Auto Agent

Installation and Support Guide

Last update: June 3, 2025

Assurance Reimbursement Management™

Optum is a registered trademark of Optum, Inc. in the U.S. and other jurisdictions. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Optum reserves the right to change specifications without prior notice. Optum is an equal opportunity employer.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Preface

This information is provided by Optum for education and awareness use only. Even though Optum believes that all the information in this document is correct as of the date of the publication of this version, Optum does not warrant the accuracy, completeness, or fitness for any particular purpose of this information. All use is at the reader's own risk. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Optum.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Contents

Preface **2**
Introduction **5**
General considerations **6**
Pre-install activities 6
Agent user name and password 6
Set up a group for the Agent 6
Verify external software 6
Agent and linked clients 6
Security 7
Installing Agent **7**
To install Agent 7
Configuring Agent as a program **8**
Configuring Agent as a service **11**
Pros 11
Cons 11
Setting up the Agent **12**
Setup and scheduling of jobs 14
Run times 14
Monitoring 14
Owner confirmation of SQL Agent jobs 15
Tool to facilitate attachment submission 15
Troubleshooting 15
Troubleshooting auto submission 15
Troubleshooting auto download 16
Setting up auto print **16**
Setting up file types 16
Setting Sweep Time 16
Stopping and restarting the Agent 17
If Agent is running as a program 17
If Agent is running as a service 17
Updating the Agent **17**
Updating the Agent as a program or service 17
Support **18**
Initial logon failure 18
Redundancy/Disaster recovery 18
Manual recovery 18
Automated recovery 18
Agent logs 18
agent.log sample – Failed logon 18
Technical log sample 19
Log management 20
Password reset rules 20
Controlling the size of agent.log 21
SwitchValues 21
Setting the maximum threads 21
Setting the TcpKeepAlive configuration key 22
Setting 22
Manually changing the Agent password 22
If the Agent is a program 22

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

If the Agent is a service 23
Adding another CID to an installed Agent 23
If the Agent is a program 23
If the Agent is a service 23
Linking clients – Agent considerations 23
Troubleshooting 24
Agent has stopped working 24
Miscellaneous issues 25
Set non-interactive status 26
Appendix 1 27
Instructions for automated recovery 27
Command file sample 28
Appendix 2 32
Agent workstation registry requirements 32
For .NET 4.6.1 (and higher) 32

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Introduction

The Agent is a local application that assumes the responsibility for moving files between an application server and a client's local system. The Agent can be configured to check for files at scheduled times and, when found, move them to another location. It can also be configured to print files on designated local printers in addition to storing them in a local file system.

This document provides instructions for installing and maintaining the Agent that is stored on the product's system server. The Agent can be installed to run as a program or as a service. The document is divided into six main parts:

- General prerequisites and considerations.
- Installing Agent
- Configuring Agent as a program
- Configuring Agent as a service
- Updating the Agent
- Support

After Agent is installed, it maintains itself:

- **No expired passwords:** Agent automatically changes its own password every 24 hours.
- **No manual updates:** Agent checks for software updates. If an update is found, it updates itself.

The initial install of the Agent on a client workstation is started from a menu option on the client site by someone with Support site access (Install Agent section). For ASP clients, that is an internal associate. For Turnkey systems, that may be one of our customer support associates or a designated user at the Turnkey site.

If the Agent will run as a program, only the basic install is required. If the Agent will run as a service, the basic install is followed by a second install that sets up the service. This document contains separate sections for installation and update of Agent as a program and as a service.

Install Agent as a program if the Agent workstation will be dedicated to the Agent. Install Agent as a service If the Agent workstation will also be used for other things.

When using the Agent with Assurance, updates to the Agent files are loaded onto systems (ASPs and Turnkeys) with the standard product uploading process. When the Agent is running as a program or as a service, the currently installed Agent periodically checks for updates, downloads them, and updates itself – strictly hands off for clients and support alike.

Additional requirements. For data security purposes, Agent workstations have additional requirements beyond standard Assurance workstations. The Agent workstation must meet the requirements defined in the Component/Configuration table in the Workstation Requirements document and these additional requirements:

- .NET Framework 4.6.1 (or higher 4.x version)
- Set TLS 1.2 as the default for Windows using the Windows Registry. (See Appendix 2 for the registry modifications for each required .NET Framework version.)
- Add TLS 1.2 support for .NET Framework using the appropriate Microsoft TLS 1.2 MSU for the operating system. (Windows 10 Build 1607 has native TLS 1.2 support.)

Customer support and implementation teams have a utility that can verify the connectivity for your Auto Agent workstation.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

General considerations

Pre-install activities

The items in this section should be addressed before the initial install of the Agent.

Agent user name and password

Installing the Agent will require that you know the existing Agent's user name and password (set in User Master). Best practice when installing the Agent is to verify that the Agent's user name is AGENTCID (e.g., AGENT9999) for several reasons:

- Standardizing Agent user names means that scripts can find all the agent users by name.
- When clients are linked, if their agent users do not have different names, all but one agent will stop working. (See the "Agent and Linked Clients" topic.)

To set up the Agent user

1. Open User Master and locate the Agent user.
2. Change the user name to AGENTCID.
3. Change the password to password so you will know the Agent user's password.
4. Empty the Interactive User check box.
5. Click Add, then OK.
6. If multiple clients will be using the same agent, log on to each CID that will be using this instance of the Agent and repeat the process of verifying the name and password of the Agent user.

When you have a list of all Agent users and passwords, you are ready to install.

Set up a group for the Agent

Log on as any user and set up an Agent group:

1. In Group Master, set up a group named AGENT.
2. Click Add.
3. Move only the Agent user to This Group.
4. Move all functions but the Grant functions to This Group.
5. Click OK.
6. Repeat this process on every client that will be using the Agent.

Verify external software

This external software must be installed on the Agent workstation before attempting to install the agent:

- Acrobat Reader: 2023.003.20201 (64bit).
- Microsoft .NET Framework 4.6.1 (or higher 4.x version).

Take this time to open Control Panel, Add or Remove Programs and check these programs. If any are missing, install them now.

Agent and linked clients

Prior to Linking clients, rename each client's Agent user to include the client's CID (AGENTCID)

Link Clients works by consolidating users from two clients into a single list of users that have access to both clients. Instead of having identical users on multiple sites, there is only one user and that single user can access the linked clients. Because of this, after linking two or more clients, changes made to user information from any linked client are effective across all linked clients.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

This poses some considerations for the continued operation of each client's Agent after linking. If the Agent users for both linking clients use the same user name, the two users will be consolidated into one. The effect of this consolidation will be that as soon as the Agent changes its password. it will stop functioning on the remaining linked clients because for those clients, the password of the Agent user no longer matches the password (in the password store) of the Agent that is requesting connection.

Renaming each Agent user to include the client's CID (AGENTCID) avoids this issue.

Security

The Agent client communicates securely with the Assurance web servers using HTTPS and TLS 1.2.

The Agent authenticates using HTTPS with a userid/password specific to the CID. The password is automatically changed daily by the Agent.

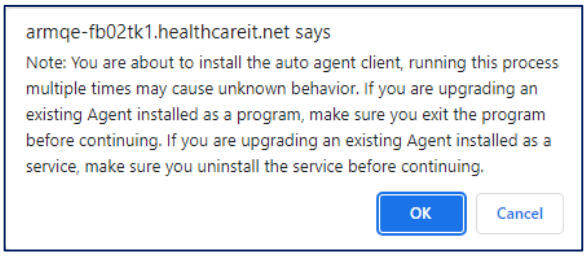
The Agent client can be set up on a machine that is on its own subnet; however, the Agent traffic should be the only traffic on this subnet. The Agent machine only needs to have access to the Assurance website and the shared network resource(s) that will contain files to upload or download.

Files placed on Assurance servers will reside on encrypted disks, but the files themselves are not encrypted on the client side or the server side.

Installing Agent

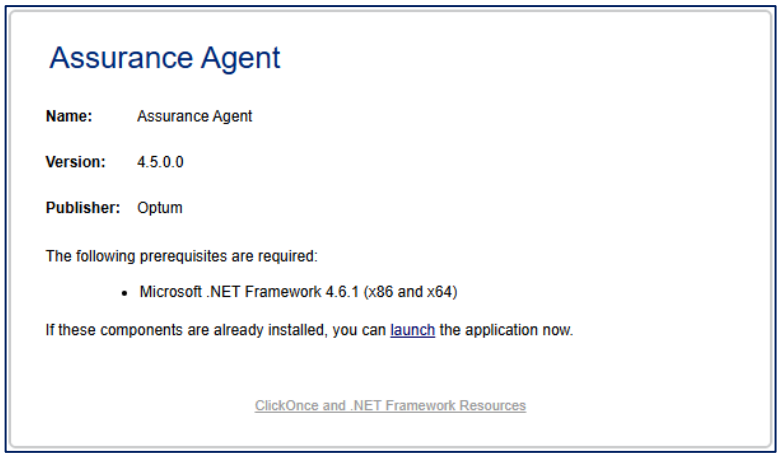
To install Agent

1. Find out if the Agent serves multiple CIDs. If so, obtain a list of all CIDs served by this agent.
2. Remotely access the Agent workstation.
3. Log on to the Agent workstation as the user who will normally start the Agent workstation. This places the Agent log files in a consistent location under C:\\Documents and Settings as shown in the Support section of this document.
4. Log off and log back on as an internal user.
5. Follow this path: **Support > Client Setup > Install Agent Client** (Note: This option is not visible unless you are logged in as an internal user with appropriate rights.)
6. Click OK at the message:



© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

7. The Agent Installer opens and provides you with confirmation data.

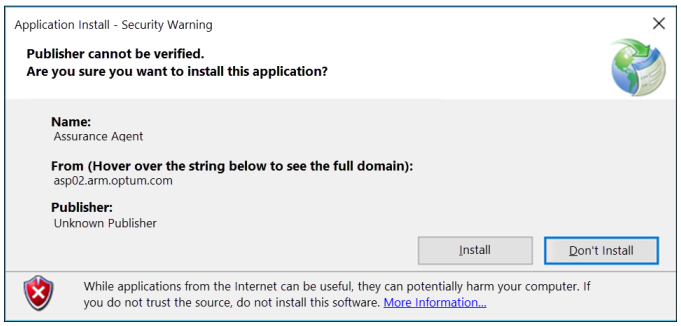


8. Install the Microsoft prerequisite (.NET Framework) if not already present on the computer. Once you have verified the presence of the prerequisite, you can start the Agent install immediately by clicking the word launch.

Notes:

- When installing .NET on some workstations, you may need to reboot after installation. If you do reboot, log on to the product, and select Install Agent Client again to return to the Installation page.
- If you cannot install the prerequisite from remote access, a Turnkey's onsite IT person must install it. Remember to supply the IT person with the prerequisite name (.NET Framework 4.6.1 or higher 4.x version). The prerequisite should be downloaded from the Microsoft download site and installed prior to restarting the installation of Agent.

9. One or more Windows download/Install dialogs open to allow you to install the Agent on the Agent workstation (sample screenshot:



10. Click Install/Run (depending on Windows or browser version) to install the Agent program. When the install finishes, an empty Assurance Agent Configuration dialog opens.

The Assurance Agent Configuration page appears. It is used to configure the agent to run as a program or configure the agent to run as a service.

Configuring Agent as a program

When Agent is running as a program:

- The Agent workstation must be dedicated to the Agent.
- The Agent must be manually started after the Agent workstation is started.
- If the Agent user logs off or if the workstation is turned off, the Agent stops working.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

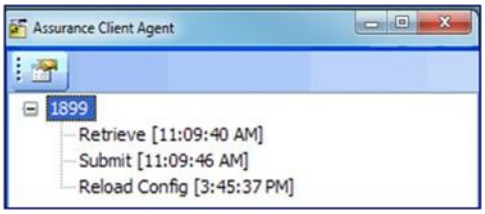
The Agent program is started from the Windows Start menu: Start, Programs, Change Healthcare, Assurance Agent. When the Agent program is running, its icon is displayed in the Windows Program Tray in the lower right corner of the workstation screen. If the icon is not visible, Agent is not running and must be restarted from the Start menu.

1. Most sites will set up only one CID. However, if this Agent will be serving multiple CIDs, you will need to add each CID here. Click Add to open the client fields. Enter the CID in Client Alias then the Username and Password assigned to the Agent user in the client's User Master.

Note: Ignore the Install button and the Web Site URL field.



2. Click Save. The Add fields close and the Client ID is in the Clients list.
3. If this Agent will be serving multiple clients, add the additional clients now: Click Add to reopen client fields, enter the data for the next client, and click Save after each addition.
4. When all clients have been added, click Close to close this dialog. The Agent starts, opens its display dialog, and uses the configuration information to login. If login is successful the agent immediately changes its password and opens its monitoring dialog.



If the Assurance Client Agent monitoring display indicates that the Agent is checking jobs and running, it will remain running until it is stopped, the network user logs off, or the workstation is turned off. From this point, the Agent takes care of itself. It automatically changes its password and it automatically updates itself if it finds an update on the product server – No intervention required.

Notes:

- If the Agent is stopped for any reason, when it is restarted, it verifies its jobs and schedules and begins processing. This processing includes changing its password and checking for updates at appropriate times.
- While the Agent is running, an icon displays in the Windows program tray:

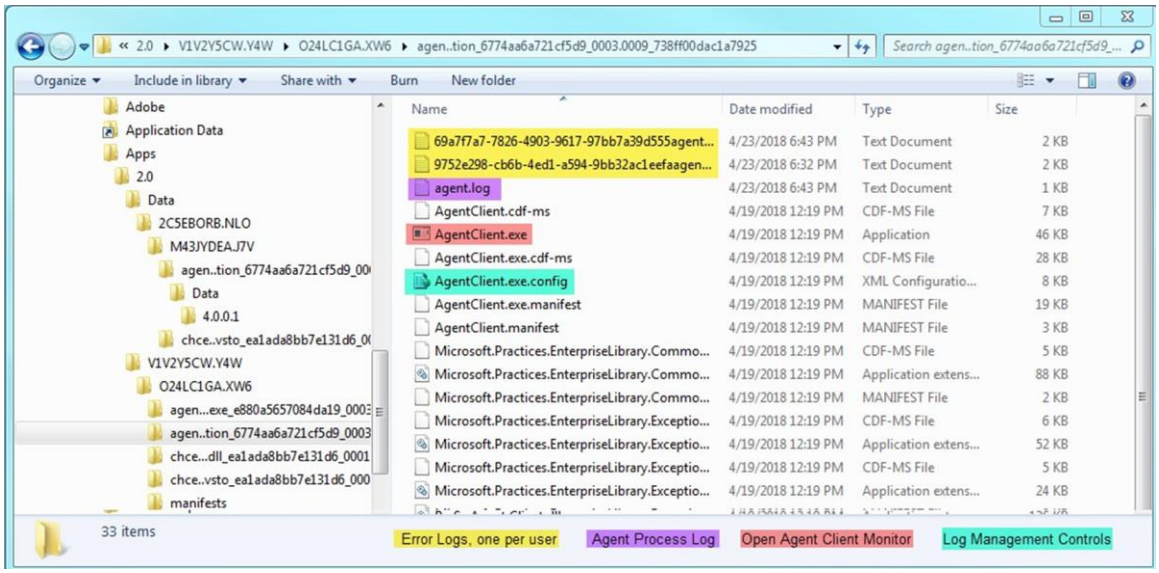


From the context menu for the icon, you can open the monitoring display or open the configuration dialog.

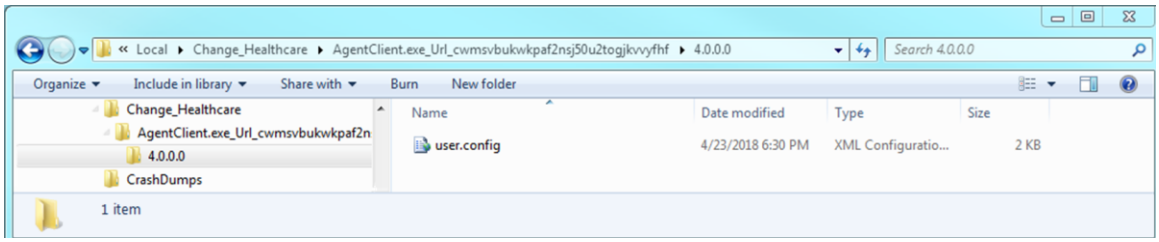
© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Figure 1: Location of Agent files

Agent installed as a program



Agent installed as a service



Notes:

- When the Agent is installed as a service, it creates the Change_Healthcare tree. The new tree contains only user.config. The Agent executable and update files remain in the program tree.
- Whether the agent runs as a service or as a program, the agent control files are always in the most current Agent program folder.
- If Service folders exist under Application Data, then Agent is running as a service. When working with user.config, you must use the service's user.config.
- Each time the agent is updated, another set of Agent folders is added to the program tree. When working with Agent control files, verify that you are using the files in the most recent Agent program folder.
- The status of Agent as a service can only be viewed and verified by opening Control Panel, Administrative Tools, Services. When running as a service, no program icon displays and no Agent Display interface opens.
- Whether Agent runs as a service or a program, always verify that you are getting the Agent's user.config file from the version folder of the newest AgentClient or agen…tion folder.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Configuring Agent as a service

Running the Agent as a service has its pros and cons:

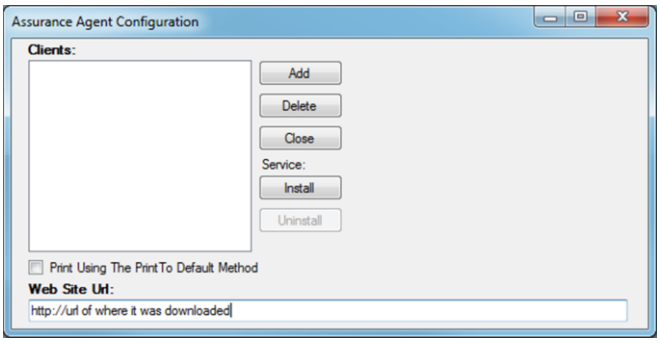
Pros

- When running as a service, the Agent can be started by Windows as it starts all services when the workstation is turned on.
- After the service is started, it will continue to run until the workstation is turned off. As long as the workstation remains on, the Agent is available day or night.
- The user who starts the workstation can log off and log in as another user without causing the Agent to stop.
- Agent 4.0 and later automatically updates itself when there are changes.

Cons

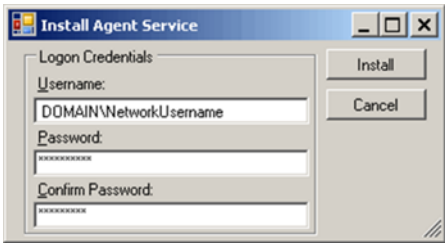
- When the Agent is running as a service, no Agent icon displays in the Program Tray in the lower right corner of the screen. Instead, the Agent service is viewed and controlled through Control Panel/Administrative Tools/Services. (On older Turnkeys, this path is Control Panel/Services.)

Configuring the Agent to run as a service begins when the Assurance Agent Configuration dialog opens at the end of the installation process.



1. Click the Install button in the Service group.

The Install Agent Service dialog opens. This dialog is used to identify the network username and password of the user who will be starting the workstation to the Agent service. This identification ensures that the agent will run under the network user's name and the logs will be in that user's Documents and Settings tree.



2. Enter the starting user's Network username and password and click Install. This installs the Agent as a service.
3. When the Assurance Agent Configuration dialog is displayed, click Close and close the dialog without adding any clients.
4. Before proceeding, verify that the Agent program icon does not appear in the Windows program tray.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

5. To add clients to an Agent that will run as a service, refer to Figure 1 to locate the Agent program folder. Open the folder and run **AgentClient.exe**.

Note: If you are updating an existing Agent, return to “Updating the Agent as a Service” at this point.

6. The Assurance Agent Configuration dialog opens again, this time ready to accept client IDs for the service.
7. If the **Adobe Acrobat Reader** that has been installed on the workstation is version 8.1.2 or higher, empty the Print Using The Print To Default Method check box.
8. In the Assurance Agent Configuration dialog, click **Add** to open the client fields. Enter the CID in Client Alias then the Username and Password assigned to the Agent user in User Master.
9. Verify that web site URL contains the URL of the web site from which the Agent is being installed.

   Wrong: https://URL/Home/UserHome.asp

   Right: https://URL

Tip: The correct URL is in the address bar that appears in the browser when the Assurance home page is open.



10. Click **Save**. The Add fields close and the Client ID is in the Clients list.
11. If this Agent will be serving multiple clients, add the additional clients now by clicking **Add** to open client fields and clicking Save after each addition.
12. When all clients have been added, click **Close** to close the dialog.
13. When the Agent is running as a service, the program version of the Agent is not needed. In the Windows program tray, right click the icon and click **Exit** to close the program.
14. Go to Services in the Control Panel, Administrative Tools menu and right click the Assurance Agent service. Open Properties.
15. Verify that Startup Type is Automatic. Click OK.
16. Start the service by right clicking the Assurance Agent service and clicking **Start**.
17. After ten seconds, open agent.log to verify that the Agent is running correctly. (See the “Agent Logs” topic for the location of agent.log.)

Setting up the Agent

Setting up the Agent allows you to set up schedules for each type of file you submit. To create a schedule for file submission, do the following:

1. Use this path to go to Auto Print File Type Maintenance:

   Maintenance > **System Administration** > **Set Up Agent**

2. Click **Add a New Auto Submit** in the Auto Submit list if not already highlighted.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

3. Type the **name of the schedule** into the Name field.
4. Select the **Enable checkbox**.
5. Refer to the table below for **Submission**, ***File Type**, and ***Claim File Mask** field settings:

File (description and notes) / Settings:	
CUF Files. Automatically send CUF files to Assurance as soon as files when ready.	
Submission field:	Single
***File Type field:**	FILE PASS-THROUGH
***Claim File Mask field:**	Enter path and mask for CUF files.
On Demand Claim Status 276 Request File Pass Through. Automatically send ANSI 276 files to Assurance.	
Submission field:	Single
***File Type field:**	Select the bridge master* name for the 276 bridge key.
***Claim File Mask field:**	Enter path and mask for 276 files. The file name must end with .276 extension.
Notes: Set up File Type feature to have Agent pick up and download 277 claim status response files.	
Customer-Submitted Remit 835 Files: Automatically import ANSI 835 files into Assurance.	
Submission field:	Single
***File Type field:**	Select the bridge master** name for the 835 bridge key.
***Claim File Mask field:**	Enter path and mask for 835 files.
Notes: First three characters of file name must be LOB of file being imported.	
Aii Files: Automatically send Aii files to Assurance as soon when ready.	
Submission field:	Single
***File Type field:**	Select the bridge master* name for the Aii bridge key.
***Claim File Mask field:**	Enter path and mask for Aii files.
Pass Through Files: Automatically send DoD Pharmacy FPT files to Assurance when are ready.	
Submission field:	Single
***File Type field:**	Select the bridge master* name for the CUF bridge key.
***Claim File Mask field:**	Enter path and mask for pass-through files (e.g., *.UCF)
****** **Bridge master** items should **only** be set up and changed with **Support** (800-457-1209). Hours: Monday - Friday, 7:00 am-7:00 pm CT.	

6. Select the **Enable checkbox**.
7. Select the **Enable Batching checkbox** to batch files for submission and submit as a single batch file.
8. Set up the options in the Schedule panel:
   - **Schedule:** Add new timeframe.
   - **Days:** Check days for which you want the schedule to run.
   - **From:** Enter time you want schedule to start on those days.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

- **Through:** Enter time you want schedule to end on those days.
- **Check status every ___ minutes:** Indicate how often you want Agent to check for a file using the mask you entered.

Reminder: Beginning at the From time and until the Through time, the Agent will check status every [#] minutes for the presence of any file using the mask you enter. When the file is found, it is automatically sent to Assurance.

9. Click **OK** to save the settings.

Setup and scheduling of jobs

These SQL Agent jobs should all be set up and scheduled to run at the intervals shown.

- 15-minute intervals – **Back up the transaction log** of each User (Assurance) database
- Nightly – Make a **Full backup** of User databases
- Weekly – **Rebuild the Indexes** of each User database (all tables with an index or primary key index)
- After reindexing tables, run an **Update Statistics** job on the same tables that have been reindexed
- Weekly – Make a **Full backup of System** databases
- Weekly – Run the **CheckDB query** against each database (User and System)
- Weekly – Run the **Updateusage query** against each database (User and System)

Run times

The timing of schedules for running these jobs is important for how quickly they can finish.

Optum recommends running these jobs at the following time:

- Midnight-7 am daily

Optum recommends not running these jobs at the following times:

- 8 pm-9 pm Monday-Friday
- 11 am-6 pm on Sunday

Monitoring

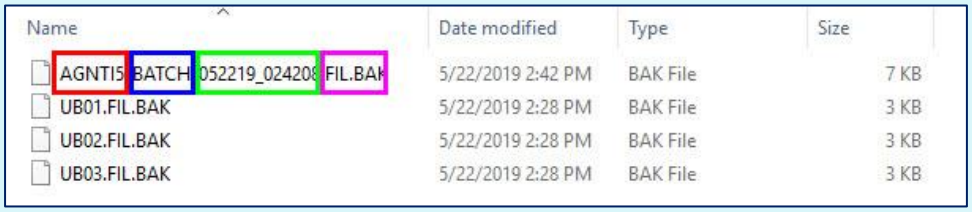
When using Agent to move files, it is critical to monitor the files to verify that they are being moved according to schedule. We recommend that the submission folder be checked at least once a day to see if submission file names do NOT have the .bak extension. If they do not, refer to troubleshooting steps.

Notes:

- Click the Add or Update button before selecting another schedule in the Auto Submit list or leaving the page.
- If your system creates files at night and you use the Agent to send them at night, do not shut down the Auto Agent service.
- If the submission type you select submits a series of files (claim submission and associated content files), identification fields for each possible content file will show directly below Claim File Mask. Add paths and masks for each required (*) file.
- The File Mask field must contain the path to the folder on your local system where the file should be placed. The Agent workstation must be able to access the folder. It also needs to contain a file name. You can use standard Windows wild cards. Example: C:\Downloads\Reports*.PDF.
- When the Enable Batching checkbox is selected, Auto Agent will do the following:
  - Rename the batched copies of the files so they are not added to a batch more than once.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

  - Batch the files for the submission and submit as a single batch (file).
  - Run the batch process before Auto Agent submits the file.
  - Log the names of the files that it batches and the name of the file it produces for troubleshooting purposes.
- The filename naming convention will include the Interface Name from the Bridge Master (in red), the word "BATCH" (in blue) the date and time stamp (in green), and the original base name (in pink), removing any sequence numbers.



- Files will fail to submit if they are bigger than about 100 MB. This limit applies to the combined file when “Enable Batching” is used. This limit does NOT apply to receiving files (reports) from Assurance.
- **Reminder:** To temporarily prevent a submission from running, clear the Enable checkbox. Then stop and restart Agent.

Owner confirmation of SQL Agent jobs

Each silo in Prod uses different accounts. The installation assigns an owner; however, the owner should be checked for accuracy. The owner of a job can be confirmed as follows:

1. Open the **properties** of the job.
2. Confirm whether the **value in the Owner field** is correct. If it is wrong, update it.

Tool to facilitate attachment submission

To facilitate attachment submission, we have developed our **ARM Attachment Tool**, a command-line utility that converts image files (e.g., .BMP, .JPG, .GIF, .TIFF) and document files (e.g., Word, Excel) into PDFs. The tool then combines multiple PDFs into a single PDF file for submission.

Added benefit of the attachment tool: The attachment tool will automatically convert a .GIF file into a PDF so that users do not have to manually convert a .GIF into another file type for submission.

Note: The **ARM Attachment Tool** is designed to be run by your IT team as part of an automation script or process. To get the tool and instructions, **customer IT teams should contact Assurance support**.

Troubleshooting

Troubleshooting auto submission

1. Submission files in the Agent folder that have not been sent to Assurance will keep their original extension without .bak. If you see these files, check the schedules and file masks in Set Up Agent to see if they should have been sent already. If Yes, go to Step 2.
2. Check to see if the Agent is running: In the Windows Control Panel, open Services (or Administrative Tools and then Services) and check the status of the Agent. If it is stopped, restart it. If it is running, stop it before you restart it.
3. When the next submission is scheduled, verify that the Agent sends the file(s). If it does not, call Customer Support.
4. If the files have not been sent by the Agent, you can use Submit Claims on the Claims menu to manually submit the outstanding claim and Aii files.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Troubleshooting auto download

- If you are missing files that should have been automatically downloaded to your system, ensure the Agent is running. In the Windows Control Panel, open Services (or Administrative Tools and then Services) and check the status of the Agent. If it is stopped, then restart it. If it is running, then stop it before you restart it.
- When the next download is scheduled, verify that the Agent downloads the missing file(s). If it does not, call Customer Support.
- If the files have not been downloaded by the agent, you can use Download Files on the Reports menu to manually download the files.

Setting up auto print

Auto print allows users to set up schedules to retrieve files from Assurance and automatically route them to a folder for download or to a local printer for printing.

After the Agent has been installed, **file types** to be retrieved and **sweep time** schedules for those files to be retrieved can be set up.

Setting up file types

To set up the file types to be included in the retrieval sweep, do the following:

1. Use this path to go to Auto Print File Type Maintenance:

   Maintenance > **Auto Print** > **File Type**

2. Select a file type.
3. Choose the desired action for that file type.
   - If you choose a print action, choose an active printer.
   - If you choose a download action and want the file type in a directory other than the specified default, enter the path into the Destination field.
     - The path must be to a folder that the Agent workstation can access.
4. Repeat steps 1-3 for each file type that needs to be set up.
5. Click **OK** to save file type settings.

Setting Sweep Time

For the Agent, “sweep” refers to the Agent’s process of retrieving files. Establishing the “sweep time” sets up the schedule(s) on which the Agent will retrieve accessible files.

To set up the file types to be included in the retrieval sweep, do the following:

1. Use this path to go to Auto Print Sweep Time Maintenance:

   Maintenance > **Auto Print** > **Sweep Time**

2. Type a path into the **Destination** field where downloaded files should be saved. (You can override this path if needed in File Type.)
3. Select the **Enabled** checkbox.
4. Select the **Day(s)** of the week for the Agent to sweep for your selected file types.
5. Type a **From** and **Through** time frame for the Agent to sweep for files on the selected Days.
6. Select the sweep interval in the **Check status every [ ] minutes** drop down list.
7. Click **Add**.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

8. To set up additional schedules, click **- ADD A NEW TIME -** in the Schedule panel and repeat steps 4-7.
9. Click **OK** to save your settings.
10. Stop and restart the Agent to update its schedule information and list of active Windows printers.

Stopping and restarting the Agent

When changes are made to Agent schedules or printers, the Agent is automatically updated. However, the update is on a schedule and may not happen for up to four hours. If you need the changes to take effect immediately, force the update by stopping and restarting the Agent.

If Agent is running as a program

If the Agent is running as a program, you will see an Agent icon in the program tray in the bottom right corner of your screen.

- **To stop:** Right-click the Agent icon in the desktop tray and click Exit.
- **To start:** Double-click the Agent icon on your desktop.

If Agent is running as a service

If the Agent is running as a service, there is no icon in the program tray. To stop and restart the Agent service:

- Go to Services in the Control Panel, Administrative Tools menu, and right-click the Agent service. Open Properties.
- Verify that Startup Type is Automatic. Click OK.
- Start the service by right clicking the Agent service and clicking Start.
- After ten seconds, open agent.log to verify that the Agent is running correctly.

Updating the Agent

The Agent should be updated whenever a new release is available. Agent 4.0.0 is the new baseline version. There is no rollback option from Agent 4.0.

Updating the Agent as a program or service

When the agent is running, it checks for updates on a scheduled timetable. If an update is detected, it is downloaded and installed without user intervention.

Each downloaded update creates a new pair of folders on the Agent workstation. (Figure 1: Location of Agent Files.) If an Agent update does not work on a client's system, roll back to the previous version:

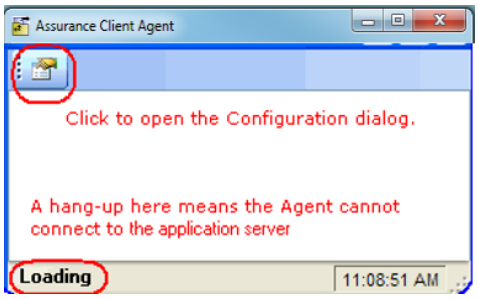
1. Verify that the Agent is not running.
2. Uninstall the current version.
    a. Program Install: Use *Add/Remove Programs* on the *Control Panel* to uninstall the current version. If a previous version exists, *Add/Remove Programs* will ask if you want to roll back or completely remove. Select *Rollback* to return to the most recent working version.
    b. Service Install: Use *Figure 1: Location of Agent Files* to locate the current Agent program folder. Double-click AgentClient.exe. The Assurance Client Agent monitoring dialog opens. In the Assurance Agent Configuration dialog, click *Uninstall*.
3. Start the older version of Agent and test it:
    a. Program Install: Run it from the Windows Start menu or double-click the Assurance Agent icon on the desktop.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

b. Service Install: In *Control Panel, Services*, start the *Assurance Agent* service.

Support

Initial logon failure



An empty Agent dialog box with Loading… displayed in the status bar indicates that the Agent program has failed to log on.

This failure is most often caused by an invalid password. Your first attempt at correction should be to change the Agent user's password. See “Manually Changing the Agent Password.”

If manually changing the Agent password does not correct the issue, check the log files for information about the failed session.

Redundancy/Disaster recovery

The Agent client can be installed and configured on a secondary machine to serve as a back-up client; however, only one Agent client may be running at a time. After installing Agent onto a secondary machine, ensure that it will not run by default.

If the primary Agent client is unable to run for any reason, the secondary Agent client can be run manually or automatically to provide disaster recovery of data.

Manual recovery

The secondary Agent client can be activated by manually changing the password in Assurance and in the Agent client. See “Manually changing the Agent password” on page 22.

Automated recovery

The secondary Agent client can also be set up to run automatically. Appendix 1 contains the instructions for automated recovery and a sample command file.

Agent logs

Whether the Agent is running as a program or as a service, its logs are generated in the same place. See Figure 1: Location of Agent Files for the location.

Caution: This folder contains many files that are part of the Windows OneClick update mechanism. Do not touch them!

agent.log sample – Failed logon

The agent.log is a high-level log of the Agent processing events. Only one agent.log is maintained. Information from multiple starts is appended to the end of the log. Because of this, agent.log can grow quite quickly, especially when the Agent is processing files for multiple clients. See “Controlling the Size of agent.log” for agent.log management tips.

Note that the time in this log file is UTC time, not local time. This sample was generated as the result of a failed start up:

```
12/13/2006 8:12:03 PM Agent Started(3304) Agent Started 12/13/2006
8:14:12 PM ALL(3304) Client Count=1
12/13/2006 8:14:12 PM ALL(3304) Initializing 12/13/2006 8:14:12 PM
ALL(3304) Initializing, stage 2
12/13/2006 8:14:12 PM ALL(3304) Application is network deployed
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

```
12/13/2006 8:14:12 PM All(3304) Network Deployed from URL:
https://URL/AgentClient/AgentClient.application
12/13/2006 8:14:12 PM ALL(3304) Client Manager starting up,
uri=https://URL/AgentClient/AgentClient.application 12/13/2006 8:14:12
PM ALL(3304) Startup: client count=1
12/13/2006 8:14:12 PM ALL(3304) Processing Configuration: Client
PerSe.Agent.Client.ClientConfiguration, Uri
https://URL/AgentClient/AgentClient.application 12/13/2006 8:14:12 PM
ALL(3304) Startup complete 12/13/2006 8:14:12 PM ALL(3304) Client
Manager up...
12/13/2006 8:14:12 PM ALL(3304) Client Manager up and running
12/13/2006 8:14:12 PM ALL(3304) Initialization complete 12/13/2006
8:14:12 PM 1899(2564) Client Process Thread Started 12/13/2006 8:14:13
PM All(3564) Client Manager Thread Started
12/13/2006 8:14:14 PM 1899(2564) Adjusting Url
(https://localhost/ws/Security.asmx) to
(https://URL/AgentClient/AgentClient.application)
12/13/2006 8:14:14 PM 1899(2564) Security Web Service URL:
https://URL/ws/Security.asmx
12/13/2006 8:14:14 PM 1899(2564) Sign On Failed
12/13/2006 8:15:15 PM 1899(3304) Client Process Thread Stopped
```

Technical log sample

Technical logs are generated by errors. This sample technical log was generated by a login failure. Technical logs are not appended to. Each error encountered by Agent will generate a new technical log file.

The GUID in the filename matches the HandlingInstanceID in the first line of the log. This sample shows the message generated when the Agent user has not been made a non- interactive user.

Also note that the time in the first line is UTC time. The time immediately below the dotted line is the same time in Local time.

```
12/13/2006 8:14:15 PM Assurance Agent(2564) HandlingInstanceID:
38a85fd3-8759-4237- 89d9-316b716415fc
An exception of type 'System.Net.WebException' occurred and was caught.
--------------------------------------------------------------------------------
12/13/2006 14:14:14
Type : System.Web.Services.Protocols.SoapException,
System.Web.Services, version 2.0.0.0, culture=neutral,
PublicKeytoken=b03f5f711d50a3a
Message : Server was unable to process request. --> Attempting to login
to a non-
interactive account.
Source : System.Web.Services Help link :
Status : ProtocolError
Response : System.Net.HttpWebResponse
Data : System.Collections.ListDictionaryInternal TargetSite :
System.Object[]
ReadResponse(System.Web.Services.Protocols.SoapClientMessage,
System.Net.WebResponse, System.IO.Stream, Boolean)
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

```
Stack Trace :   at
System.Web.Services.Protocols.SoapHttpClientProtocol.ReadResponse(SoapC
lientMessage message, WebResponse response, Stream responseStream,
Boolean asyncCall)
at System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(String
methodName, Object[] parameters)
at
PerSe.Agent.Client.WebServices.Security.SecurityWse.LogonAgent(String
userName, String password, String clientAlias)
at PerSe.Agent.Client.ClientProcess.SignOn()


Additional Info:
MachineName : MACHINE1
TimeStamp : 12/13/2006 8:14:15 PM
FullName : Microsoft.Practices.EnterpriseLibrary.ExceptionHandling,
Version=2.8.0.0, Culture=neutral, PublicKeyToken=
AppDomainName : DefaultDomain
ThreadIdentity : WindowsIdentity : DOMAIN\User
```

Log management

This section describes the only customizations that may be made to the Agent configuration files. The customizations are effective for the Agent running as a program or as a service.

Password reset rules

Whether to automatically change the Agent password and the interval between automatic changes are controlled by two settings in the AgentClient.exe.config file. This file is located on the on the Agent workstation – see Figure 1: Location of Agent Files.

AgentClient.exe.config is an xml file. It can be opened in Notepad. The password settings are in the <appSettings> node:

```
<appSettings>
 <add key="AgentPasswordResetTime" value="1440" />
 <add key="AutoPasswordReset" value="true" />
</appSettings>
```

Default settings are to automatically change the password and to change it every 1440 minutes. (24 hours).

To change the values:

Open AgentClient.exe.config in notepad and scroll to the end of the file. Locate the <appSettings> node.

1. To turn off the automatic password change, change the value for "AutoPasswordReset" to false.
2. To change the interval between automatic password changes, change the value for "AgentPasswordResetTime."
3. Save the file.

Caution: Turning off the password reset compromises the Agent's security.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Controlling the size of agent.log

The agent.log file grows indefinitely as the agent operates. Clients that use one Agent to serve several clients or who have a lot of Agent activity can quickly develop an agent.log that is several hundred MB in size. A simple solution is to periodically delete agent.log. (If there is a reason to preserve a large agent.log, it can be moved to another location.) The next time the Agent runs, it will create a new agent.log.

In addition, the growth of agent.log can be curbed by two settings in AgentClient.exe.config which is located in the folder that contains the logs:

```
<categorySources>
 <add switchValue="Error" name="General">
  <listeners>
   <add name="Formatted EventLog TraceListener" />
   <add name="Trace Activity Log Listenter" />
  </listeners>
 </add>
 <add switchValue="Error" name="Trace">
  <listeners>
   <add name="Trace Activity Log Listenter" />
  </listeners>
 </add>
</categorySources>
```

Note: Changing values in AgentClient.exe.config affects only agent.log. The technical log will still be generated whenever an error is encountered.

If you change the SwitchValue associated with name="General" to "Off", nothing will be added to agent.log.

- If you change the *switchValue* associated with *name="Trace"* to *"Off"*, agent.log will contain only general entries and not the trace entries.

SwitchValues

You can also expand or contract the size of the log by changing the level of criticality of events that will be logged. Any switchValue in this list can be substituted for Error in the sample above. The recognized switchValues are as follows:

Off - Does not log any events. Critical - Logs only Critical events. Error - Logs Critical and Error events.

Warning - Logs Critical, Error, and Warning events.

Information - Logs Critical, Error, Warning, and Information events.

Verbose or All - Logs Critical, Error, Warning, Information, and Verbose events.

Best practice: if you change a switchValue to a more verbose setting when troubleshooting Agent, remember to set it back to a more normal setting when you are finished troubleshooting.

Setting the maximum threads

The maximum available threads needed by the Agent is calculated when the Agent starts. This is the formula:

ThreadCountMultiplier x Number of CIDs + ThreadFixIncrements = Max threads

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

On a system that has 50 CIDs using the same agent, the default formula works out to (3 x 50) + 2 = 152 available threads.

Unless the system has very heavy file transport activity, the default setting for maximum threads available to the Agent should be sufficient. If you need to increase the maximum available threads, open Agent.config.exe for the current update and scroll to the bottom of the file:

```
<appSettings>
<add key="AgentPasswordResetTime" value="1440" />
     <add key="AutoPasswordReset" value="true" />
     <add key="RenameContentFiles" value="false" />
     <add key="AdobeWaitForIdle" value="300000" />
     <add key="AdobeWaitForClose" value="300000" />
     <add key="AdobeBytesPerSecond" value="300" />
```

<add key="ThreadCountMultiplier" value="3"/>

```
     <add key="ThreadFixIncrements" value="2"/>
</appSettings>
```

Adjust the ThreadCountMultiplier or the ThreadFixIncrements a little. To reset the threads, save the file and restart the Agent.

Setting the TcpKeepAlive configuration key

The TcpKeepAlive configuration key controls the closing and opening of the TCP/IP port. If the configuration key is not present or if it is set to 0, the FTPS Agent will close the TCP/IP port when it completes a single call.

Setting

The value for the TcpKeepAlive configuration key is measured in minutes and ranges from 0 to 1440 (24 hours). Unless there is a technical need, no maximum setting is enforced so the value may be as high as 1440.

The default setting for the key is zero (0), meaning it is disabled and, as indicated above, the TCP/IP port will be closed when it completes a single call.

Manually changing the Agent password

Because the Agent maintains its own password by changing it far more frequently than it would be change manually, the password should never need to be changed manually in User Master. However, if the Agent password is changed in User Master, it must also be changed in Agent Configuration.

If the Agent is a program

1. Log on to the Agent workstation as the Agent network user.
2. Use the Agent Icon in the Program Tray to stop the Agent.
3. In *User Master*, change the password of the Agent user so that you know what it is.
4. Open *Agent Configuration* by right clicking the Agent icon in the Windows Taskbar and selecting *Agent Configuration*.
5. Highlight the appropriate client, and click *Add* to open the configuration fields.
6. Change the password to match the password assigned in *User Master*.
7. Click *Save*.
8. Start the Agent.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.



If the Agent is a service

1. Stop the Agent service
2. In *User Master*, change the password of the Agent user so you know what it is.
3. Open *Assurance Agent Configuration*:
4. Navigate to the current Agent program folder and double-click ***agentclient.exe***.
   The *Assurance Client Agent* dialog opens.
5. Click the first button in the toolbar to open *Assurance Agent Configuration*.
6. In Agent Configuration, highlight a client and click ***Add*** to open the configuration fields.
7. Change the password to match the password assigned in *User Master*.
8. Click ***Save***.
9. Restart the Agent service.

Adding another CID to an installed Agent

After Agent is running, if it needs to begin serving an additional client, the client is added to the Agent in the Assurance Agent Configuration dialog.

If the Agent is a program

1. On the Agent workstation, right click the Agent icon in the Windows taskbar
2. Select *Config Settings* to open the *Assurance Agent Configuration* dialog.
3. Enter the information for the client being added: CID, Agent user name, and password from client's *User Master*.
4. Click ***Save***.

If the Agent is a service

1. Stop the Agent service
2. Navigate to the current Agent program folder and double-click **agentclient.exe**. The *Assurance Client Agent* dialog opens.
3. Click the first button in the toolbar to open the *Assurance Agent Configuration* dialog.
4. In Agent Configuration, click ***Add*** to open the configuration fields then add the new client.
5. Click ***Save*** and then ***Close***.
6. Start the Agent service.

Linking clients – Agent considerations

Link Clients consolidates the *User Master* accounts for each client that is being linked so that two clients use the same common set of users. After linking, when a password is changed on one site, it is changed on the other sites because there is only one user. Also, when a new user is added to one client, the new user is added to the other linked clients.

Although creating a single user list for both linked clients simplifies life for interactive users, it can break the Agent processing for the two sites if the Agent users on each site have the same user name in *User Master* at the time the clients are linked. The two Agent users will be consolidated into one. As soon as the first Agent is restarted and changes its password, the second Agent will break because it is not using

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

the current password. To prevent this, ***before*** linking clients, change the user names of the Agent users on each client site:

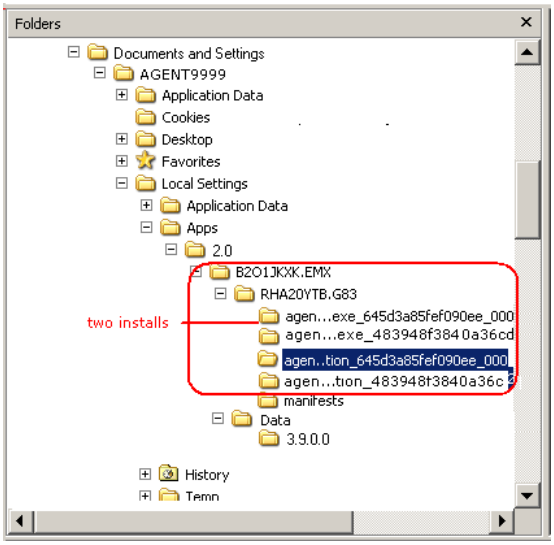
- Log into the first client and open *User Master*.
  1. Highlight the Agent user.
  2. Change the *User Name* to AGENTCID (AGENT9999).
  3. Click ***Update***, then ***OK***.
  4. In the Agent workstation's Windows program tray, right click the Agent icon
  5. Choose *Config settings* from the menu. The *Assurance Agent Configuration* dialog opens.
  6. Double-click the client and change the Agent's *User Name* to the new name.
  7. Click ***Save*** and close the configuration dialog.
  8. Log into the other client(s) to be linked and repeat the process.

After the user names have been changed in User Master and in the Assurance Agent Configuration dialogs, you are ready to link the clients.

Troubleshooting

To determine if the Agent is running as a program or service, open Control Panel, Administrative Tools, Services and check for Assurance Agent in the list of services. If it is absent, the Agent is installed as a program.

To determine if the Agent has been updated, open the tree that contains the Agent folders. Each update installed adds another pair of folders. If there is more than one set of folders, the Agent has been updated. Check the date of the most recent agen…exe file.



Agent has stopped working

Cause	Solution
The Agent has been stopped.	Restart: • Program: Right click the Agent Icon in the Programs tray and select *Start*. • Service: Open *Administrative Tools, Services* in the Control Panel and restart the *Agent* service.
The Agent workstation has been turned off.	Start the workstation and log on as the Agent user.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Cause	Solution
	• Program: Right click the Agent icon in the Programs tray and select Start. • Service: The Agent service will be automatically started with the other Windows services.
The client has been linked to another client without verifying beforehand that the two Agent accounts are different.	Log into the non-functioning client, change the Agent user name, and then update the that client in the *Assurance Agent Configuration* dialog. Restart the Agent.
The network Agent user has been logged off and another user is logged into the Agent workstation. *(This is a problem only when the Agent is running as a program.)*	Log the current user off and log on as the network Agent user. Right click the Agent icon in the Programs tray and select Start.
The Agent has run out of available threads.	Use the “Setting the Maximum Threads” topic to expand the number of available threads.

Miscellaneous issues

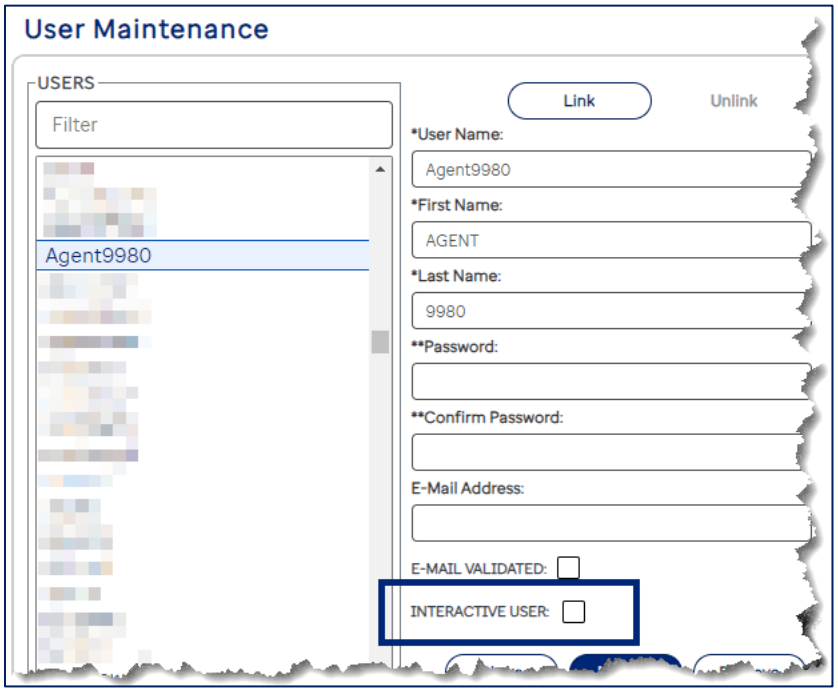
Issue	Solution
No information in *Agent.log*.	Refer to the “Controlling the Size of agent.log” topic for a discussion of setting the switchValues that control what is written to this log.
The client reports garbage when printing large PDF files such paper claim files.	Open the configuration page and empty the *Print Using The PrintTo Default Method* check box. When the check box is empty, files are printed with the alternative *Print* method instead of the more common *PrintTo* method. *Print* method must be used to print large PDFs. When clearing the check box, remind the client that the trade-off is that when using the *Print* method, the Agent will close all instances of the Acrobat Reader as it queues a file that will be sent to a different printer. If someone is using the Reader at that time, their Reader may close unexpectedly.
Acrobat Reader closes with no warning.	(See above) When Files are being printed with the *Print* method. When files are being printed, Acrobat Reader must be closed between each print to allow the next file to be directed to the correct printer.
Note about use of Acrobat Reader 9.3 and higher with Agent.	On systems configured to run the Agent as a service and that use Acrobat Reader 9.3 or higher on the Agent workstation, if the client prints large files like paper claim files, *Print Using The PrintTo Default Method* must be checked. *Print Using The PrintTo Default Method* works as follows: • **If checked:** Acrobat Reader opens and remains open as long as the Agent is running. If the Agent is stopped, the Reader must be closed manually before restarting the Agent. If the Reader is not closed, its icon remains visible, but nothing will print until it is closed and the Agent can reopen it as part of its next print job. • **If empty:** Acrobat Reader opens and closes for every print job. A side effect of this configuration is that on the Agent workstation, all open instances of the Reader will close. If the Agent workstation is also being used as a product workstation and the product user has Acrobat Reader open for another task, that instance of the Reader will also close.

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Issue	Solution
Acrobat Reader 10 on a Windows 7 workstation does not print reports	Beginning with version 10, Acrobat Reader has a protection mode that must be worked around. There are two methods: 1. Acrobat Reader solution: Disable *Protected Mode* in Adobe –Edit > Preferences > General. Empty the *Enable Protected Mode at Startup* checkbox 2. Windows 7 solution: Change User Account Control Settings – In Control Panel > User Accounts. Click *Change User Account Control Settings* and set to *Never Notify.*

Set non-interactive status

The Agent functions only if it is set up as a non-interactive user in the user master: the Interactive User checkbox is empty. This change should already be in place. However, it is worth checking if a client reports that their Agent is not running.



© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Appendix 1

Instructions for automated recovery

- Create a command file similar to the sample below

- Install Agent on both machines

- Modify local environment variables in the file:

```
REM SMB share path for the Primary and Backup agent servers
REM e.g.
REM SET PRIMARY_NAME=\\AGENTSRV001.healthproviderx.com
REM SET BACKUP_NAME=\\AGENTSRV002.healthproviderx.com
SET PRIMARY_NAME=
SET BACKUP_NAME=

REM Username under which the Agent service is set up to run.
REM e.g.
REM SET AGENT_USER_NAME=fileMgrAdmin
SET AGENT_USER_NAME=

REM SMB share path for shared backup location
REM e.g.
REM SET
CONFIG_MIRROR_PATH=\\BACKUPSRV001.healthproviderx.com\BaseSmbSharePath\Auto
Agent\Agent Config Files (mirror)
SET CONFIG_MIRROR_PATH=
```

- Save onto each server.

- This setting will be different on both machines:

```
REM Path under the C:\Users\{username}\AppData\Local\Change_Healthcare to
which agent has been installed.
REM This is dynamic per install so it must be looked up.
REM e.g.
REM SET
AGENT_INSTALL_INSTANCE=AgentClient.exe_Url_adft41hbf1frr5jqnzkb3e1loxy1w4f2
SET AGENT_INSTALL_INSTANCE=
```

- On the "backup" server modify this environment variable:

```
REM Primary or Backup configuration setting
REM e.g
REM 1 = TRUE, 0 = FALSE
SET PRIMARY=1
```

- Make sure the Agent Service is set to manual!! The schedule jobs will restart the services.

- Make sure the Agent Service is running on the Primary and stopped on the Secondary.

- Create Schedule Jobs on each machine to run these commands.

- Start the schedule Jobs

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

To change Assurance login on the shared Agents.

1. Stop the Scheduled Jobs that mirror the Agent config files on both servers
2. Stop the Agent services on both servers (should be just primary)
3. Change config via Assurance standard procedure
4. Restart Agent on primary
5. Start the scheduled jobs on both servers
6. Wait and check the mirror file logs for the copy.

Command file sample

```
@echo off

ECHO AGENT CHECK BEGIN
DATE /T
TIME /T

REM Primary or Backup configuration setting
REM e.g
REM 1 = TRUE, 0 = FALSE
SET PRIMARY=1
SET FIRST_PASS=1
SET SLEEP_SECS=10

REM SMB share path for the Primary and Backup agent servers
REM e.g.
REM SET PRIMARY_NAME=\\AGENTSRV001.healthproviderx.com
REM SET BACKUP_NAME=\\AGENTSRV002.healthproviderx.com
SET PRIMARY_NAME=
SET BACKUP_NAME=

REM Username under which the Agent service is set up to run.
REM e.g.
REM SET AGENT_USER_NAME=fileMgrAdmin
SET AGENT_USER_NAME=

REM Path under the
C:\Users\{username}\AppData\Local\Change_Healthcare to which agent
has been installed.
REM This is dynamic per install so it must be looked up.
REM e.g.
REM SET
AGENT_INSTALL_INSTANCE=AgentClient.exe_Url_adft41hbf1frr5jqnzkb3e1lox
y1w4f2
SET AGENT_INSTALL_INSTANCE=

REM SMB share path for shared backup location
REM e.g.
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

```
REM SET
CONFIG_MIRROR_PATH=\\BACKUPSRV001.healthproviderx.com\BaseSmbSharePat
h\Auto Agent\Agent Config Files (mirror)
SET CONFIG_MIRROR_PATH=

SET
USER_CONFIG_PATH=C:\Users\%AGENT_USER_NAME%\AppData\Local\Change_Heal
thcare\%AGENT_INSTALL_INSTANCE%\4.1.0.0

SET AGENT_SVC_NAME=AssuranceAgent

echo Sync user configs
ROBOCOPY /XO "%USER_CONFIG_PATH%" "%CONFIG_MIRROR_PATH%"
ROBOCOPY /XO "%CONFIG_MIRROR_PATH%" "%USER_CONFIG_PATH%"

IF %PRIMARY%==1 GOTO PRIMARY_LOGIC

:BACKUP_LOGIC
ECHO RUNNING BACKUP AGENT SERVER LOGIC

:CHECK_BACKUP
sc.exe %BACKUP_NAME% query %AGENT_SVC_NAME% > sc.out
find /i "RUNNING" < sc.out
IF %ERRORLEVEL% == 0 (
  IF FIRST_PASS==0 GOTO SCRIPT_END
  GOTO BACKUP_RUNNING
)

ECHO BACKUP %BACKUP_NAME% IS NOT RUNNING

ECHO CHECKING PRIMARY %PRIMARY_NAME% AGENT STATUS
sc.exe %PRIMARY_NAME% query %AGENT_SVC_NAME% > sc.out
find /i "RUNNING" < sc.out
IF %ERRORLEVEL% == 0 (
  ECHO PRIMARY %PRIMARY_NAME% RUNNING
  GOTO SCRIPT_END
)

ECHO PRIMARY %PRIMARY_NAME% IS NOT RUNNING STARTING BACKUP

sc.exe %BACKUP_NAME% start %AGENT_SVC_NAME%

TIMEOUT /T %SLEEP_SECS% /NOBREAK

sc.exe %BACKUP_NAME% query %AGENT_SVC_NAME% > sc.out

find /i "RUNNING" < sc.out
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

```
IF %ERRORLEVEL% == 0 (
  GOTO SCRIPT_END
)

GOTO FAILED_TO_START_BACKUP

:BACKUP_RUNNING
ECHO BACKUP %BACKUP_NAME% RUNNING

sc.exe %PRIMARY_NAME% query %AGENT_SVC_NAME% > sc.out
find /i "RUNNING" < sc.out
IF %ERRORLEVEL% == 0 (
  ECHO PRIMARY %PRIMARY_NAME% RUNNING
  GOTO STOP_BACKUP
)

ECHO BACKUP %BACKUP_NAME% IS RUNNING AND PRIMARY %PRIMARY_NAME% IS
STOPPED

GOTO SCRIPT_END


:STOP_BACKUP
ECHO STOPPING BACKUP %BACKUP_NAME%

sc.exe %BACKUP_NAME% stop %AGENT_SVC_NAME%

TIMEOUT /T %SLEEP_SECS% /NOBREAK

sc.exe %BACKUP_NAME% query %AGENT_SVC_NAME% > sc.out
find /i "RUNNING" < sc.out
IF %ERRORLEVEL% == 0 (
  GOTO FAILED_TO_STOP_BACKUP
)

ECHO BACKUP %BACKUP_NAME% STOPPED SUCCESFULLY

GOTO SCRIPT_END

:PRIMARY_LOGIC
ECHO RUNNING PRIMARY AGENT SERVER LOGIC

sc.exe %PRIMARY_NAME% query %AGENT_SVC_NAME% > sc.out
find /i "RUNNING" < sc.out

IF %ERRORLEVEL% == 0 (
  ECHO PRIMARY %PRIMARY_NAME% RUNNING
  GOTO SCRIPT_END
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

```
)

IF FIRST_PASS==0 GOTO FAILED_TO_START_PRIMARY
SET FIRST_PASS=0

ECHO PRIMARY %PRIMARY_NAME% NOT RUNNING CHECKING BACKUP

sc.exe %BACKUP_NAME% query %AGENT_SVC_NAME% > sc.out
Find /i "RUNNING" < sc.out
IF %ERRORLEVEL% == 0 (
  ECHO BACKUP %BACKUP_NAME% RUNNING
  GOTO SCRIPT_END
)

ECHO BACKUP %BACKUP_NAME% NOT RUNNING, STARTING PRIMARY

sc.exe %PRIMARY_NAME% start %AGENT_SVC_NAME%

TIMEOUT /T %SLEEP_SECS% /NOBREAK

GOTO PRIMARY_LOGIC

:FAILED_TO_STOP_BACKUP
ECHO ERROR: BACKUP %BACKUP_NAME% FAILED TO STOP WHEN PRIMARY
%PRIMARY_NAME% ALREADY RUNNING , EXITING...
GOTO SCRIPT_END

:FAILED_TO_START_BACKUP
ECHO ERROR: BACKUP %BACKUP_NAME% FAILED TO START, EXITING...
GOTO SCRIPT_END

:FAILED_TO_START_PRIMARY
ECHO ERROR: PRIMARY %PRIMARY_NAME% FAILED TO START, EXITING...
GOTO SCRIPT_END

:SCRIPT_END

DATE /T
TIME /T
ECHO AGENT CHECK COMPLETE
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.

Appendix 2

Agent workstation registry requirements

This appendix defines the Windows registry modifications required for the Auto Agent workstation. The Auto Agent workstation requires .NET 4.6.1 (and higher).

For .NET 4.6.1 (and higher)

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto"=dword:00000001
```

© 2025 Optum, Inc. and/or one of its subsidiaries. All rights reserved.