Installation & Configuration Guide for Auto Updater 1.0, SigmaSafe & Interface Local Agents

DOCUMENT OVERVIEW

This document will provide the necessary steps to install the SigmaCare Auto Updater 1.0, Legacy and Passthrough Local Agents and the SigmaSafe 5.5 Local Agent software. The Auto Updater is a critical component that will enable the software to be updated remotely and automatically without any manual operations.

PROCESS OVERVIEW

1. **Perform SigmaCare Setup**
    a. Setup SigmaCare Setup
        i. SigmaSafe
            1. SigmaSafe Instance
            2. System User
        ii. Interfaces
            (Legacy and Passthrough Agents)
            1. System User
            (Passthrough Agent Only)
            2. Vendor
            3. Vendor Interface
                a. Code Crosswalk
                b. Policies
2. **Create Configuration Using Utility**
3. **Deploy Configuration File (XML) to Production**
4. **Install Auto-Updater & Setup Service Manager**
    a. Specify Account Code
    b. Specify Authorization Code
    c. Start Service Manager Service

PREREQUISITES

Section estimated time for completion 5-30 minutes.

There are several items which are necessary to perform the installation of the SigmaCare Auto Updater 1.0 any of the associated applications. These items must be completed or obtained before the proceeding to the next section of this process.

1. Obtain the following software:

- SigmaCare AutoUpdate.Configuration.Creator (location: https://it.sigmacare.net)
- SigmaSafe Auto Updater (MSI Only) (location: https://it.sigmacare.net)
- Microsoft .NET 4 (**dotNetFx40_Full_x86_x64.exe**)
  http://go.microsoft.com/fwlink/?LinkId=181013

2. Uncompress the SigmaCare Auto Updater solution to a local host machine. (example C:\AutoUpdater)

3. Verify you have a method to connect remotely to the target computer and have the ability to copy files from your local machine to the target computer. A remote connection is necessary to perform the installation of the Auto Updater and SigmaSafe solutions.

4. Ensure the target computer can access the web URLs listed below. These URLs are needed for the ability for the Auto Updater to connect from the target computer to our Data Center. If the associated URLs are being blocked by the Account's Firewalls, ensure their IT staff is alerted to unblock these domains.

NOTE: You only need to test the URL's associated with applications that you are installing below.

Auto-Update

- https://updater.sigmacare.com/AutoUpdate/AutoUpdateService.svc

SigmaSafe

- https://safe.sigmacare.com/SigmaSafeRouting/

Legacy Local Agent

- https://interfaces.sigmacare.com/sigmacarewebservices/ResidentUpdateservice.asmx

Passthrough Local Agent

Inbound

- https://interfaces.sigmacare.com/SigmaCareWebServices/InboundADTWebService.asmx

Outbound

- https:// interfaces.sigmacare.com/SigmaCareWebServices/ResidentNotificationService.asmx

5. Supported Operating Systems for the computer that the Auto-Updater will be installed on are: Windows 7; Windows Server 2003 Service Pack 2; Windows Server 2008; Windows Server 2008 R2; Windows Vista Service Pack 1; Windows XP Service Pack 3. These requirements are due to the Microsoft .NET software.

AUTO-UPDATER CONFIGURATION UTILITY

Section estimated time for completion 10-20 minutes.

This section will guide you through the necessary steps in installing and using the Auto Updater Configuration Utility.

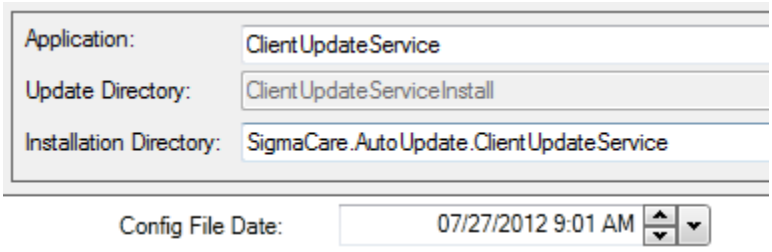
Installing the AutoUpdate.Configuration.Creator Utility

1. This step will guide you through installing the AutoUpdate.Configuration.Creator Utility.
    a. **Unzip the AutoUpdate.Configuration.Creator** to a folder on your local host machine (Example: C:\AutoUpdate.Configuration.Creator).
    b. **Navigate to the directory** where the AutoUpdate.Configuration.Creator Utility was uncompressed on the target computer.

c. **Double** click **setup.exe** file to start the installation wizard.
d. Click Next on the Welcome Screen
e. Select Installation Folder – On this screen you can pick the installation directory that will be created or the utility will be installed in.
f. Select Just Me – These radio buttons allow you to choose if the utility will be available to the just the windows user performing this action or to everyone who can access this computer
g. Confirm Installation – Choose Next to proceed with the installation.
h. Installation Complete - Select Close to complete the installation

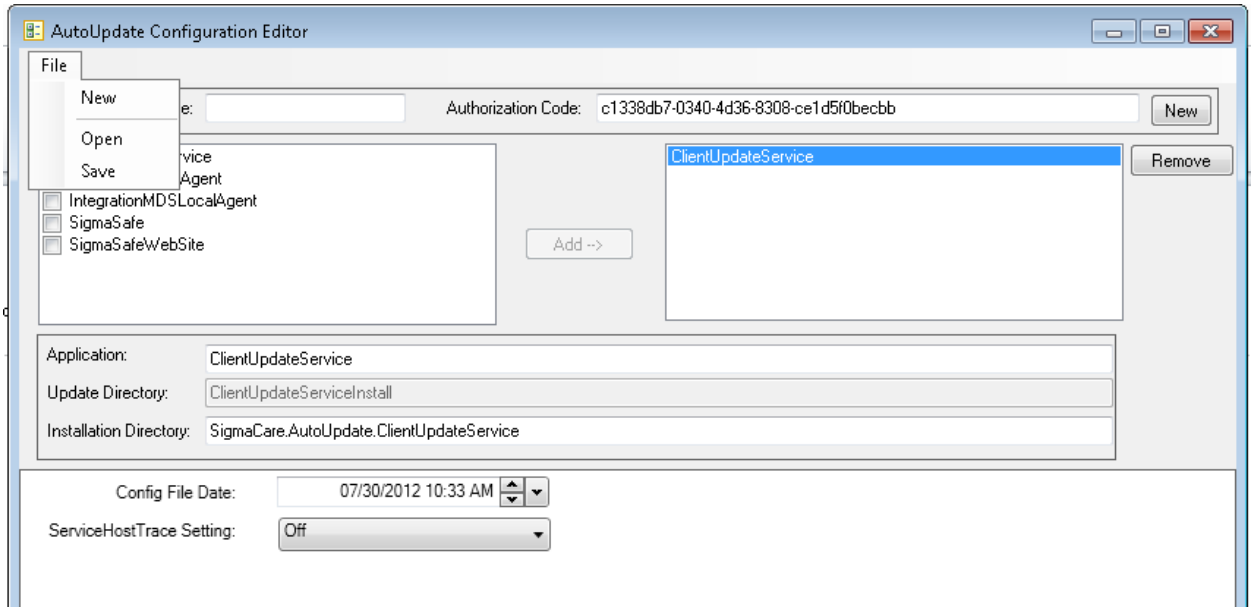
General Configuration Information
This information applies to all applications that can be configure by the AutoUpdater Configuration Utility

1. **Application:ClientUpdateService**
   a. Description of the Application
   b. Should not be altered
2. **Installation Directory: SigmaCare.AutoUpdate.ClientUpdateService**
   a. Directory that the Auto-Updater will install the Application
   b. Should not be altered
3. **Config File Date:** This date is what the Auto-Updater uses to compare the Configuration XML that is stored on production to the Configuration date of the Configuration XML stored locally at the client site. If the date of the Application Files are newer on production then the ones installed on the local interface computer, the Auto-Updater will copy down the newer files from the Data Center to the local copy of the Auto-Updater.



CREATING A NEW CONFIGURATION FILE

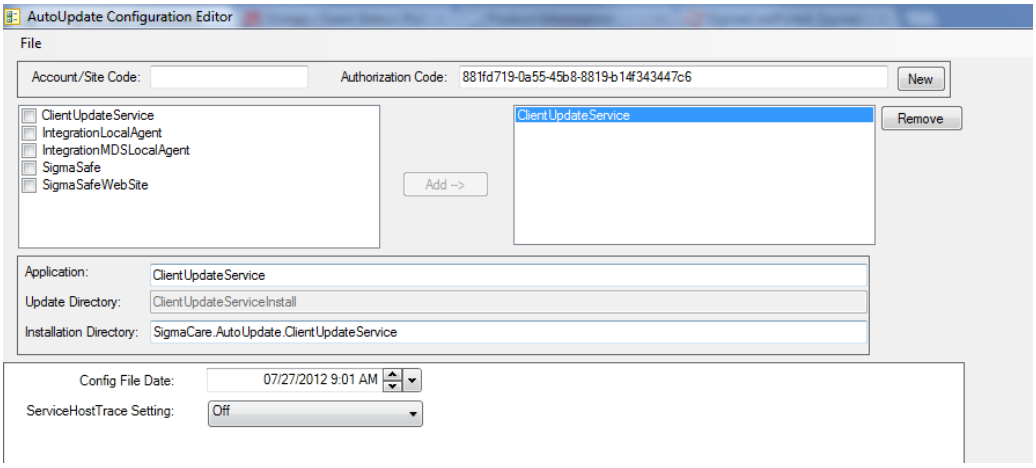
Section estimated time for completion 10-60 minutes.



1. Select **File**
2. Select **New** (Notice that the Authorization Code automatically generates a unique GUID for you)
3. **Enter the Account / Site Code**
4. **Copy and store the Authorization Code** as it will be needed during the Auto-Updater Installation
5. **Select** the check boxes of the applications that you would like to configure

Note: *The Client Update Service doesn't need to be selected as it is already in the right hand configuration box*

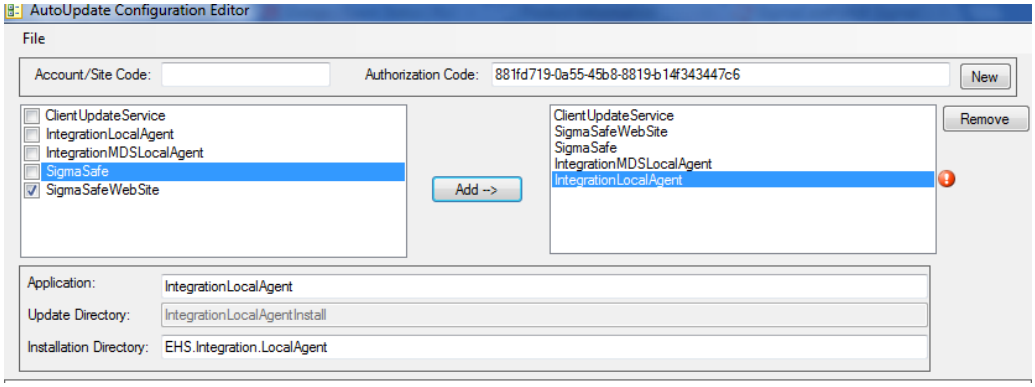
- **a. IntegrationLocalAgent**
  - **i.** This should be selected to configure all inbound ADT interfaces
- **b. IntegrationMDSLocalAgent**
  - **i.** This should be selected to configure the outbound MDS interface
- **c. SigmaSafe**
  - **i.** When selecting the SigmaSafe application, SigmaSafe Website will automatically be selected. You can uncheck the SigmaSafe Website checkbox if you do not wish to configure it at this time
- **d. SigmaSafeWebSite**



6. **Select Add →**
    a. Notice that all applications have been added to the right hand configuration box
    b. You can remove any erroneously added applications by selecting them and pressing **Remove.**

Note*: The ClientUpdateService application cannot be removed as it is need for the AutoUpdater to work properly.*

    c. Select the application in the right hand configuration box that you would like to configure



i. ClientUpdateService

1. Service HostTrace Setting: Off

a. Off (Default & Recommended After Setup)

i. Will not write events to the Service Host Trace Log

b. Error

i. Will only write an error event to the Service Host Trace Log

c. Warning

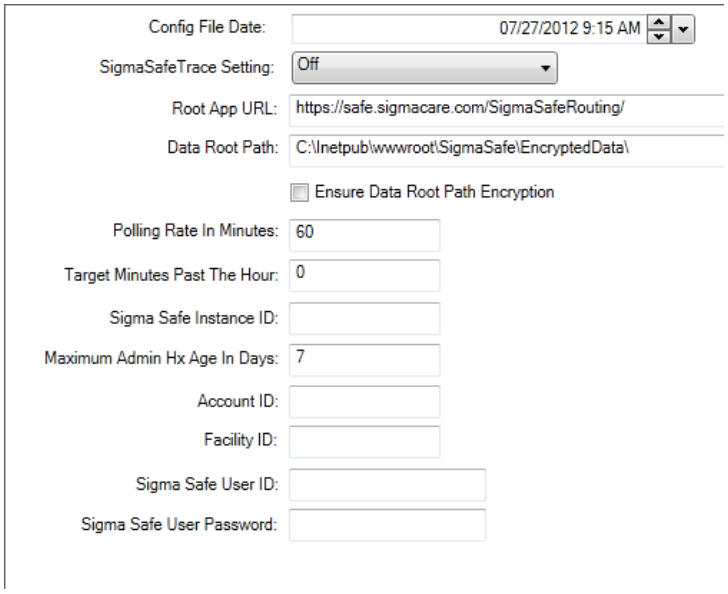
i. Will write warnings and errors to the Service Host Trace Log

d. Info

i. Will write Errors, Warnings and Additional Information to the Service Host Trace Log

e. Verbose (Recommended During Setup)

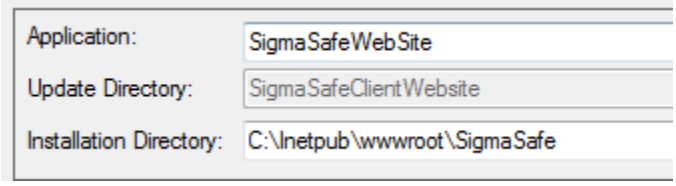
i. Will write all events to the Service Host Trace Log



ii. SigmaSafe

1. **SigmaSafeTrace Setting**
   - **a. Off (Default)**
     - i. Will not write events to the SigmaSafeTrace Log
   - **b. Error**
     - i. Will only write an error event to the SigmaSafeTrace Log
   - **c. Warning**
     - i. Will write warnings and errors to the SigmaSafeTrace Log
   - **d. Info**
     - i. Will write Errors, Warnings and Additional Information to the SigmaSafeTrace Log
   - **e. Verbose**
     - i. Will write all events to the SigmaSafeTrace Log
2. **RootApp URL**
   - **a.** https://safe.sigmacare.com/SigmaSafeRouting/ **(Default)**
3. **Data Root Path**
   - **a.** C:\Inetpub\wwwroot\SigmaSafe\EncryptedData\ **(Default)**
4. **Ensure Data Root Path Encryption**
   - **a.** This checkbox will be checked only if the SigmaSafe server is a domain controller
5. **Polling Rate in Minutes**
   - **a. 60 (Default)** - **This value should not be changed** without consultation with Development first.

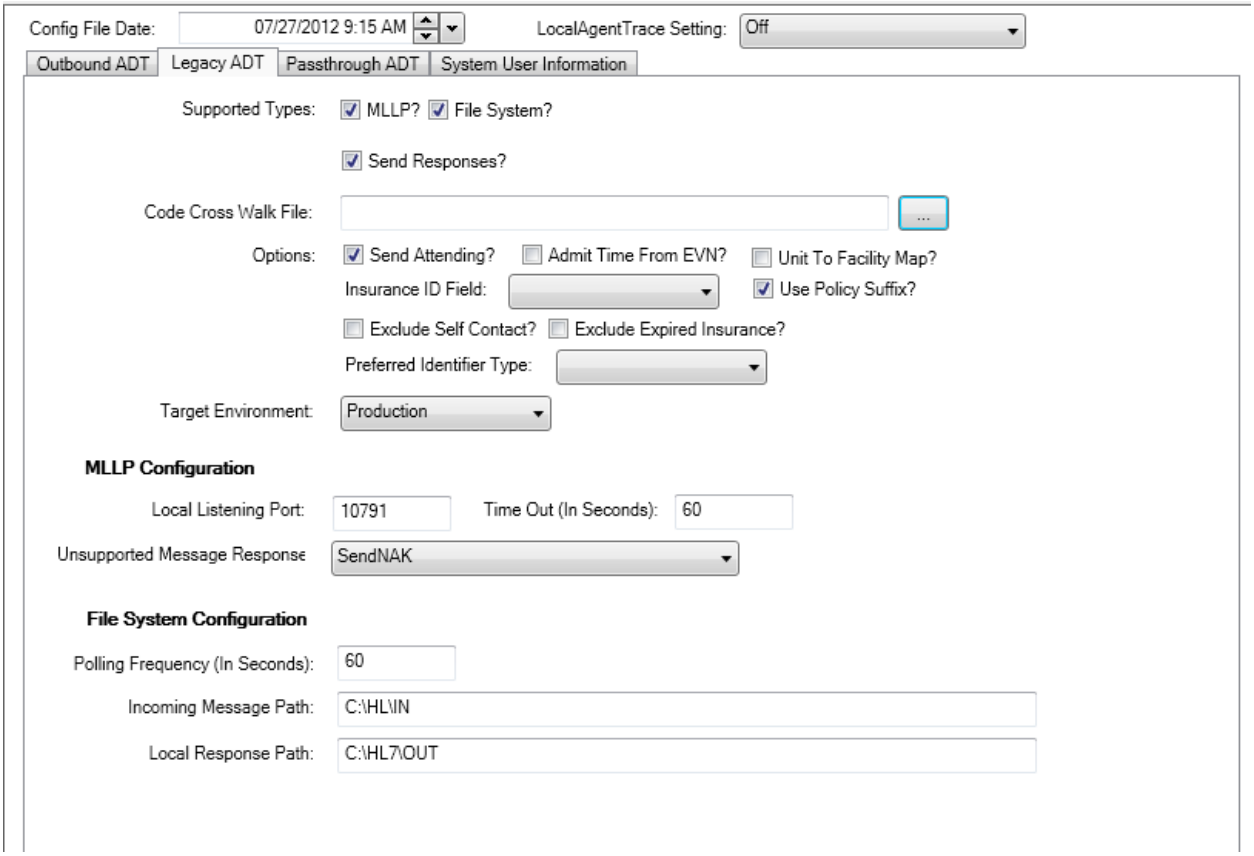
6. **Target Minutes Past the Hour**
    a. This sets the time that the data is pulled down from the data center
7. **SigmaSafe Instance ID**
    a. This ID identifies the associated SigmaSafe instance to the configuration being setup
    b. This is retrieved from SigmaCare Support Tools
8. **Maximum Admin Hx In Days**
    a. **This should not be changed** without consultation with Development first
    b. This setting will configure how many days back the Administration History is pulled down from the data center.
    c. 7 (Default)
9. **Account ID**
    a. **This is the SigmaCare Account ID**
        i. Can be obtained from SigmaCare Support Tools/Account Maintenance
10. **Facility ID**
    a. **This is the SigmaCare Facility ID**
        i. Can be obtained from SigmaCare Account/Setup/Account Setup/Facilities
11. **SigmaSafe User ID**
    a. **SigmaSafe System User Name**
        i. Can be obtained from SigmaCare Support Tools/Account Maintenance/System Users
12. **SigmaSafe User Password**
    a. **SigmaSafe System User Password**
        i. Can be obtained from SigmaCare Support Tools/Account Maintenance/System Users



iii. **SigmaSafeWebSite**
1. **Application**
    a. SigmaSafeWebSite (Default)
2. **Installation Directory**
    a. C:\Inetpub\wwwroot\SigmaSafe (Default)

iv. IntegrationLocalAgent

1. **System User Information**
   - **a. Account ID**
     - i. This is the **SigmaCare Account ID**
       - 1. Can be obtained from SigmaCare Support Tools/Account Maintenance
   - **b. Facility ID**
     - i. This is the **SigmaCare Facility ID**
       - 1. Can be obtained from SigmaCare /Setup/Account Setup/Facilities
   - **c. System User Name**
     - 1. Can be obtained from **SigmaCare Support Tools/Account Maintenance/System User**
   - **d. System User Password**
     - 1. Can be obtained from **SigmaCare Support Tools/Account Maintenance/System User**
   - **e. Test Mode**
     - i. Will enter the interface in Test Mode



2. **Legacy ADT**
    a. **Config File Date**
        i. This date is what the Auto-Updater uses to compare the Configuration XML that is stored on production to the Configuration date of the Configuration XML stored locally at the client site. If the dates of the Application Files are newer on production then the ones installed on the local interface computer, the Auto-Updater will copy down the newer files from the Data Center to the local copy of the Auto-Updater.
    b. **LocalAgentTrace Setting**
        i. **Off (Default)**
            1. Will not write events to the LocalAgentTrace Log
        ii. **Error**
            1. Will only write an error event to the LocalAgentTrace Log
        iii. **Warning**
            1. Will write warnings and errors to the LocalAgentTrace Log
        iv. **Info**

1. Will write Errors, Warnings and Additional Information to the LocalAgentTrace Log

v. **Verbose**

1. Will write all events to the LocalAgentTrace Log

c. **MLLP**

i. If checked will allow for messages to be sent in via the network that the interface computer resides

d. **File System**

i. If checked will allow for messages to be sent by dropping/polling folders on the interface computer

e. **Send Responses**

i. If checked acknowledgments (ACKs/NAKs) are sent back to the vendor

f. **Crosswalk File**

i. A codecrosswalk.xml file can be imported into the utility to have it added to the AutoUpdater Configuration XML file

g. **Options**

i. Send Attending

1. If checked the attending physician from the HL7 message will be processed by the ADT local agent.

ii. Admit Time from EVN?

1. If checked the admission date/time will be taken from EVN-6 of the HL7 message. This setting is used when a vendor does not send the admission date/time consistently in the PV1 segment.

iii. Unit to Facility Map?

1. If checked expects mapping in codecrosswalk.xml that has codetype of facility. The facility would need to be mapped to its units directly. Example facility A is mapped to Unit 1, Unit 2 and Unit 3. Facility B is mapped to Unit 4, Unit 5 and Unit 6.

iv. Use Policy Suffix

1. It will combine policy number and suffix in sub field

a. Example IN1|1|555555^X| would send 555555X to SigmaCare

v. Insurance ID Field

1. This setting determines which field in the IN1 segment is used for mapping the insurance

vi. **Exclude Self Contact**

1. If sent over in NK1 segment ignore self contact if it is mapped in codecrosswalk.xml

vii. **Exclude Expired Insurance**
    1. If selected an expired insurance will not be added to SigmaCare from the HL7 message

viii. **Preferred Identifier Type**
    1. This field allows you to pick which ID should be entered into SigmaCare's vendor ID field from the PID-3 field in the HL7 message.
    2. PID-3 is a reoccurring field that can contain multiple ID numbers for a resident.

ix. **Target Environment**
    1. **QA**
        a. Will configure the interface to point towards QA instead of production
    2. **Production**
        a. Will configure the interface to point towards production instead of QA

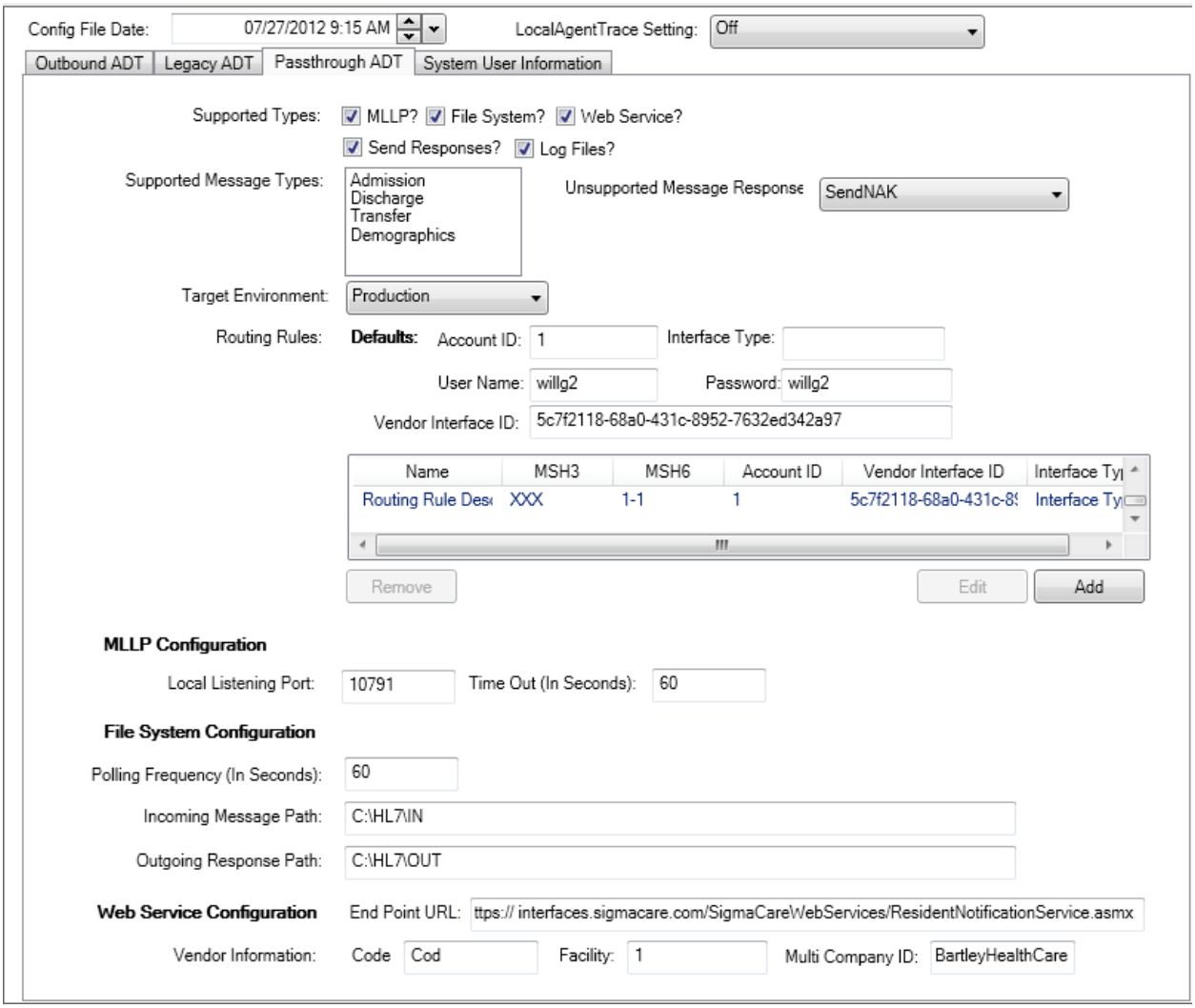
h. **MLLP Configuration**
    i. **Local Listening Port**
        1. **10791 (Default)**
            a. Determines the port that the interface is listening on
        2. **Timeout (In Seconds)**
            a. 60 (Default)
            b. 0 Recommended for a persistent connection
        3. **Unsupported Message Response**
            a. Determines what response to send back to the vendor if a non-Admission or Resident Demographic Update message is sent to the interface
                i. No Response – Doesn't send a response back
                ii. Send ACK – Sends an ACK (positive acknowledgement) response back
                iii. Send NAK – Sends a NAK (negative acknowledgment) response back

i. **File System Configuration**
    i. **Polling Frequency (In Seconds)**
        1. This setting determines the amount of time in seconds that the folder is polled for messages
    ii. **Incoming Message Path**

1. This is the path of the folder that will be used for incoming messages to be placed for processing by the local agent

iii. Outgoing Message Path

1. This is the path of the folder that will be used for ACK/NAK's messages to be place for processing by the local agent



3. **Passthrough ADT**
   a. **Config File Date**
      i. This date is what the Auto-Updater uses to compare the Configuration XML that is stored on production to the Configuration date of the Configuration XML stored locally at the client site. If the date of the Application Files are newer on production then the ones installed on the local interface computer, the Auto-Updater will

copy down the newer files from the Data Center to the local copy of the Auto-Updater.

b. **LocalAgentTrace Setting**
   i. **Off (Default)**
      1. Will not write events to the LocalAgentTrace Log
   ii. **Error**
      1. Will only write an error event to the LocalAgentTrace Log
   iii. **Warning**
      1. Will write warnings and errors to the LocalAgentTrace Log
   iv. **Info**
      1. Will write Errors, Warnings and Additional Information to the LocalAgentTrace Log
   v. **Verbose**
      1. Will write all events to the LocalAgentTrace Log
c. **Supported Types** – This setting configures the different ways in which the Passthrough Agent can receive messages
   i. **MLLP**
      1. If checked will allow for messages to be sent in via the network that the interface computer resides
   ii. **File System**
      1. If checked will allow for messages to be sent by dropping/polling folders on the interface computer
   iii. **Web Service**
      1. If checked will allow for messages to be retrieved from a Web Service
   iv. **Send Responses?**
      1. If checked acknowledgments (ACKs/NAKs) are sent back to the vendor
   v. **Log Files?**
      1. If checked the interface will log a copy of the message that was processed by the local agent
d. **Supported Message Types** (This is a multi-select field)
   i. Allows the user to select the messages that will be processed by the Passthrough Agent
e. **Unsupported Message Response**
   i. Determines which response will be sent when an unsupported message type is sent through the Passthrough Agent
   ii. **No Response**
      1. No response will be sent back to the vendor
   iii. **Send ACK**

1. A positive acknowledgment will be sent back to the vendor

iv. Send NAK

1. A negative acknowledgment will be sent back to the vendor

v. Target Environment

1. QA

a. Will configure the interface to point towards QA instead of production

2. Production

a. Will configure the interface to point towards production instead of QA

f. Routing Rules

i. Defaults

1. This section will configure the default routing rule for the Passthrough agent. If a routing is configured incorrectly or if messages are sent in that do not match a routing rule the Passthrough Agent will default to use this configuration.

a. Account ID

i. Will set the default Account ID for the Passthrough Agent

b. Interface Type

i. Will set the default Interface Type for the Passthrough Agent

ii. Interface Types are only needed if a version of HL7 is being used that is not v2.4 or if we are using a custom map for the interface. Please refer to the vendor specific implementation guide to see if you need to use this field.

c. User Name

i. System User Name that was setup for the interface

d. Password

i. System User Password that was setup for the interface

e. Vendor Interface ID

i. Vendor Interface ID of the vendor interface setup in SigmaCare

2. Routing Rule

Adding a Routing Rule

a. Select **ADD** to add a routing rule
b. **Name**
    i. Add a descriptive name for the routing rule
    ii. Example: FacilityNameRoutingRule
c. **MSH3**
    i. This should be the same value for every instance of an interface. This value is provided by the vendor and will be identified in the vendor specific implementation guide
d. **MSH6**
    i. This is a unique value that will be provided by SigmaCare or the vendor depending on the interface. Please refer to the vendor specific implementation guide.
e. **Account ID**
    i. This will set the Account ID for the interface, please obtain this value from SigmaCare.
f. **Vendor Interface ID**
    i. Vendor Interface ID of the vendor interface setup in SigmaCare
g. **User Name**
    i. System User Name that was setup for the interface
h. **Password**
    i. System User Password that was setup for the interface
i. **Interface Type**
    i. Will set the Interface Type for the Passthrough Agent
    ii. Interface Types are only needed if a version of HL7 is being used that is not v2.4 or if we are using a custom map for the interface. Please refer to the vendor specific implementation guide to see if you need to use this field.

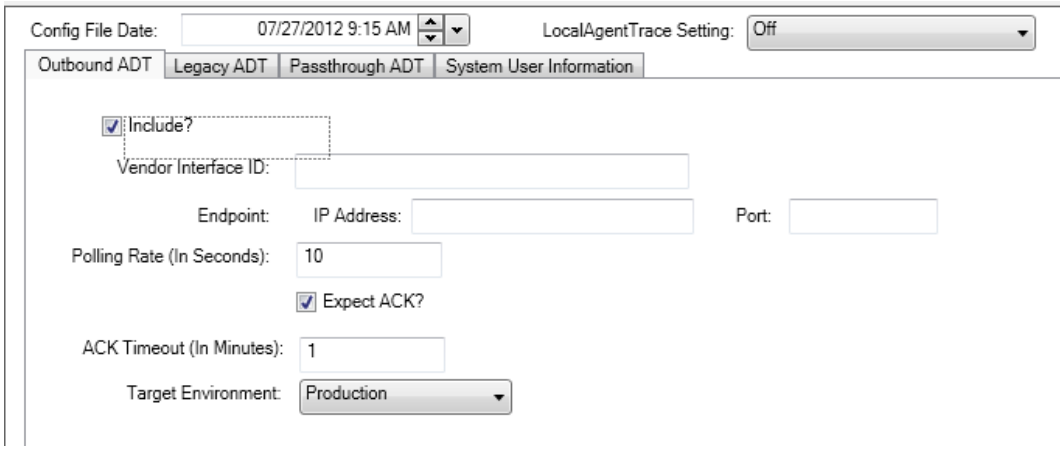
Edit a Routing Rule

a. Select the routing that you would like to edit by clicking on it
    i. Select **Edit**
    ii. Make changes in pop-up window
    iii. Select **OK**

Remove a Routing Rule

a. Select the routing that you would like to edit by clicking on it
    i. Select **Remove**

g. **MLLP Configuration**
    i. **Local Listening Port**
        1. 10791 (Default)
            a. Determines the port that the interface is listening on
        2. Timeout (In Seconds)
            a. 60 (Default)
h. **File System Configuration**
    i. **Polling Frequency (In Seconds)**
        1. This setting determines the amount of time in seconds that the folder is polled for messages
    ii. **Incoming Message Path**
        1. This is the path of the folder that will be used for incoming messages to be placed for processing by the local agent
    iii. **Outgoing Message Path**
        1. This is the path of the folder that will be used for ACK/NAK's messages to be place for processing by the local agent
i. **Web Service Configuration**
    i. **End Point URL**
        1. This will configure the interface to poll a particular Web Service
            a. Please refer to the vendor specific implementation guide to obtain the correct URL to enter here
    ii. **Vendor Information**
        1. These are specific values needed to poll the SOS Web Service
            a. Code
            b. Facility ID
            c. MultiCompany ID



4. **Outbound ADT**
    a. **Config File Date**
        i. This date is what the Auto-Updater uses to compare the Configuration XML that is stored on production to the Configuration date of the Configuration XML stored locally at the client site. If the date of the Application Files are newer on production then the ones installed on the local interface computer, the Auto-Updater will copy down the newer files from the Data Center to the local copy of the Auto-Updater.
    b. **LocalAgentTrace Setting**
        i. **Off (Default)**
            1. Will not write events to the LocalAgentTrace Log
        ii. **Error**
            1. Will only write an error event to the LocalAgentTrace Log
        iii. **Warning**
            1. Will write warnings and errors to the LocalAgentTrace Log
        iv. **Info**
            1. Will write Errors, Warnings and Additional Information to the LocalAgentTrace Log
        v. **Verbose**
            1. Will write all events to the LocalAgentTrace Log
    c. **Include?**
        i. Will allow the user to configure the Outbound ADT portion of the Passthrough Agent
    d. **Vendor Interface ID**
        i. Vendor Interface ID of the vendor interface setup in SigmaCare
    e. **Endpoint**

i. **IP Address**
   1. Will identify the IP address of the vendor interface computer

ii. **Port**
   1. Will identify which port to send the Outbound ADT messages to on the vendor interface computer

iii. **Polling Rate (In Seconds)**
   1. 10 (Default)
   2. Identifies the interval at which the vendor interface will expect messages to be passed

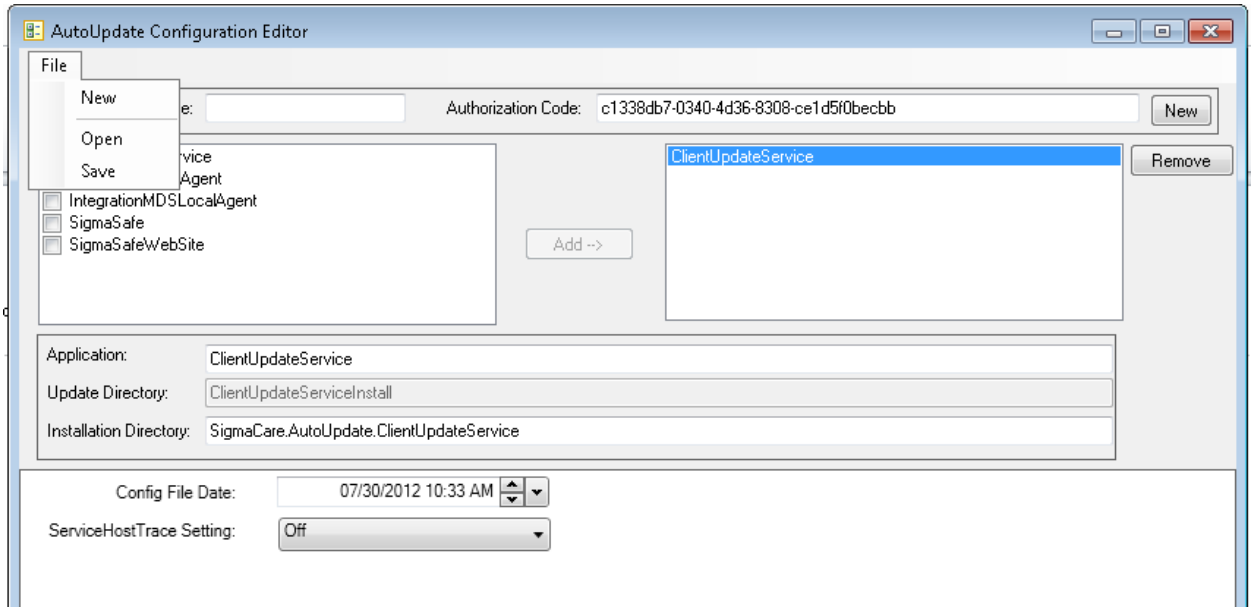
iv. **Expect ACK**
   1. If checked the Passthrough Agent will expect to receive an Ackowledgment back from the vendor interface

v. **ACK Timeout (In Minutes)**
   1. 1 (Default)
   2. Setting configures the amount of time in minutes that we will wait for a response back from the vendor interface before marking the transmission of the message as a Timeout Error

vi. **Target Environment**
   1. **QA**
      a. Will configure the interface to point towards QA instead of production
   2. **Production**
      a. Will configure the interface to point towards production instead of QA

UPDATING AN EXISTING CONFIGURATION FILE

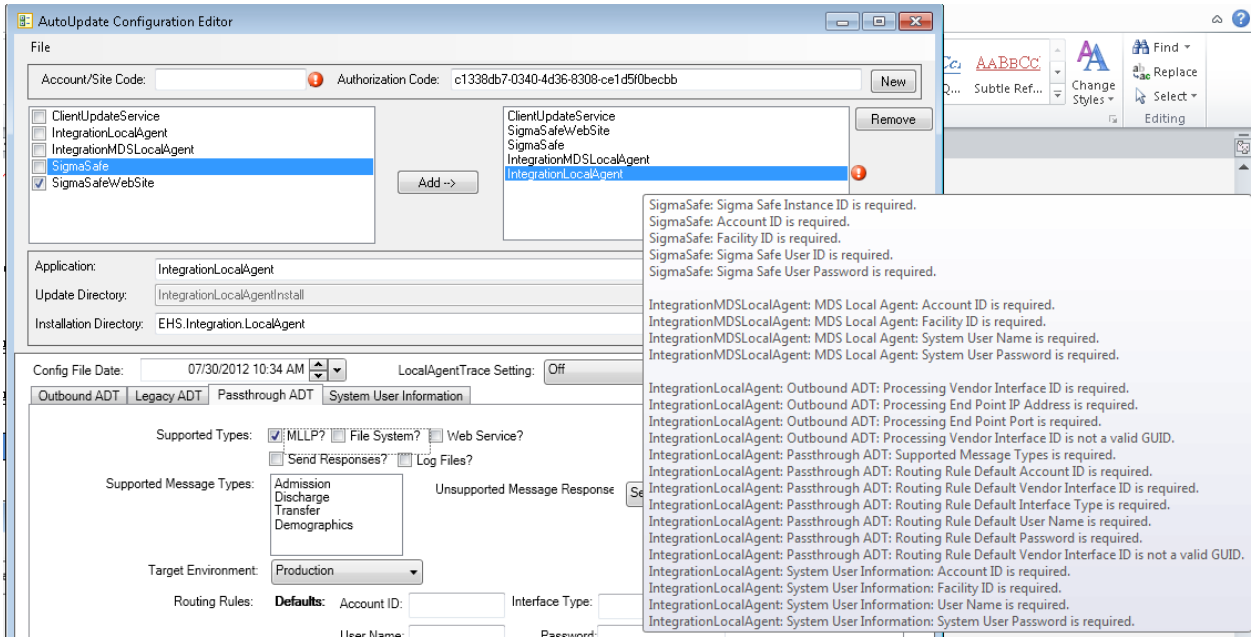
Section estimated time for completion 10-30 minutes.



1. Select **File**
2. Select **Open**
3. **Navigate to the directory** where you have the Configuration XML stored on your local computer
4. Select **Open**
5. **Select the Application** that you would like to make changes to in the right hand configuration box
6. **Navigate through the tabs** associated to the Application to make any necessary changes
7. Select **File**
8. Select **Save**
9. You must **restore the Configuration XML file at the Data Center**
10. **After confirmation that the Configuration XML file has been stored at the Data Center** you can **restart the Service Manager Windows Service** to have the new XML changes be applied to the interface computer at the client site

TROUBLESHOOTING A CONFIGURATION FILE ERROR

Section estimated time for completion 10-30 minutes.



If you the **configuration file rules and validations are not met** you will receive **a red warning icon** next to the **problem area.** If you hover over this icon the utility will identify the areas that need attention. If you see sections of the utility that you do not wish to configure at this time you can simply remove them by selecting the application in the right hand configuration box and then pressing remove.

AUTO UPDATER 1.0 INSTALLATION

Section estimated time for completion 10-20 minutes.

This section will guide you through the necessary steps in installing the Auto Updater 1.0 software. The Auto Updater software installation will result in a new Windows Host Service called SigmaCare Service Manager. This new Windows Service will control all SigmaCare related installations within its umbrella, such as SigmaSafe Local Agent.

1. **Install the Auto Updater 1.0 software**. This step will guide you through installing the Auto Updater 1.0 software through the installation MSI (Microsoft Installer) file.

a) Navigate to the **temporary directory** where the Auto Updater software was uncompressed on the SigmaSafe Server (example c:\temp).
b) Navigate to the following sub-directory, **.\AutoUpdater\AutoUpdater_MSI**
c) Double click the **setup.exe** file to start the installation process.
A Microsoft Installer (MSI) will be launched.
d) At the "Welcome" window for the SigmaCare Service Host, select the **Next** button.
e) At the "Installation Directory" window, leave the **default installation directory**, select the **Everyone** radio button and select the **Next** button.
***Note**: The default installation directory might not the desired location for this installation, if it is not, chose a different installation directory.*

f) At the "Confirm Installation" window, select the **Next** button to perform the installation. *At the end of the Installation process a Service Configuration window will appear.*

g) Using the information gathered in the Preparation Section, fill in the following details, then press **OK**. (Figure 3):

- **User Name** – Windows Administrative Username
- **Password** – Windows Administrative Username's Password
- **Available Services** – ensure Auto-Update is checked; Task Relay should remain unchecked.
- **Account Code** – SigmaCare Account Code
- **Authorization Code** – Authorization Code obtained from the Auto-Updater Configuration XML
- **Service URL** – leave default value; do not change

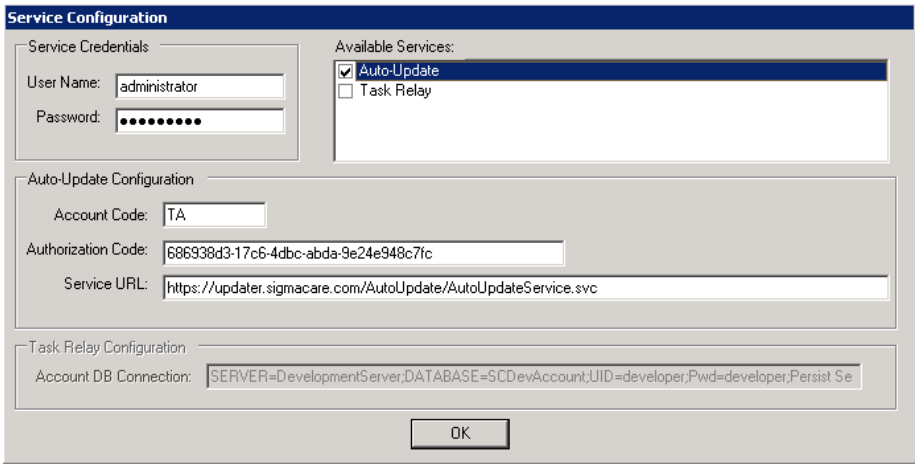


Figure 3

2. **Starting the SigmaCare Service Manager Windows Service**. The following steps will guide you through starting the SigmaCare Auto Updater (Service Manger) solution. The Windows Service which is installed is by default to set to Manual and will need to be updated to Automatic once the installation is confirmed successful.

a) Navigate to the **Windows Services window**. Typically on most Windows Operating Systems the path will be **Start > Control Panel > Administration Tools > Services**.

b) In the Windows Services window, locate **SigmaCare Service Manager**.

c) **Right Click** on the SigmaCare Service Manager Service and select the **Start** option.

INSTALLATION VERIFICATION

Section estimated time for completion 10-25 minutes.

Auto-Updater Verification

Once the Auto Updater 1.0 and the all associated applications are installed you must now ensure the data synchronization between the SigmaCare Data Center and the Auto-Updater will process correctly.

Installation & Configuration Guide for Auto Updater 1.0, SigmaSafe & Interface Local Agents

This section will guide you through the steps necessary to ensure the Auto-Updater and applications ares installed correctly and processing.

1. **Ensure the SigmaCare Service Manager starts**. The following steps will guide you to ensure the SigmaCare Service Manager windows Service is in a started state.

a) Navigate to the **Windows Services window**. Typically on most Windows Operating Systems the path will be **Start > Control Panel > Administration Tools > Services**.
b) In the Windows Services window, locate **SigmaCare Service Manager**.
c) Ensure the SigmaCare Service Manager is in a **Started** state.

2. **View Windows Application Event Log for errors**. The following steps will guide you to the Windows Event viewer to ensure the log file had no recent error messages from the newly installed software.

a) Navigate to the **Windows Event Viewer Application Log**. Typically on most Windows Operating Systems the path will be **Start > Control Panel > Administration Tools > Event Viewer > Application Log**.
b) Review the recent events in the Application Log to ensure there are no errors related to the SigmaCare Service Manager, SigmaSafe or the ADT Local Agent.

3. **Update SigmaCare Service Manager to be automatically started**. These steps will change the Auto Updater solution to start automatically when the Interface Computer is restarted.

a) Navigate to the **Windows Services window**. Typically on most Windows Operating Systems the path will be **Start > Control Panel > Administration Tools > Services**.
b) In the Windows Services window, locate **SigmaCare Service Manager**.
c) **Right Click** on the SigmaCare Service Manager Service and select the **Properties** option.
d) Select **Automatic** from the **Startup Type** option list.
e) Select the **OK** button to save your changes.
f) **Right Click** on the SigmaCare Service Manager Service and select the **Restart** option to ensure the current Service is enabled with your changes.

ADT Local Agent Verification

4. **View Trace Agent Log for errors.** The following steps will guide you to the ADT Trace Agent Log to ensure that the log file had no recent error messages and the ADT Agent started successfully.

a) **Navigate** to the Installation Directory C:\AutoUpdater\EHS.Integration.LocalAgent
b) **Open** the LocalAgentTrace.Log
c) **Review** that the log to ensure that the Service Started correctly and without error.

Example:

```
Test Mode = False
Message Processor Count = 2
        Processor Type EHS.Integration.HL7.PassthroughAdapter.PassthroughMessageProcessor,
EHS.Integration.HL7.PassthroughAdapter, Init
Data=removeMessageDate=true;port=10791;sendResponses=true;unsupportedMessageResponse=SendNAK;supportedMessageTypes=AD
T^A01,ADT^A08,ADT~A01,ADT~A08;LogFiles=true
        Processor Type EHS.Integration.HL7.PassthroughAdapter.PassthroughFileSystemMessageProcessor,
EHS.Integration.HL7.PassthroughAdapter, Init
Data=pollingFrequency=10000;messagePath=C:\HL7\IN\;responsePath=C:\HL7\OUT\;sendResponses=true;LogFiles=true;unsupportedM
essageResponse=SendNAK;supportedMessageTypes=ADT^A01,ADT^A08
Account ID = 1
Facility ID = 1
User Name = inboundADT
[07/10/2012 08:42:28 AM] Starting Message Processor PassthroughMessageProcessor
[07/10/2012 08:42:28 AM] Starting Receive Endpoint PassthroughReceiveEndpoint
[07/10/2012 08:42:28 AM] Started Receive Endpoint PassthroughReceiveEndpoint
[07/10/2012 08:42:28 AM] Starting Message Processor PassthroughFileSystemMessageProcessor
[07/10/2012 08:42:28 AM] Starting Receive Endpoint PassthroughFileSystemReceiveEndpoint
[07/10/2012 08:42:28 AM] Started Receive Endpoint PassthroughFileSystemReceiveEndpoint
[07/10/2012 08:42:28 AM] Starting TCP Listener on endpoint 0.0.0.0:10791
```

SigmaSafe Verification

4. **Activate SigmaSafe Instance to start data synchronization**. This step is performed in SigmaCare Support Tools. The process of activating starts the SigmaSafe instance at the Data Center to process to the SigmaSafe Server to pass Resident data.

a) Log into **SigmaCare Support Tools**.
b) Select the **Account Maintenance** option from the Internal Support Tools menu options.
c) Select the **Magnify Glass** for the Account which you are going to be performing this installation.
d) Select the **SigmaSafe** option from the Account Menu options list.
e) Select the **Red X** icon, to activate the instance and start processing resident data to the SigmaSafe server.
f) At the confirmation message, select the **OK** button.

5. **Restart SigmaCare Service Windows Service**. These steps will guide you through restarting the SigmaCare Host Service windows service to start pulling down the SigmaSafe data.

g) Navigate to the **Windows Services window**. Typically on most Windows Operating Systems the path will be **Start > Control Panel > Administration Tools > Services**.
h) In the Windows Services window, locate **SigmaCare Service Manager**.
i) **Right Click** on the SigmaCare Service Manager Service and select the **Restart** option to ensure the current Service is enabled with your changes.

6. **Verify Data is being transferred from SigmaCare**. The steps below will guide you through checking SigmaCare Support Tools to see what transactions are currently being processed or are queued up waiting to be processed.

a) Log into **SigmaCare Support Tools**.
b) Select the **Account Maintenance** option from the Internal Support Tools menu options.
c) Select the **Magnify Glass** for the Account which you are going to be performing this installation.
d) Select the **SigmaSafe** option from the Account Menu options list.
e) Select the **SigmaSafe Transactions** icon.
f) In the **Status** filter select the **New** option, then select the **Search** button. This will show you all the transactions which still needs to be processed to the SigmaSafe Server. If you select the Search button again, and if the SigmaSafe is pulling data, you will see that the results will have changed and fewer items are present on the new list. You can also select the **Processed** option from the **Status** filter and select the **Search** button. That will show you all the items which have been passed down to SigmaSafe successfully.

7. **Verify Data is being transferred on SigmaSafe Server**. Another way to ensure the resident data is processing correctly is to view the EncryptedData folder within the IIS folders within the SigmaSafe Server.

a) Using Windows Explorer, navigate to the **SigmaSafe IIS Data directory**, standard installation directory is **C:\Inetpub\wwwroot\SigmaSafe\EncryptedData\.**
b) **Verify** files contained are now being created within the directory. There should be a Site.xml file, a Users folder, as well as a Residents folder. Within the Residents folder there should be many subfolders which are Resident System IDs. Within those Resident's folders there should be other files and folders contain that Resident's specific data which is used by the SigmaSafe application.

8. **Have Client access SigmaSafe and verify SigmaCare Resident data**. The last step in the verification process is to contact the client and have them access their SigmaSafe solution to ensure they can still access the software and to ensure the resident data appears correct.

9. **Remove Installation Files from Temporary directory.** Once the installation has been completed remove the installation files from the temporary directory in which you originally copied too. (example c:\temp).