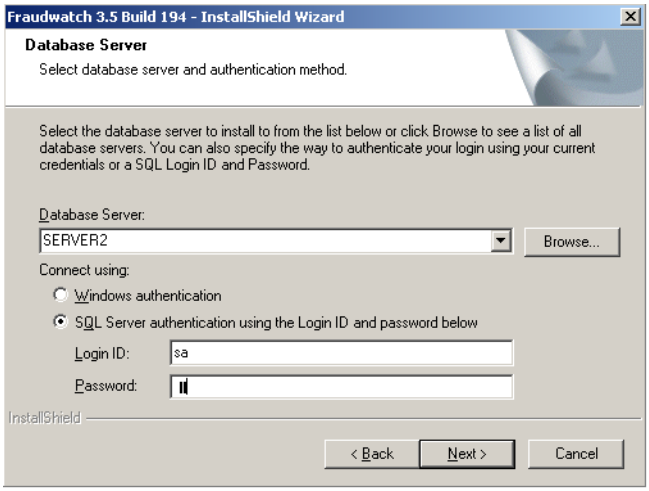
- Use the default location or click **Change** and choose another location and/or file name.

6. Click **Next** to continue the installation process.
7. Enter the FraudWatch **Administrative Database Name**. This information is used to set the SQL connection parameters.



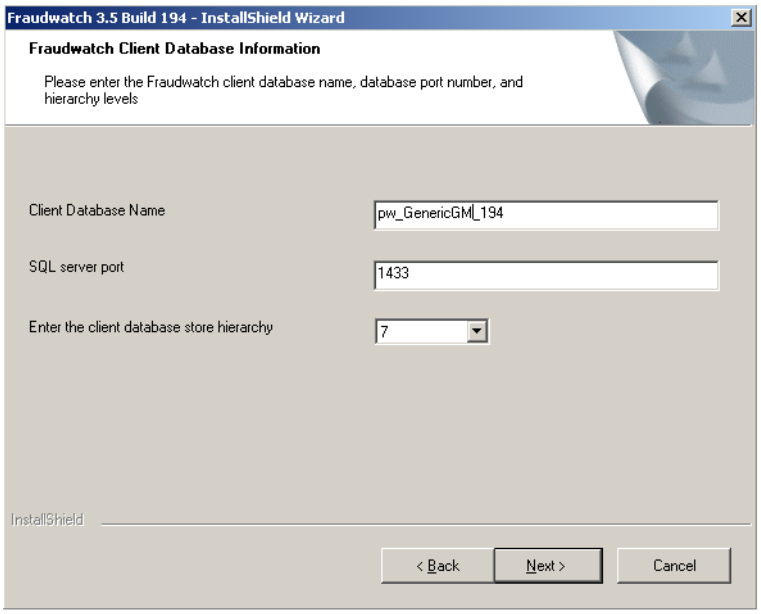
- Enter the **Database name**. The default Database server name is the current (local) system. If installing the Administrative component, this should not be changed. (Components cannot be installed to remote systems.)
- Enter the **Port number** that the SQL server listens to. The default port is 1433 for a database that does not have an SQL instance.

8. Click **Next** to continue the installation process.
9. Specify the **Data Base Server**.



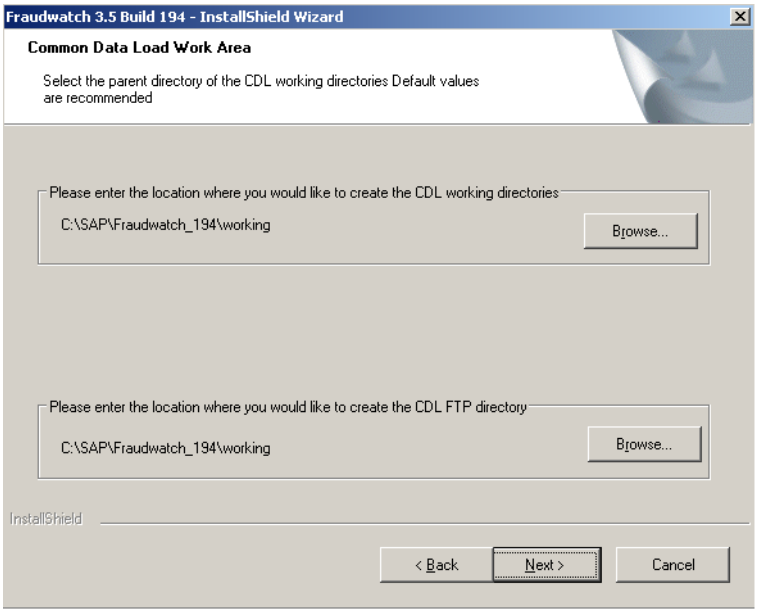
- Enter the **Database Sertver** or Click Browse and select a server connected to system.
- Do not select Windows authentication radio button
- Enter the **Database administrator login ID** and **Password** you use to log on to the SQL server. This user ID should also have system administrator rights.

10. Click **Next** to continue the installation process.
11. Enter server information for the FraudWatch **client database name**.



- Enter the **Database server name** for the client.
- Enter the **Port number** that the SQL server listens to. The default is 1433 for a database that does not have an SQL instance.
- Enter the number of **Hierarchical** retail levels in your organization. This sets up the structure for transaction summary data. Note that once the number of levels is set, it cannot be increased or decreased within the application.

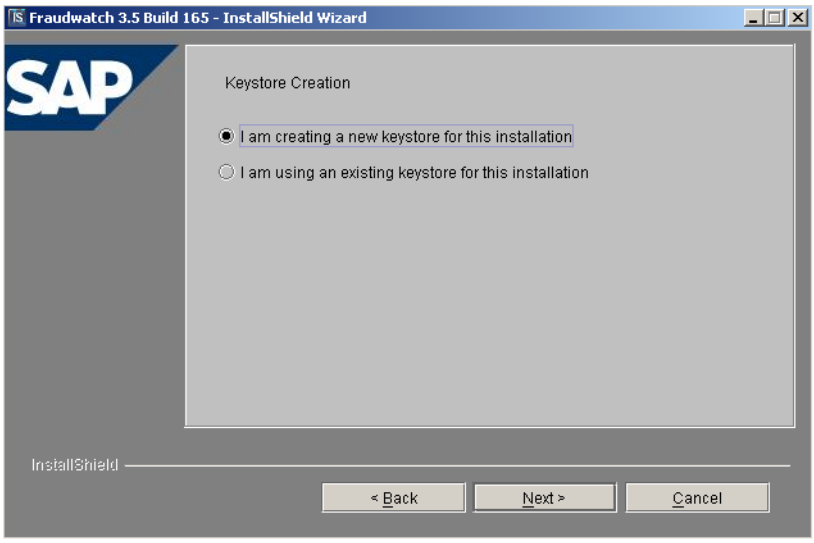
12. Click **Next** to continue the installation process.
13. Specify the **directory name and location** where FraudWatch program files will be located.



- Use the default CDL working directory as shown or click **Browse** and choose another location and/or file name.
- Use the default CDL FTP directory as shown or click **Browse** and choose another location and/or file name.

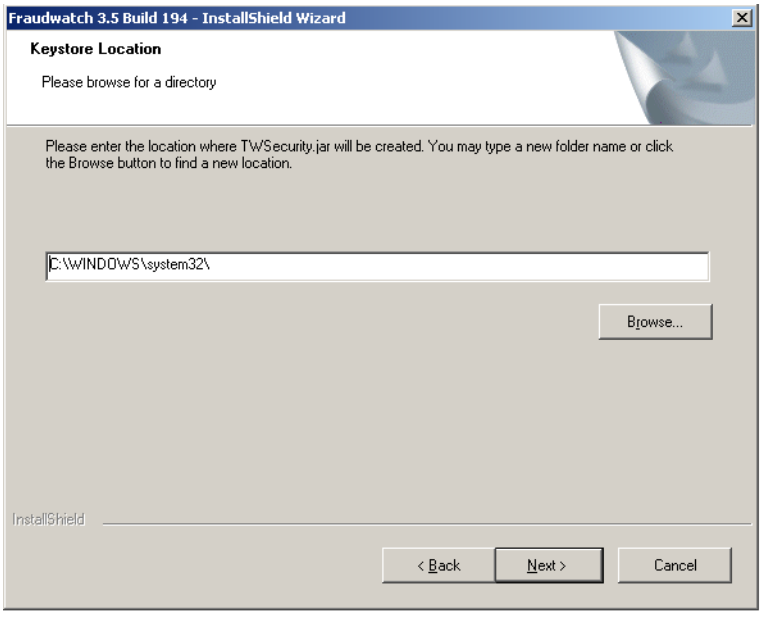
14. Click **Next** to continue the installation process.

15. Select whether or not you want to create a new keystore at this point or use an existing keystore.



- A keystore can be a file or a registry setting that stores the keys that are used for decrypting data.
- If you choose to use an existing keystore, the InstallShield Wizard will allow you to retrieve the key from the location where it is stored on your computer.

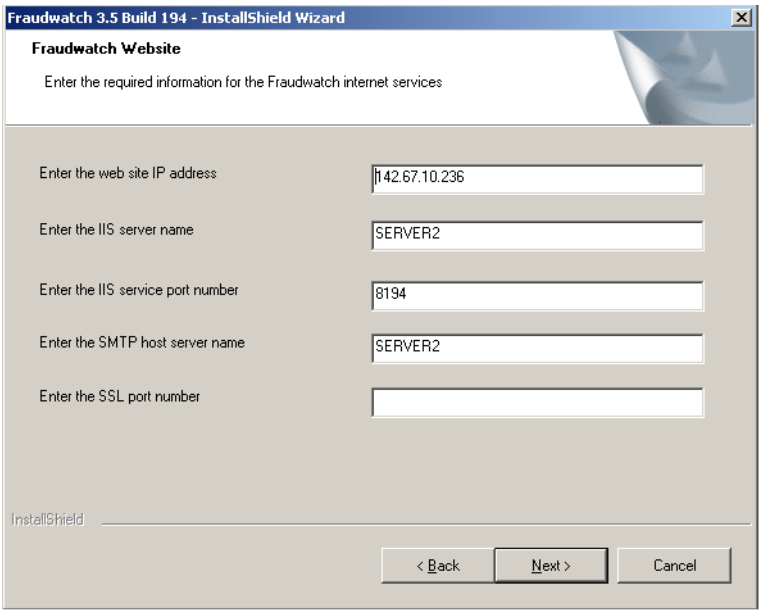
16. Click **Next** to continue the installation process.
17. Select the directory in which to install the TWSecurity.jar file. The TWSecurity.jar file is a keystore file for the Java version of TWSecurity, which is a Triversity utility for encryption and decryption.



- Use the default directory as shown or click **Browse** and choose another location and/or file name.

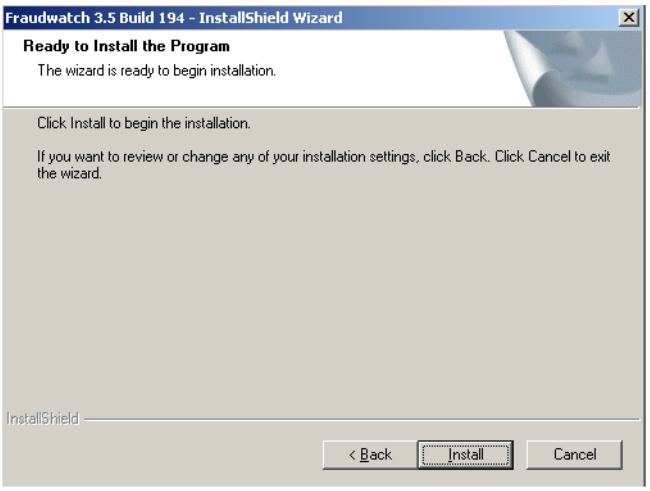
18. Click **Next** to continue the installation process.

19. Enter internet information for the FraudWatch **Internet Services**.



- Enter the **Wed Site IP Address**.
- Enter the **IIS Server Name**.
- Enter the **IIS Service Port Name**.
- Enter the **STMP Host Server Name**.
- Enter the **SSL Port Number**

20. Click **Next** to continue the installation process.



21. Click **Install** to continue the installation process. As the installation executes, several windows will open and close.
22. When all the system files are successfully installed, click **Finish** to exit the InstallShield Wizard.

To install FraudWatch at your Site (Fraudwatch Only):

1. Install new Instance of SQL Server.
2. Fill out Information Checklist for new Instance.
3. Insert the installation CD into your PC and run the *FraudwatchInstaller.exe* file from the CD. This executes the InstallShield Wizard that installs FraudWatch. The InstallShield presents various windows in which you will need to enter details about your system from the Information Check List to properly set up and map the FraudWatch components.

To install FraudWatch at your Site (Version Upgrade):

Note: The test feature of the Custom Query will not be available for upgraded database.

Backup

1. Stop Fraudwatch service from Windows Services.
2. Detach Client Database.
3. Detach Postwatch Database.
4. Backup both databases.
5. Reattach Poswatch database.
6. Reattach Client database.

Upgrade the database using DBTools

1. Create ODBC data source for Postwatch and client databases.
2. Create registry keys for postwatch and client databases under HKEY_LOCAL_MACHINE\SOFTWARE\Trimax Retail Systems Inc.\Application Databases.
3. After the above steps, the user should be able to select the postwatch or client databases in the DBTools' dropdown list.
4. Copy tmx_db03000x2_to_030502.zip to C:\Program Files\DBTools of upgrading postwatch database.
5. Run DBTools, select the poswatch database and connect to it.
6. Select Upgrade from the Tools menu.
7. Click Start

Note: If DBTools complains about the version, rename the file totmx_db300x2_to_030502.zip.

Note: The x is the number sequence in the sub-version, for example, the file FW 3.0.8 is tmx_db300082_to_030502.zip.

---

8. Copy tmx_db03000x_to_030500.zip to C:\Program Files DBtools for upgrading client Database.
9. Run DBTools, select the client database and connect it.
10. Select Upgrade Database from the Tools Menu.
11. Click Start.

Note: The x is the number sequence in the sub-version, for example, the file for FW 3.0.8 is tmx_db30008_to_030500.zip

Note: The client upgrade will fail and error message will appear.

12. Close DBTools.
13. Open the zip file, tmx_db03000x_to 030500.zip. there should be a file update_backoff_030500.zip
14. Open the zip file BOcomp1.zip and extract the SLQ file sp_pr_GetTxnlogWithExcR10.sql.
15. Run MS SQL Query Analyzer, execute sp_pr_GetTxnLogWithExcR10.sql.
16. In the zip update_backoff_030500.zip, there should be a file update_backoff_030500.sql.
17. Locate the update statement at the bottom of the file. Copy it and apply it to the client database by using the MS SQL Query Analizer.
18. Rename the zip file to tmx_db_030500.zip.
19. Run DBTools, select the client database and connect it.
20. Select Upgrade Database from the Tools menu.
21. Click Start. The process should skip all scripts that applied previously and apply the rest of the remaining scripts.
22. After the Upgrade process, check the Client Database, if any of the tExcTxnNNN tables do not have the column excCount, extract the scripts al_tExcTxn01.sql and dat_tExcTxn01.sql from BOcomp1.zip mentioned in Step 15 above. Run MS SQL Query Analizer and exicute al_tExcTxn01.sql.

Install FraudWatch 3.5

1. Detach Client Database.
2. Detach Postwatch Database.
3. Install FraudWatch 3.5 using the same poswatch and client database names as old version.
4. When the installer prompt for the Security Key File, use the existing one from the old version, which can be found under the System32 directory under the Windows directory. The file name is TWSecurity.jar.

Post Installation of FraudWatch 3.5

1. Copy the Config\all\thirdParty directory from the old version to the new version.
2. Copy the config\demo directory from the old version to the new version.
3. Copy the working\demo directory from the old version to the new version.
4. You may need to modify the following files in the cinfig\demp directory manually to match the new enviroment by changing the directory name if you install FraudWatch 3.5 to a directory different from the old version:
   - autostore.bat
   - autorestore_u.bat
   - cdl.properties
   - demo.xml
   - logging.properties
   - pipline.bat

Note: The reference to “demo” in steps 2,3 and 4 should be replaced with the corresponding retailer’s banner.orname.

5. Stop the FraudWatch service from the Windows Services.
6. Detach the new databases created by FraudWatch 3.5 installer.
7. Stop the Microsoft Search service from the Windows Services.
8. Move the database directory to another location for backup.
9. Copy the database directory that contains the updated client database from the old installation to the new.
10. Copy the FW_Admin directory that contains the updated poswatch database from the old installation to the new.
11. Start the Microsofy Search Services.
12. Attach the upgraded poswatch database.
13. Attach the upgraded client database.
14. Start the FraudWatch service from Windows Services.
15. Start the Fraudwatch 3.5 web application.
16. Upload the logo of the company.

Distributing Fraudwatch across two or more servers

There are different permutations of the install. If desired, the Administrative Database and Client Database can be installed on the same server, with the Fraudwatch website installed on a second server

Since the Fraudwatch administrative and client databases are restored from backup sets, these steps must be taken on separate servers.

1. Start the installer and choose Custom install.
2. Choose the Administrative Database and Fraudwatch Service components.

Note: The administrative database must be installed first. It may be installed on a database server from a previous installation or installed from scratch.

Dependencies

The Fraudwatch service must be installed along with the Administrative database. If the component isn't automatically checked, please choose the Fraudwatch service component from the Custom install screen.

3. After the installer starts, fill in the pertinent information in the dialog boxes.
4. Next, take the install CD over to the second server.
5. Start the installer again, choose Custom install, and then check the client database box.
6. It is also highly desirable to choose the Restore Exceptions component while installing the client database.
7. After the installer starts, fill in the pertinent information in the dialog boxes.
8. The client database must "know" where the administrative database is located. Fill in the database information asked for. The CDL, or datload component will automatically be chosen while doing this.
9. Let the installer complete the installation.

10. Client Database Dependencies - the CDL, or dataload component requires that TWSecurity is installed to encrypt sensitive data as it is loaded client database. The installer should automatically ask for Twsecurity information.
11. The Fraudwatch website can be installed on either database server, or a third server.
12. Once again, take the install CD, start the installer, and choose the Fraudwatch Website component, and follow along filling the required information in the dialog boxes.

    Website Dependencies:

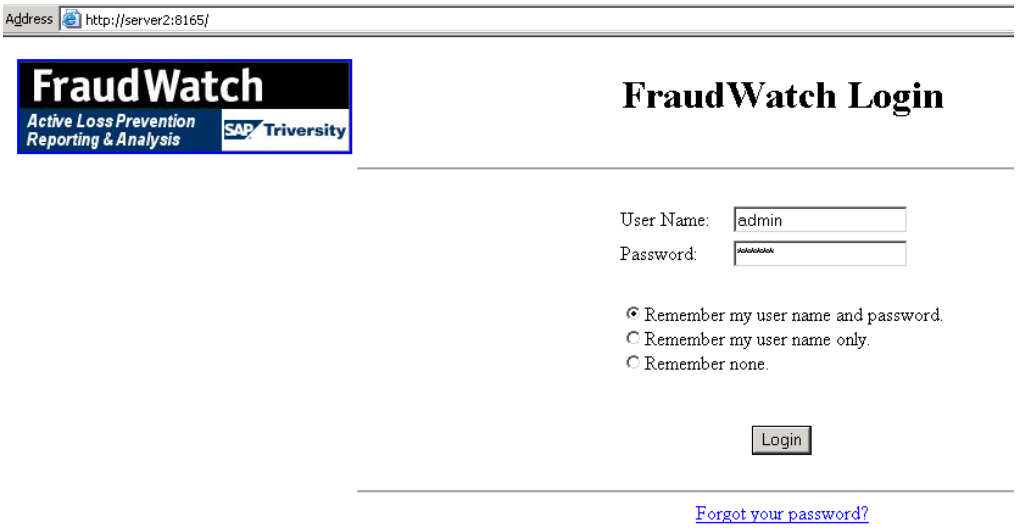
    TWSecurity is required to decrypt sensitive information to users with a high enough security clearance. The Website also needs to "know" where the Administrative Database is installed.

Initial Default Login

After a Complete install of FraudWatch you will be able to Login to the Default SuperUser created automatically when FraudWatch is installed.

Using Default Port #80

1. Enter url: **http://localhost:Port**
2. Click **Go** or press **Enter**.



3. Enter Login Information
   - User Name: **admin**
   - Password: **123456**
4. Click Login

Using Different Port e.g. #8080

1. Enter url: **http://localhost:8080/**
2. Click **Go** or press **Enter**.
3. Enter Login Information
   - User Name: **admin**
   - Password: **123456**
4. Click Login.

FraudWatch Configuration

3

The section describes FraudWatch exception parameters, exception schemes, and email alerts. In this section, you will find the following topics:

Configuring Fraudwatch

Download SQL Server 2000 Driver for JDBC Package

Three files for the Microsoft SQL Server 2000 Driver for JDBC package must be downloaded.before Fraudwatch 3.5 will run.

1. Microsoft SQL Server 2000 Driver for JDBC can be obtained from:http://www.microsoft.com/. Download the following three files required for the Microsoft SQL Server 2000 Driver for JDBC package.
    - msbase.jar
    - mssqlserver.jar
    - msutil.jar
2. Place them in: **C:\Fraudwatch_Install_Location\config\all\lib\ext**

Because of dependencies of the Fraudwatch service on these files, the installer will no longer automatically start the service. Please start the service manually after placing these jar files in place, or simply reboot the system.

If starting the service manually: From the **Start->Programs->Administartive Tools >Services,** find the **Fraudwatch_xxx** service in the list of services, and **Start** the service.

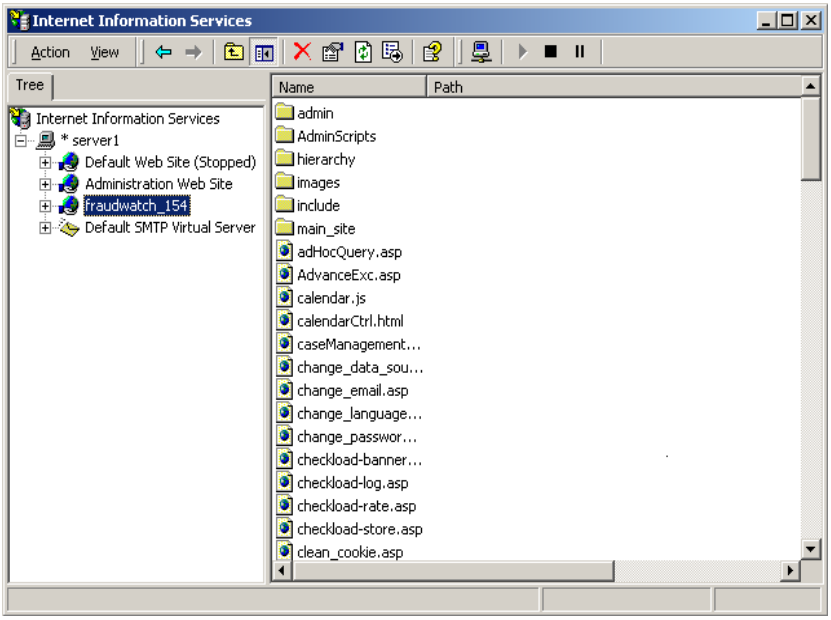
The service will always start by itself upon reboot.

Checking the web server

This step is recommended to ensure that the FraudWatch website can be browsed correctly.

To check the web server setup:

1. In the Windows task bar, click **Start** > **Programs** > **Administrative Tools** > **Internet Services Manager**.



2. Click on the web server name, then right-click on the host server (i.e. fraudwatch_xxx) and select **properties**.
3. Confirm that the TCP Port number is the same as the one you just used during the installation of the FraudWatch software. For example, the default number 80.
4. Highlight the host server and select **Browse**. The Login window appears confirming that the web server is running.

Loading data

In order to keep your transaction data current you must copy your TLog data to your FTP server.

loading your transaction data:

- Copy your daily transaction data to TriversityInc\Fraudwatch_xxx\working*clientname*\ftp.

Note: If you encrypt your data, then you should set up decryption keys according to your system setup.

---

1. Open a DOS box and go to the TriversityInc\Fraudwatch_xxx\config*clientname* directory. At the prompt type **>pipeline** and press the **Enter** key. The data loading begins.
2. When the process is complete, click the **Transactions** tab in the main FraudWatch window and check for sales data.

A default administrator user name and password are provided with FraudWatch upon installation. It is recommended to change this default password after installation. For more information on changing passwords, see.

If your FraudWatch system is being hosted by a Triversity ASP, your administrator User Name will be provided by Triversity. If FraudWatch has been installed at your site, the default administrator User Name is "admin." The administrator Password will generally be 123456 by default. You should change it to a unique password after logging on for the first time.

Configuring the communication ports

The following is a list of ports you may need to configure when installing FraudWatch. Port users are defined through the standard Microsoft server configuration utility.

Port number	Protocol	Description
21	FTP	file transfer protocol; used for uploading transaction files
80	HTTP	hyper text transfer protocol; used to access the FraudWatch web application
443	S-HTTP	protocol for securely transmitting data via the Internet
990	SFTP	secure file transfer protocol; used for securely uploading data
1433	TCP/IP	transmission control protocol/internet protocol; used by application server to access the SQL server (internal function)

User preferences

The User Preferences tab is where you define data sources, set up user e-mail addresses, change language settings and passwords, and clean cookies. When you click User Preferences, the following list of options appears:

- **Change Data Source**
- **Change Email Address**
- **Change Language Setting**
- **Change Password**
- **Clean Cookie**

For more information on User Preferences, see *FraudWatch Administration Guide*.

Check data load

As the administrator, you can check the data load for all stores, a single store, or the entire organization. When you click Check Data Load you are also presented with the opportunity to check the data load rate and view the data load log for a given period. When you click Check Data Load, the following list of options appear:

- **All Stores**
- **Single Store**
- **Banner**
- **Data Load Rate**

- **Data Load Log**

For information on the check data load options, see *FraudWatch Administration Guide*.

FraudWizard

FraudWizard allows users to create and run schemes and alerts. When you click FraudWizard, the following list of options appear:

- **Credit Card Alert**
- **Customer Information Alert**
- **Control Panel**
- **Run Scheme**

For more information on FraudWizard, see *FraudWatch Administration Guide*.

The maintenance tab

The Maintenance tab is where most of the administrative functions are performed. This is where you set up everything from new users and hierarchy groups, to creating new exceptions and jobs. When you click the Maintenance tab, the following list of options appear:

- **Customer ID Type**
- **Hierarchy**
- **Hierarchy Groups**
- **Tender Type**
- **Transaction Type**
- **Data Sources**
- **Password Functionality**
- **Users**
- **Jobs**
- **Country Setting**
- **Edit Exception Parameters**
- **Create New Exception**
- **View Error**
- **Update Store Operating Hours.**

For more information on Maintenance, see *FraudWatch Administration Guide*.

Glossary

This glossary contains definitions and synonyms for a variety of retail and FraudWatch specific terms and jargon.

ASP

ASP stands for *Application Service Provider*; an Application Service Provider hosts Web-based applications under secure conditions. All server hardware and functionality is located at the host.

Banner

A *banner* is a chain of stores, or a collection of chains owned by a single corporation.

Client Card

A *client card* is a card number used to identify a customer uniquely in a transaction. This can be a retailer-specific loyalty program, or cross-retailer program such as AirMiles (Canada) or Flybuy (Australia).

Discount

A *discount* is a reduction of value, expressed as either a percentage or dollar value, typically initiated by the cashier during the transaction.

Drilling down

To *drill down* is to search through information from a very high level to ever increasing layers of details.

Entities

Each hierarchal level of the retail organization is an *entity*. The company, region, store, and cashier are all entities used for determining what data level is to be searched for and reported upon.

Exceptions

An *exception* is a set of conditions within a transaction, or a series of transactions, that represents a violation of business policy related to fraud.

Fuzzy search

A *fuzzy search* is a multiple/variable parameter search that allows you to search the alpha-numeric information in your point of sale transaction data. For example, if you have the name, address, or phone number of someone making fraudulent returns, you can use the fuzzy search to quickly bring up all their transactions.

The Fuzzy Search uses information that is often collected when a customer makes a return. In cases where someone is using multiple names, addresses, and phone numbers, the fuzzy search can create new leads to investigate.

Host

A *host*, in computer terms, is a main or central system on which core server functionality and database information resides.

Item discount

An *item discount* is a discount applied by the cashier to an individual line item in the transaction.

Line void

A *line void*, also referred to as a *line item void*, removes a single line from a transaction after it has been entered by a cashier.

Orphaned

An *orphaned* refund/post-void is a refund/post-void performed before/after a lengthy period of register inactivity. This exception is useful for retailers with front end cash lanes and steady traffic flow.

Post-void

In retail terms, a *post-void* is a post-transaction void transaction. In loss prevention terms, this is typically a case in which a cashier rings in a transaction, fails to give the customer a receipt, and then voids the transaction and keeps the cash.

Price override

A *price override* occurs when a cashier overrides the item price that is provided by the POS.

Refund

Also referred to as a *return*, a *refund* is a transaction in which goods are returned to the store, and funds are given back to the customer.

Register over

A *register over* occurs when there is an excess of funds when the register is balanced against the total sales registered.

Register short

A *register short* occurs when there is a shortage of funds when the register is balanced against total sales registered.

Sale

A *sale* is a transaction in which goods or services are exchanged for funds.

Scheme

In FraudWatch terms, a *scheme* is a set of exceptions defined by a loss prevention investigator, to produce investigative reports for tracking down fraud and theft.

Self authorized

Retailers tend to restrict certain transactions, such as refunds and post voids, to management only. As a result, the POS requires a manager's authorization or override when a cashier initiates a restricted activity. When the manager processes a restricted transaction, the transaction is said to be *self authorized*.

Shrinkage

Shrinkage represents the difference between the actual inventory on hand and what it should be according to purchase and sales records.

SKU

A SKU is a *Stock Keeping Unit*, a number attached to an item for inventory tracking purposes. It can contain style, color, and size information, and so forth. Note that the SKU serves a similar, but distinct, purpose from PLU (*Price Look-up*) and UPC (*Universal Pricing Code*) numbers.

TLOG

TLOG stands for *Transaction Log*; a TLOG is a record of all transactions, a binary file containing all information processed through each register at the POS.

Transaction discount

A *transaction discount* is a reduction applied to the total value of the transaction, expressed as either a percentage or dollar value. Depending upon the POS, the discount will either be a lump sum value, shown as a separate line item in the transaction, or will be pro-rated against all the items in the transaction.

Void

A cancellation of a sale before or after it has been completed, typically within the transaction itself. A *transaction void* or *transaction cancel* refers to the void of an entire transaction. A *line item void* refers to a void of a single item within the transaction. If a void occurs after the transaction has been completed and tendered, it is referred to as a *post void* or a *manager void*.

Index