

People. Your most valuable asset.
Your greatest risk.

ObserveIT Proof of Concept Guide

ObserveIT is designed for simplicity and ease of deployment, configuration and use. Hands-on testing is an important aspect of the ObserveIT evaluation process. This guide is intended to serve as a Proof of Concept (POC) plan that any organization may use as a starting point for building their own customized plan. It outlines the necessary steps that are needed to begin working with ObserveIT. For more detailed instructions please consult either the online product documentation, or the product help file.

To assist in the creation of a more comprehensive plan, or if you have questions regarding this document, feel free to contact your technical representative.

This document has the following sections:

- **POC Phases of Testing**
 1. Deployment Evaluation Criteria
 2. Management and Operation Evaluation Criteria
- **POC Deployment Guidelines**
 3. Download the latest build of ObserveIT
 4. Meet hardware and software requirements
 5. Decide on what servers should be monitored
 6. Decide on the best way to deploy the ObserveIT Agent software
 7. Install ObserveIT server components
 8. Log on to the ObserveIT Management web console
 9. Install ObserveIT License
 10. Deploy the ObserveIT agents
 11. Begin recording sessions
 12. Finding the information you need
 13. View recorded sessions
 14. Implement a backup solution for the ObserveIT database
- **POC Testing Procedures**
 1. Case Scenario 1 - Troubleshooting Human Error
 2. Case Scenario 2 - ObserveIT Reporting

People. Your most valuable asset.
Your greatest risk.

POC Phases of Testing

Testing in this guide is divided into two phases: **Deployment**, and **Management and Operation**.

1. **Deployment tests** – ObserveIT evaluation should focus on the operational labor and administrative overhead required for initial pilot system installation and configuration.

Table 1: Deployment Evaluation Criteria	Score
To what extent were changes to web applications or network infrastructure required? (1=Significant change, 10 = Zero change)	
How much downtime was required? (1=Significant Downtime, 10 = Zero Downtime)	
How much operational labor was required for installation and configuration? (1=Significant labor, 10 = Zero labor)	
How much web application and general software development expertise was required? (1=Significant knowledge, 10 = Zero knowledge)	
Rate the product's overall ease of deployment (1=Difficult, 10=Easy)	

2. **Management and Operation tests** - ObserveIT should be measured by its effectiveness when using its features to generate reports and reply videos. Another measurement of effectiveness should be the consideration of having to use the built-in Windows Event Viewer logs or other application-specific log files in comparison to the ability to easily view user session transcripts and video recordings.

Table 2: Management and Operation Evaluation Criteria	Score
What was the amount of administrative overhead required to configure ObserveIT? (1=Significant amount, 10 = Zero amount)	
How complicated was the process of finding who accessed a specific application on one or more servers?	

People. Your most valuable asset.
Your greatest risk.

(1=Significant complexity, 10 = Zero complexity)	
How complicated was the process of finding all the applications accessed by a specific user across one or more servers? (1=Significant complexity, 10 = Zero complexity)	
How much web application and general software development expertise was required to generate usage reports? (1=Significant knowledge, 10 = Zero knowledge)	
How clear were the recorded textual transcripts in representing the user actions? (1=Totally unclear, 10 = Very clear)	
How clear were the recorded videos in representing the user actions? (1=Totally unclear, 10 = Very clear)	
How effective were the recorded textual transcripts in representing user actions versus having to go through the Event Viewer logs or other application-specific logs? (1=Totally ineffective, 10 = Very effective)	
Rate the product's overall ease of use (1=Difficult, 10=Easy)	

POC Deployment Guidelines

These guidelines will describe the steps needed to be taken in order to install, configure and use ObservelT. By following these steps you will have the best Proof of Concept experience for ObservelT's installation and usage. It is recommended that testing should be carried out in the order presented below.

1. Download the latest build of ObservelT

The latest build can be obtained at the following URL:

<http://www.observeit-sys.com/download.asp>

2. Meet hardware and software requirements

As with any software, there are minimum software and hardware requirements you should meet prior to installing ObservelT.

People. Your most valuable asset. Your greatest risk.

For most POC deployments, a simple server can be used to run the Application, Web Management, and Database server components. Actual recommended resources will depend on the number of Agents deployed, the amount of activity on each Agent, and the amount of historical data retained in the database.

The following is list of the minimum system requirements for each ObserveIT component:

Software Requirements

- **Application Server:** Windows 2000/2003/2008 Server, Internet Information Server (IIS), .NET Framework
- **Web Management Console:** Windows 2000/2003/2008 Server, Internet Information Server (IIS), .NET Framework
- **Database Server:** Windows 2000/2003/2008 Server, SQL Server 2000/2005
- **Agent:** Windows NT/2000/2003/XP/2008/Vista, .NET Framework

Hardware Requirements

ObserveIT's minimal hardware requirements are easily met in today's modern computer hardware specifications. However, in order to provide adequate performance for a major enterprise, one must make carefully plan the hardware specifications. For example, one of our existing clients uses the following hardware configuration to monitor approximately 1000 servers:

- **Application Server and Web Management Console:** Dual Core 3.2 GHz (4 MB); 2 GB RAM; 2 X 72 GB Disk (in a RAID 1 array)
- **Database Server:** Dual Core 3.2 GHz (4 MB); 4 GB RAM; 4 X 146 GB Disks (in a RAID 10 array)

3. Decide on what servers should be monitored

The ObserveIT Agent can be installed on any Windows-based server or workstation. While supported on Windows XP and Windows Vista, remember that ObserveIT is a server-side product. It is best to install the agent on servers that you wish to monitor and that will provide you with the base idea on the overall performance and usefulness of the recorded data. For instance, it is recommended that for the POC phase you do not install the agent on servers that are hardly ever accessed on one hand or on a very highly-loaded on the other hand. Choose servers that have a moderate user/administrator access workload.

People. Your most valuable asset. Your greatest risk.

4. Decide on the best way to deploy the ObserveIT Agent software

The deployment of the ObserveIT Agent can be done in several ways. Choose the right method suited for your needs:

- You can use the MSI file to deploy the ObserveIT Agent through GPO, SMS, SCCM or similar
- You can use either the EXE or the MSI files to manually install the ObserveIT Agent on each server
- You can use the provided batch file to automate the ObserveIT Agent installation

In most POC implementations, the ObserveIT Agent will only be installed on several servers; therefore for most scenarios the manual installation will be sufficient. For more information about the deployment options of the ObserveIT Agent please consult the online product documentation, or the product help file.

5. Install ObserveIT server components

Installation of the server components of ObserveIT can be done in one of 2 ways:

- **By using the “One Click Installation” method** - This installation method is recommended if you are installing all the ObserveIT Server components on a single platform, or if you will install the Web/Management and Application Servers on a single platform and have a separate SQL Server platform.
- **By performing a manual installation for each of the server components** – Useful when there is need to install each server component on a separate server. For this type of installation please refer to the product documentation.

The following instructions will take you step by step through the process of installing ObserveIT by using the “One Click Installation”.

1. Run *setup.exe* from ObserveIT's root folder which was created when you extracted the setup files from the archive, and respond “Yes” or “Run” to the security warnings.
2. You will see the main installation screen
3. If you are installing all components on the local server, use “[local]” for the destination server. Otherwise, select the remote SQL Server from the list.
4. If the account you are currently using is a SQL Server administrator, you can use Windows Authentication for the installation. Otherwise, choose “SQL Server authentication” and provide a User and Password with privileges to create databases and user accounts. If you select “Windows

People. Your most valuable asset. Your greatest risk.

Authentication” as the authentication method you will need to perform additional tasks. Please refer to the product documentation. Either way, you must use a SQL Server or Window login username that has 'dbcreator' privileges at the minimum. The default SQL Server login is "SA" (without the quotes). You can also use a Windows user that has administrative rights on the server.

5. Select the checkbox to agree to the Terms of Service and click “Install” to begin the installation.
6. As the installation proceeds, you will see messages about its progress in the text window.
7. When the installation is complete, click on “Exit” to close the ObserveIT Installer.
8. If there were any errors during the setup, you will be presented with a message describing the error. Please refer to the product documentation for additional troubleshooting information.

After installation, ObserveIT is already running, capturing, and recording any human interaction with any server that the agent is installed on.

6. Log on to the ObserveIT Management web console

The Web Console is available using a web browser and connecting to <http://servername/ObserveIT>

If you are logged in at the console of the server where the Web Console is installed, you can access it from Start Menu > All Programs > ObserveIT.

The default operator credentials are:

- User Name: admin
- Password: admin (note that passwords are case sensitive)

7. Install ObserveIT License

The first time you access the Web Management Console, you will need to activate the product.

1. Click the “Browse” button to get a list of files.
2. Find the license file provided to you by ObserveIT Software when you registered the product.
3. Click “Activate” to use the specified license file. If you do not have a license file, please contact Support to get a Demo license or your sales representative to get a full license. When your product has been activated, you will be taken automatically to the Web Management Console Login Screen.

People. Your most valuable asset. Your greatest risk.

8. Deploy the ObservelT agents

You will now need to install the ObservelT Agent on any additional server that you wish to monitor. The following steps will walk you through the manual installation process:

1. To run the ObservelT Agent Installer, run the *Setup.exe* file located in the *ObservelTAgent* folder which was created when you extracted the setup files from the archive.
2. When you execute the Installer, you might see a Security Warning telling you that the publisher could not be verified. Click "Run" to continue.
3. Next, specify a URL to the ObservelT Application Server, the one which the Agent will communicate with. Click "Next" to continue. If you've made changes to the default port add a ":<port number>" (without the quotes) to the end of the URL. For example, if the ObservelT Application server was installed on a server named "SRV100", the URL would look like this:
"*HTTP://SRV100/ObservelTApplicationServer*" (without the quotes).
4. When the installation is complete, click "Close" to exit.

For more information about the deployment options of the ObservelT Agent please consult the online product documentation, or the product help file.

9. Begin recording sessions

By default, ObservelT is configured to begin recording all user access to the monitored servers. Therefore, you do not need to perform any additional tasks in order to begin recording.

For more information about the Recording Policy configuration options of the ObservelT please consult the online product documentation, or the product help file.

10. Finding the information you need

One of the main benefits of ObservelT is its ability to quickly locate the information you need. This is done by using one of the following views, all of which are accessed from the ObservelT Web Management Console.

In the ObservelT Web Management Console, use the Serve Diary, User Diary, or FreeText Search tabs to find the session you're interested in viewing.

People. Your most valuable asset. Your greatest risk.

- **Server Diary** – Shows “who did what” on a server. Each user session is listed by date and can be expanded to see exactly what the user accessed. Sessions can be viewed in the Slide Viewer to see the sequence of actions.
- **User Diary** – Shows all activity on all servers for a user. You can see the user’s actions by session or you can see a list by the resources (applications, configuration settings, files, etc.) that the user accessed. The Slide Viewer can be used to see the sequence of actions for any particular session or resource access.
- **Reports** – Reports are created by querying from three main components – server, user, and a resource which can be any screen element that the user interacts with: menus, application dialog, files, etc. For example, you can list users that have accessed selected servers by date and time or list resources (applications, screens, files, registry entries, etc.) that were accessed on selected servers by date and time.
- **FreeText Search** – Because ObserveIT captures metadata in addition to screenshots, you can search for text that matches an application name, a registry key, a file or directory name or any other information related to a user’s activity.
- **Context Sensitive Search** – Press F12 to find all previous activity for the currently accessed Resource. The feature is available at all times to get a list of previous user actions related to that configuration setting and see exactly what choices were made.

For more information about using each of the search options please consult the online product documentation, or the product help file.

11. View recorded sessions

ObserveIT allows you to replay recorded sessions by using a VCR-like Slide Viewer or player. The Slide-Viewer opens in a separate browser window. The ObserveIT's Slide Viewer can be used to play the recorded session starting from the first slide, and through the entire recording till it reaches the last slide. The Slide Viewer can also be used to begin playing the recorded session starting from a specific point in time. This feature saves time and allows the auditor or administrator to move to the exact point in time when the specific action that was performed by the user is of particular interest.

In the ObserveIT Web Management Console, use the Server Diary, User Diary, or FreeText Search tabs to find the session you're interested in viewing.

People. Your most valuable asset. Your greatest risk.

In order to reply the entire recorded session from start to finish, click on the black player icon on the right of the corresponding session line to launch the Slide Viewer and begin viewing the recorded session.

You can expand the session you're interested in by clicking the + sign on the left of the user session and read through the textual transcript of the recorded session. If you need to begin replying it from a specific point in time click the orange player icon on the right of the corresponding line.

ObserveIT's Slide Viewer will open in a new browser window and begin playing the recorded session. You can use the VCR-like buttons to quickly stop, resume, rewind or fast forward the playing of the slides. You can also zoom in or out in order to get a better view of the recorded screenshot.

By looking at the lower right-hand textual description imprinted on the recorded session you can keep track of the date time when the action was performed, the number of slides in that session and the number of current slide that is displayed on the player.

12. Implement a backup solution for the ObserveIT database

All the data captured by ObserveIT for Servers along with the configuration data is stored within a Microsoft SQL database. By utilizing your existing backup solutions you can easily backup your SQL server, and thus protect your ObserveIT data and configuration. Please consult your backup software manual for information on how to backup the SQL server.

POC Testing Procedures

In order to collect performance data as well as understand the ObserveIT functionality, two case scenarios are suggested:

1. Case Scenario 1 - Troubleshooting Human Error
2. Case Scenario 2 - ObserveIT Reporting

Case Scenario 1 - Troubleshooting Human Error

People. Your most valuable asset. Your greatest risk.

Use this scenario to recreate a human error that has disabled the Microsoft Error Reporting feature and changed the startup type of the Messenger service. By using ObserveIT, the human error will easily be found and fixed.

This scenario demonstrates the usage of the **ObserveIT Server Diary**, **User Diary** and **FreeText Search**.

Making the configuration change that will simulate the human error:

1. On one of the monitored servers, right-click "My Computer" and select "Properties". Go to the "Advanced" tab.
2. Click on the "Error Reporting" button. The default setting of the error reporting is to send errors to Microsoft. Select "Disable Error Reporting". Click Ok all the way out.
3. On one of the monitored servers, open "Services" from the Administrative Tools folder in the Control Panel or Start menu.
4. Locate the "Messenger" service, and double-click on it.
5. The default startup type setting for this service should be "Disabled". Change the startup type to "Manual". Click "OK".
6. Repeat steps 3-5 on a different monitored server.

Using the ObserveIT **Server Diary** to find the configuration error:

1. Logon to the ObserveIT web management console.
2. On the "**Server Diary**" tab, make sure "**Activities**" is selected. Then, locate the server and the date corresponding with the date where the above actions were performed. Note that the field is self-filling according to the servers that are known to ObserveIT. Click "Go".
3. Note the date, user name and client name from where the actions were performed.
4. Expand the recording that matches the actions above and look at the transcript. Amongst the items listed you should see System Properties > Error Reporting, then Services > Messenger Properties (Local Computer). Each line has a corresponding play button that allows you to view the exact point in time where the action was performed.
5. On the "**Server Diary**" tab, make sure "**Applications**" is selected. The server and the date corresponding with the date where the above actions were performed should already be selected.
6. Amongst the items listed you should see Run a DLL as an App > System Properties and Error Reporting, and Microsoft Management Console > Services and Messenger Properties (Local Computer). Again, each line

People. Your most valuable asset. Your greatest risk.

representing an application has a corresponding play button that allows you to view the exact point in time where the action was performed.

Using the ObservelT **User Diary** to find the configuration error:

1. Logon to the ObservelT web management console.
2. On the “**User Diary**” tab, make sure “**Activities**” is selected. Then, type the user name that has performed the actions described above. Note that the field is self-filling according to the users that are known to ObservelT. Click “Go”.
3. You can filter the results based on server names. Select the server corresponding with the above actions.
4. Note the date, user name and client name from where the actions were performed.
5. Expand the recording that matches the actions above and look at the transcript. Amongst the items listed you should see System Properties > Error Reporting, then Services > Messenger Properties (Local Computer). Each line has a corresponding play button that allows you to view the exact point in time where the action was performed.
6. On the “**User Diary**” tab, make sure “**Resources**” is selected. The user name should already be selected.
7. Note that you can filter the results based on application names.
8. If you don't filter by applications, you will see a detailed list of all the applications that have been accessed by that user in the past month. Each application has an expanding menu showing you on which server they have been accessed and a corresponding play button that allows you to view the exact point in time where the action was performed.

Using the ObservelT **Free Text Search** capability to find the configuration error:

1. Logon to the ObservelT web management console.
2. On the “**Search**” tab, type the application name, or window name that you are looking for. For example, you can type “error” or “messenger”. Click “Search”.
3. Note the date, user name and client name from where the actions were performed.
4. Expand the recording that matches the actions above and look at the transcript. Amongst the items listed you should see System Properties > Error Reporting, then Services > Messenger Properties (Local Computer). Each line has a corresponding play button that allows you to view the exact point in time where the action was performed.

People. Your most valuable asset. Your greatest risk.

Case Scenario 2 - ObservelT Reporting

This scenario displays the simplicity of slicing and finding data aggregated from multiply servers/workstation. Advanced reporting will generate reports for selected application usage, selected users activity and selected server/workstation activities. This scenario will show how to find all people who accessed the Registry editor across all servers/workstations, find all activities a selected person has done across all servers/workstation and view all activities performed on a single server/workstation.

Making the configuration change that will simulate the human error:

1. On one of the monitored servers, open the Registry editor (regedit.exe) from the Start > Run menu.
2. Navigate to the following path:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger
3. Double-click on the "Start" DWORD value. If you've performed the tasks described in scenario #1 above, the value listed should be 3. Change the value to 4, and click "OK".
4. If you haven't made the changes listed in scenario #1, then the value should be 4. In any case, make sure you double-click on the value, and after the Edit DWORD Value window is displayed, close it without making any changes.
5. Navigate to the following path:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting
6. Double-click on the "DoReport" DWORD value. If you've performed the tasks described in scenario #1 above, the value listed should be 0. Change the value to 1, and click "OK".
7. If you haven't made the changes listed in scenario #1, then the value should be 1. In any case, make sure you double-click on the value, and after the Edit DWORD Value window is displayed, close it without making any changes.
8. Close the Registry editor.
9. Repeat steps 3-5 on a different monitored server.

Using the ObservelT **Reports** capability to find the configuration error:

1. Logon to the ObservelT web management console.
2. Navigate to "**Reports**" tab.
3. To generate a report of all the users and times where the Registry editor has been accessed, select "**Registry Editor**" entry from the "**Application**" dropdown list.

People. Your most valuable asset.
Your greatest risk.

4. Click on the “**Generate Report**” to generate a report of all people that accessed the Registry editor across all servers or workstation.
5. Clear the “**Application**” dropdown list by selecting the “**choose**” entry.
6. To generate a report of all the applications accessed by a specific user, type a login name in the “**Login**” textbox
7. Click on the “**Generate Report**”.
8. Clear the “**Login**” textbox.
9. To generate a report of all the users that have accessed a specific server, and the applications these users used, type a server/workstation name in the agent textbox
10. Click on the “**Generate Report**”.