

# PERFORMING A CUSTOM INSTALLATION OF OBSERVEIT

# TABLE OF CONTENTS

<b>TABLE OF CONTENTS</b> .....	<b>2</b>
<b>OVERVIEW</b> .....	<b>4</b>
DOCUMENT VERSIONS .....	4
PRODUCT VERSION .....	4
RELEASE DOCUMENTATION .....	4
DOCUMENTATION FEEDBACK.....	4
PREREQUISITES AND ASSUMPTIONS FOR THIS DOCUMENT .....	5
INSTALLATION PROCESS OVERVIEW .....	7
DOWNLOADING THE LATEST VERSION .....	8
<b>PREPARING THE ENVIRONMENT</b> .....	<b>9</b>
FORMATTING A DISK FOR GRAPHIC IMAGES STORAGE AND THE DATABASE.....	9
CREATING AND SHARING THE GRAPHICS IMAGE FOLDERS .....	10
INSTALLING PREREQUISITES .....	10
CONFIGURING WINDOWS FIREWALL.....	11
<i>Configuring Windows Firewall on SQL server</i> .....	11
<i>Configuring Windows Firewall on ObserveIT Application Server</i> .....	11
<b>PREPARING PERMISSIONS</b> .....	<b>12</b>
CREATING A SERVICE ACCOUNT USER IN ACTIVE DIRECTORY .....	12
ASSIGNING SQL PERMISSIONS TO THE SERVICE ACCOUNT USER.....	12
ADDING THE SERVICE ACCOUNT USER TO THE LOCAL ADMINISTRATORS GROUP .....	13
ADDING THE SERVICE ACCOUNT USER TO THE LOCAL IIS_IUSRS GROUP .....	14
<b>INSTALLING AND CONFIGURING DATABASES</b> .....	<b>15</b>
INSTALLATION OVERVIEW .....	15
CHOOSING THE LOCATION OF THE RECORDED GRAPHIC SCREENSHOTS STORAGE .....	15
EDITING THE DATABASE INSTALLER TO USE FILE SYSTEM STORAGE FOR RECORDED GRAPHIC SCREENSHOTS .....	16
INSTALLING THE OBSERVEIT DATABASES .....	17
VERIFYING SUCCESSFUL DATABASE INSTALLATION .....	19
CONFIGURING SIMPLE RECOVERY MODEL FOR THE OBSERVEIT DATABASES ON THE SQL SERVER .....	19
PLACING THE DATABASE FILES ON DESIGNATED DRIVES.....	20
SETTING INITIAL MDF AND LDF FILE SIZE FOR THE OBSERVEIT DATABASES ON THE SQL SERVER .....	22
INSTALLING THE AUTOMATED MAINTENANCE PROCEDURE .....	24
<b>CONFIGURING THE INTERNET INFORMATION SERVICES</b> .....	<b>25</b>
PREPARING IIS TO INSTALL THE OBSERVEIT WEB APPLICATIONS.....	25
ASSIGNING A DIGITAL CERTIFICATE FOR THE WEB CONSOLE .....	25
<i>Option 1: Creating an internal Enterprise Certificate Authority certificate for the Web Console</i> .....	25
<i>Option 2: Creating a self-signed certificate for the Web Console</i> .....	26
CREATING AND CONFIGURING THE OBSERVEIT APPLICATION POOL.....	26
CREATING THE WEBSITE FOR THE OBSERVEIT APPLICATION SERVER .....	27
CREATING THE WEBSITE FOR THE OBSERVEIT WEB CONSOLE .....	28
<b>INSTALLING THE OBSERVEIT COMPONENTS</b> .....	<b>29</b>
INSTALLING THE OBSERVEIT APPLICATION SERVER.....	29
VERIFYING THE OBSERVEIT APPLICATION SERVER INSTALLATION .....	29
INSTALLING ADDITIONAL OBSERVEIT APPLICATION SERVERS.....	30

INSTALLING THE OBSERVEIT WEB MANAGEMENT CONSOLE.....	30
VERIFYING THE WEB MANAGEMENT CONSOLE INSTALLATION.....	31
CONFIGURING THE OBSERVEIT SERVICES .....	31
INSTALLING THE WEB CATEGORIZATION MODULE .....	32
<i>Prerequisites for installing the Website Categorization module .....</i>	<i>32</i>
<i>Performing the Website Categorization module installation .....</i>	<i>33</i>
<i>Configuring Internet proxy settings for Website Categorization module.....</i>	<i>33</i>
<b>CONFIGURING OBSERVEIT INSTALLATION.....</b>	<b>35</b>
CONFIGURING THE DEFAULT OBSERVEIT ADMIN PASSWORD.....	35
GENERATING THE LICENSE REGISTRATION KEY (FOR NON-TRIAL INSTALLATIONS ONLY) .....	35
INSTALLING THE OBSERVEIT LICENSE.....	36
CONFIGURING LDAP SETTINGS.....	36
CONFIGURING SMTP SETTINGS.....	37
<b>CONFIGURING ENCRYPTION .....</b>	<b>38</b>
DATA IN TRANSIT ENCRYPTION OVERVIEW AND REQUIREMENTS.....	38
CONFIGURING OBSERVEIT APPLICATION SERVER FOR DATA IN TRANSIT ENCRYPTION .....	38
CONFIGURING OBSERVEIT AGENTS FOR WINDOWS TO USE SSL.....	39
<i>New ObserveIT Agent installations.....</i>	<i>39</i>
<i>Existing ObserveIT Agent installations.....</i>	<i>39</i>
CONFIGURING OBSERVEIT AGENT FOR UNIX/LINUX TO USE SSL .....	40
ENCRYPTING THE OBSERVEIT APPLICATION SERVER TO DATABASE SERVER TRAFFIC.....	40
CONFIGURE OBSERVEIT IMAGE SECURITY .....	42
<b>INSTALLING OBSERVEIT AGENTS.....</b>	<b>43</b>
INSTALLING OBSERVEIT AGENT FOR WINDOWS .....	43
INSTALLING OBSERVEIT AGENT FOR UNIX/LINUX .....	44
VERIFYING SUCCESSFUL USER ACTIVITY RECORDING .....	45
<b>APPENDIXES.....</b>	<b>46</b>
SETTING THE OBSERVEIT DATABASES TO A SIMPLE RECOVERY MODE.....	46

# OVERVIEW

ObserveIT can be easily and quickly installed using the default “One Click” installation, with product deployment taking under 15 minutes from start to first session replay.

However, in some cases, customers may want to manually install each component of ObserveIT. This is usually true for environments with higher security procedures, requiring each component of the ObserveIT product to be installed separately and using dedicated service accounts; or in large-scale environments requiring custom modifications of some of the server-side components.

This document contains detailed procedures and instructions on how to install ObserveIT by performing a custom installation.

## Document versions

Creator/Contributor/Editor	Date	Version
Jonathan Boyko	August 27, 2017	0.2

## Product version

Date	Product Version
August 27, 2017	7.1.0.136

## Release documentation

The most up-to-date release documentation is available at: <http://documentation.observeit.com/>.

## Documentation feedback

ObserveIT is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to: [doc@observeit.com](mailto:doc@observeit.com).

## Prerequisites and Assumptions for this document

In this document, it is assumed the following deployment architecture will be used:

Name	Function	Software
SQLSrv	Database server File Server	MSSQL Server 2016 Standard Windows Server 2016 Standard SQL Management Studio 17
OITsrv1	ObserveIT Application Server ObserveIT Web Console	Windows Server 2016 Standard Microsoft IIS 10
OITAgent	ObserveIT Agent	Windows Server 2016 Standard

When a more complex environment is required, the following deployment architecture will be used:

Name	Function	Software
SQLSrv	Database server File Server	MSSQL Server 2016 Standard Windows Server 2016 Standard SQL Management Studio 17
OITsrv1	ObserveIT Application Server #1	Windows Server 2016 Standard Microsoft IIS 10
OITsrv2	ObserveIT Application Server #2	Windows Server 2016 Standard Microsoft IIS 10
OITweb	ObserveIT Web Console	Windows Server 2016 Standard Microsoft IIS 10
FILEsrv	File Share	Windows Server 2016 Standard
OITAgent	ObserveIT Agent	Windows Server 2016 Standard

For all computers, these prerequisites are met:

- All computers are members of the same Active Directory domain
- Logon permissions to these computers with administrative permissions (local administrator)
- Permissions to create a service account user in Active Directory
- Permissions to access the SQL Server database engine (SYSADMIN permissions)
- Permissions to grant the service account DBCREATOR permissions on the SQL Server
- Full network connectivity with no firewall restrictions between the components of the deployment, or permissions to create the appropriate firewall rules to allow the requested traffic type

For data encryption (data in transit, data at rest, Web Console traffic):

- An internal Certificate Authority (CA) capable of issuing the correct digital certificates (it is possible to use self-signed certificates, however that may add complexity to the deployment)

For detailed instructions, hardware recommendations and sizing – please refer to the “ObserveIT General Prerequisites and Recommendations” document which can be obtained by contacting ObserveIT’s professional Services team at [proserv@observeit.com](mailto:proserv@observeit.com).

Other assumptions this document makes are:

- This guide assumes installation on Windows Server 2016 and SQL Server 2016. This guide also assumes SQL Management Studio version 17 is installed. All commands and queries performed in this guide are tested to work on with these components at their latest iterations.
- The server hosting the ObserveIT server-side website application is a member of an Active Directory domain, but not a domain controller (DC). Hosting IIS on a domain controller may cause adverse security issues and should be avoided. However, it may be possible when installing in an isolated lab environment. When installing on a DC, you need to use the “Active Directory Users and Computers” MMC snap-in, and add the ObserveIT service account to the “Administrators” group found in the “Builtin” container, but this will affect all the DCs in the domain.
- You are performing the installation using the default values such as folder structures, file sizes and logon account names.
- The reader has prior knowledge of Public Key Infrastructure (PKI) and its related terminology.
- Your organization has an SQL server administrator who follows the best practices for deploying and maintaining SQL server.
- Your organization has backups administrator, who follows best practices for backing up databases, Operating Systems, and file shares.

## Installation process overview

The installation steps include:

1. Preparing the environment:
  - 1.1. Format a disk for graphic images storage and the database.
  - 1.2. Create and sharing the graphics image folders.
  - 1.3. Install prerequisites.
  - 1.4. Configure Windows Firewall.
2. Preparing permissions:
  - 2.1. Create a Service Account in the Active Directory.
  - 2.2. Assign SQL permissions to the Service Account user.
  - 2.3. Add the Service Account user to the local permission groups.
3. Install ObserveIT databases:
  - 3.1. Choose image storage location.
  - 3.2. Install the databases.
  - 3.3. Verify installation.
  - 3.4. Configure database recovery model.
  - 3.5. Place the database file on designated drives.
  - 3.6. Set initial database file sizes.
  - 3.7. Install the automated maintenance procedure.
4. Configure the IIS:
  - 4.1. Prepare the IIS for ObserveIT web applications.
  - 4.2. Assign a digital certificate to the ObserveIT web applications.
  - 4.3. Create and configure the ObserveIT Application Pool.
  - 4.4. Create websites for ObserveIT Application Server and Web Console.
5. Install ObserveIT components:
  - 5.1. Install ObserveIT Application Server and verify installation.
  - 5.2. Install ObserveIT Web Console and verify installation.
  - 5.3. Install additional ObserveIT Application Servers (if required).
  - 5.4. Configure ObserveIT services.
  - 5.5. Install ObserveIT Website Categorization module.
6. Configure ObserveIT installation:
  - 6.1. Configure the default *Admin* password.
  - 6.2. Generate license registration key and install the license.
  - 6.3. Configure LDAP and SMTP.
7. Configure encryption (if required):
  - 7.1. Configure ObserveIT Application Server for data encryption.
  - 7.2. Configure ObserveIT Agents for Windows to use SSL.
  - 7.3. Configure ObserveIT Agents for Unix/Linux to use SSL.
  - 7.4. Configure the ObserveIT Application Server to database server traffic.
  - 7.5. Configure ObserveIT Image Security.
8. Install ObserveIT Agents:
  - 8.1. Install ObserveIT Agent for Windows.
  - 8.2. Install ObserveIT Agent for Unix/Linux.
  - 8.3. Verify successful activity recording.

## Downloading the latest version

To download the application files containing the .MSI installers that are required for the installation:  
[http://www.observeit.com/support/product\\_releases\\_download?download=1](http://www.observeit.com/support/product_releases_download?download=1)

Copy binaries to the ObserveIT Application server to C:\Temp. Extract the content of the ZIP file to C:\Temp.

**Note: File location screenshots and paths are updated to the GA version as of May 2016, but should remain unchanged in future versions.**

A new folder will be created.

## PREPARING THE ENVIRONMENT

This section describes preparation of your Windows Server machines for ObserveIT deployment. It assumes the server machines have Windows Server 2016 Operating System installed, and that it is up-to-date.

### Formatting a disk for graphic images storage and the database

As a matter of best practice, ObserveIT recorded images should be stored on a file share. This guide assumes the file share is to be located on a Windows Server 2016 Operating System, and describes the procedure to configure the disks (and later – the file share) on this Operating System.

By default, all the recorded graphic screenshots are stored in the "ObserveIT\_Data" database.

In medium to large deployments of ObserveIT, it is recommended to configure all recorded graphic screenshots to be stored in the file system network share (a UNC path) instead of in the SQL database. This will reduce the overall I/O overhead on the SQL Server.

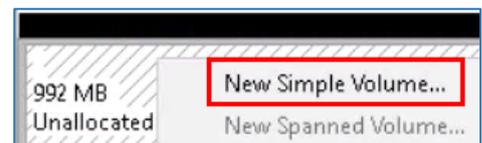
Because all the graphic images are typically small, the disk on which they will be located needs to be formatted in ReFS for Windows Server 2016 and NTFS for Windows Server 2012R2 and lower, using the allocation unit size of 4KB (4096K). This will ensure best disk location usage and reduce disk space waste. This can be done using Disk Management or the DISKPART command line utility.

**Note: Do not enable disk compression.**

To format the disk using the Disk Management snap-in, follow these steps:

**Note: This guide assumes the new disk has just been connected to the machine and no action was performed on it.**

1. Connect to the computer acting as the ObserveIT file share.
2. Open the Start menu and type in `COMPMGMT.MSC`. Press the Enter key.
3. Expand the Computer Management (Local) node, expand the Storage node, and click the Disk Management node.
4. Find the new disk in the list. Usually, it is the only one with the status Offline.
5. Right-click the disk and select Online.
6. Right-click the disk again and select Initialize Disk.
7. Click the GPT (GUID Partition Table) radio button and click OK.
8. Right-click the partition and select New Simple Volume.
9. Click Next.
10. Make sure maximum the values specified in the Maximum disk space in MB and Simple volume size in MB are equal. Click Next.
11. Assign an appropriate drive letter. Click Next.
12. Click the Format this volume with the following settings radio button and select **ReFS** (for Windows Server 2016) or **NTFS** (for Windows Server 2012R2 or lower) at the File system field.
13. Set the Allocation unit size:
  - a. 4096 for image storage.
  - b. 64KB for SQL database.



14. Assign an appropriate volume label at the `Volume Label` field.
15. Make sure `Perform a quick format` checkbox is checked.
16. Click `Next` and review the settings. Click `Finish`.

## Creating and sharing the graphics image folders

This step is provided as reference purposes. For instructions on using a Network Access Storage (NAS) or a different storage type please see your storage vendor documentation.

To create and share folders at a Windows Server file server follow these steps:

1. Connect to the computer acting as the ObserveIT file share.
2. Open the `Start` menu and type in `EXPLORER`. Press the `Enter` key.
3. Navigate to a disk where the ObserveIT image store folder is to be located.
4. Right-click the empty space inside the File Explorer window, click `New` and click `Folder`.
5. Give the folder an appropriate name, for example: `OITImages`.
6. Right-click the folder, click `Share With`, and click `Specific people`.
7. Type in `OITServiceAccount` and click `Add`.
8. At the `Permission Level` for the `OITServiceAccount` account choose `Read/Write`. Click `Share`.
9. Perform steps 3-8 for the ObserveIT Archive folder, for example: `Oligarchize`.



## Installing prerequisites

ObserveIT Application Server and ObserveIT Web Console require several prerequisites, such as the Microsoft Internet Information Services and the .Net Framework. To install the prerequisites automatically, please follow these steps:

1. Mount a Windows Server 2016 installation DVD to the virtual machine, or insert a Windows Server 2016 DVD into the DVD drive of the server.
- Note: The following steps are similar for Windows Server 2012/2012R2 Operating Systems. If using one of these systems, mount or insert the appropriate DVD to the machine.**
2. Open the `Start` menu and type in `POWERSHELL`.
  3. Right-click the PowerShell shortcut and choose `Run as administrator`.
  4. If prompted `Do you want to allow this app to make changes to your device?` click `Yes`.
  5. Paste the following command, replacing the `<dvddrive>` string with the letter of the DVD drive in your machine:

```
Import-Module ServerManager
Install-WindowsFeature Web-Server, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-Dir-Browsing, Web-Http-Errors, Web-Static-Content, Web-Health, Web-Http-Logging, Web-Performance, Web-Stat-Compression, Web-Security, Web-Filtering, Web-App-Dev, Web-Net-Ext, Web-Net-Ext45, Web-Asp, Web-Asp-Net, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Mgmt-Tools, Web-Mgmt-Console, Web-Mgmt-Compat, Web-Metabase, Web-Lgcy-Mgmt-Console, Web-Lgcy-Scripting, Web-WMI -
IncludeManagementTools -Source <dvddrive>:\Sources\SxS
Add-WindowsFeature NET-Framework-45-Core, NET-Framework-45-Features -Source
<dvddrive>:\Sources\SxS
```

## Configuring Windows Firewall

In instances when Windows Firewall is enabled, an additional step of configuring the firewall may be required. Please follow these steps to configure Windows Firewall:

### Configuring Windows Firewall on SQL server

**Note:** This guide assumes default ports are used.

1. Open the Start menu and type Run. Press the Enter key.
2. Type in `POWERSHELL`.
3. Right-click the PowerShell shortcut and choose Run as administrator.
4. If prompted Do you want to allow this app to make changes to your device? click Yes.
5. Paste the following code into the PowerShell window:
 

```
New-NetFirewallRule -DisplayName "SQL Server" -Direction Inbound -Protocol TCP -LocalPort 1433 -Action allow
New-NetFirewallRule -DisplayName "SQL Admin Connection" -Direction Inbound -Protocol TCP -LocalPort 1434 -Action allow
New-NetFirewallRule -DisplayName "SQL Database Management" -Direction Inbound -Protocol UDP -LocalPort 1434 -Action allow
New-NetFirewallRule -DisplayName "SQL Service Broker" -Direction Inbound -Protocol TCP -LocalPort 4022 -Action allow
New-NetFirewallRule -DisplayName "SQL Debugger/RPC" -Direction Inbound -Protocol TCP -LocalPort 135 -Action allow
#Enabling SQL Analysis Ports
New-NetFirewallRule -DisplayName "SQL Analysis Services" -Direction Inbound -Protocol TCP -LocalPort 2383 -Action allow
New-NetFirewallRule -DisplayName "SQL Browser" -Direction Inbound -Protocol TCP -LocalPort 2382 -Action allow
```
6. Close the PowerShell window.

### Configuring Windows Firewall on ObserveIT Application Server

Note: This guide assumes default ports are used.

1. Open the Start menu and type Run. Press the Enter key.
2. Type in `POWERSHELL`.
3. Right-click the PowerShell shortcut and choose Run as administrator.
4. If prompted Do you want to allow this app to make changes to your device? click Yes.
5. Paste the following code into the PowerShell window:
 

```
New-NetFirewallRule -DisplayName "HTTP" -Direction Inbound -Protocol TCP -LocalPort 4884 -Action allow
New-NetFirewallRule -DisplayName "SSL" -Direction Inbound -Protocol TCP -LocalPort 443 -Action allow
```
6. Close the PowerShell window.

## PREPARING PERMISSIONS

### Creating a service account user in Active Directory

Use the following steps to create a service account user in Active Directory that will be used for connecting to the ObserveIT databases, also used for running the ObserveIT services:

1. Connect to a Domain Controller or to a computer with Active Directory Remote Server Administration Tools installed.
2. Click `Start` and type in `DSA.MSC` and press `Enter` key.
3. Navigate to the Organizational Unit where the ObserveIT Service Account will be located.
4. Right-click the Organizational Unit, click `New > User`.
5. Optional: Type in `OBSERVEIT` into the First Name field, `SERVICE ACCOUNT` into the Last Name field.
6. Type in `OITSERVICEACCOUNT` into the User logon name field and choose the appropriate UPN suffix. Click `Next`.
7. Configure a password based on your organization's password policy requirements, uncheck the `User must change password at next logon` checkbox, and check the `Password never expires` checkbox. Click `Next`. Click `Finish`.
8. Close the Active Directory Users and Computers window.

Active Directory User Creation dialog box. Fields include: Create in: joit.lab/JOIT/Consulting; First name: ObserveIT; Last name: Service Account; Full name: ObserveIT Service Account; User logon name: ObserveITServiceAccount; User logon name (pre-Windows 2000): JOIT\ObserveITServiceAccd.

Password and Account Options dialog box. Fields include: Password: [dots]; Confirm password: [dots]; User must change password at next logon: ; User cannot change password: ; Password never expires: ; Account is disabled: .

**Note:** From now on, this document assumes "OITServiceAccount" as the Service Account username.

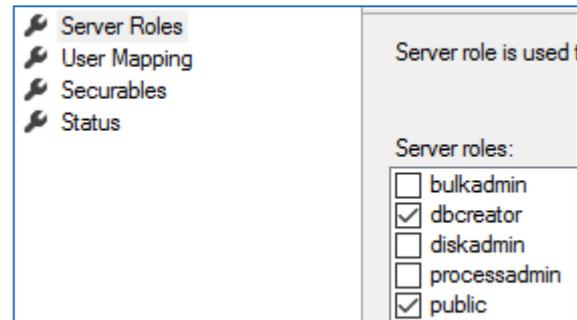
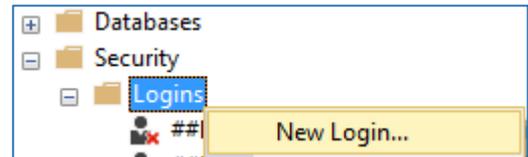
### Assigning SQL permissions to the Service Account user

Use the following steps to grant the ObserveIT Service Account user the `dbcreator` role on the SQL server.

**Note:** This permission is required only during the installation phase, and may be removed when the installation is complete. However, please note, that removing this permission will prevent ObserveIT from creating additional archive databases with the service account, and will require appropriate credentials when creating a new archive.

1. Connect to the SQL server or to a computer with SQL Management Studio installed.
2. Open the `Start` menu, expand the Microsoft SQL Server 2016 folder and click `SQL Management Studio`.
3. Type in the SQL server's FQDN or IP address into the `Server name` field.

4. Choose `Windows Authentication` if your account has `sysadmin` permissions on the SQL server. Otherwise, choose `SQL Server Authentication` and log in with a `sysadmin`-level account.
5. Click `OK` to connect.
6. Expand `Security`. Right-click `Logins` and choose `New Login`.
7. Click `Search`.
8. Click `Locations` button and choose the location where the `ObserveIT Service Account` is located. Click `OK`.
9. In the `Enter the object name to select` box type the username for the `ObserveIT Service Account` user account, in this instance - `OITSERVICEACCOUNT`. Click `OK`.
10. Click `Server Roles` from `Select a Page` menu.
11. Check the `dbcreator` checkbox. Click `OK`.
12. Close the `SQL Management Studio` window.

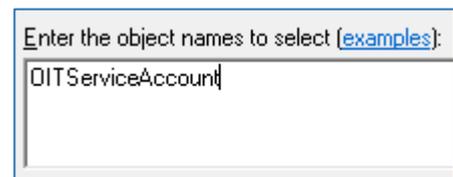
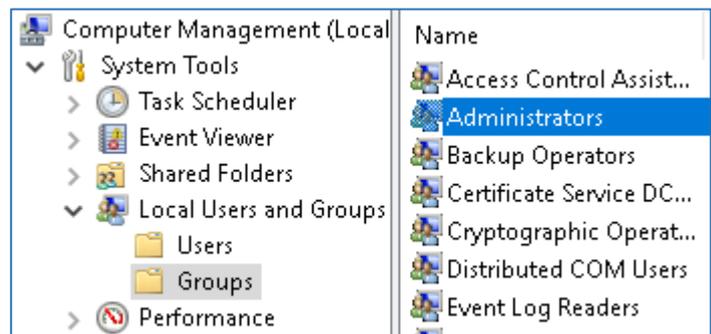


## Adding the Service Account user to the local Administrators group

Use the following steps to add the `ObserveIT` service account user to the local `Administrators` group on the `ObserveIT Application Server(s)` and `Web Console` machine (if installed on a separate computer).

**Note:** This is only required during the installation phase; it can be removed as soon as the installation has completed successfully.

1. On the `ObserveIT Application Server`, click the `Start` button.
2. Type in `COMPMGMT.MSC`. Press `Enter` key.
3. Expand `System Tools` and click `Local Users and Groups`.
4. Expand `Groups` and double-click the `Administrators` group.
5. Click the `Add` button. In the `Enter the object name to select` box type the username for the `ObserveIT Service Account` user account, in this instance - `OITSERVICEACCOUNT`. Click `OK`.
6. Click `OK`. Click `OK` in the next window.
7. If you plan to deploy more than one `ObserveIT Application Server`, or if you plan to install the `ObserveIT Web Console` on a separate machine, repeat on all the computers that will host the `ObserveIT Application` and `Web Console` applications.



## Adding the Service Account user to the local IIS\_IUSRS group

Use the following steps to add the ObserveIT service account user to the local IIS\_IUSRS group on the ObserveIT Application Server(s) and the Web Console machine (if installed on a separate computer).

**Note: This step is only required during the installation phase; it can be removed as soon as the installation has completed successfully.**

1. On the ObserveIT Application Server, click the Start button.
2. Type in `COMPUTER MANAGEMENT`. Press Enter key.
3. Expand `System Tools` and click `Local Users and Groups`.
4. Expand `Groups` and double-click the `IIS_IUSRS` group.
5. Click the Add button. In the Enter the object name to select box type the username for the ObserveIT Service Account user account, in this instance - `OITSERVICEACCOUNT`. Click OK.
6. Click OK. Click OK in the next window.
7. If you plan to deploy more than one ObserveIT Application Server, or if you plan to install the ObserveIT Web Console on a separate machine, repeat on all the computers that will host the ObserveIT Application and Web Console applications.

# INSTALLING AND CONFIGURING DATABASES

## Installation overview

The database is the first component of ObserveIT that needs to be installed. To successfully install the database, you would need to:

1. Choose the location of the recorded graphic screenshots storage.
2. Edit the database installer configuration file to use file system storage for recorded graphic screenshots.
3. Install the ObserveIT databases.
4. Install the ObserveIT Analytics database.
5. Add the ObserveIT Application Server(s) machine account to the ObserveIT databases.

## Choosing the location of the recorded graphic screenshots storage

By default, all the recorded graphic screenshots are stored in the "ObserveIT\_Data" database.

In medium to large deployments of ObserveIT, it is strongly recommended to configure all recorded graphic screenshots to be stored in the file system network share (a UNC path) instead of in the SQL database. This will reduce the overall I/O overhead on the SQL Server.

**Note: A functional SQL Server database is still required for storing all the recorded metadata, image pointers, and configuration settings.**

**Note: Due to NTFS file system limitations, you must create a new share when the current one reaches approximately 4 billion objects. This can be done through the Web Console.**

For example, you could use this type of UNC paths for the production graphic screenshots and archived graphic screenshots storage:

Example UNC path for the images: \\filesrv\OITData\OITImages

Example UNC path for the images archive: \\filesrv\OITData\OITArchive

See [Formatting a disk for graphic images storage and the database](#) for more.

If you plan to keep the default setting skip to the database installation section.

## Editing the database installer to use file system storage for recorded graphic screenshots

If you plan to keep the default setting skip to the database installation section. However, it is strongly recommended you configure image storage on an external file share.

It's easiest to configure the graphical image storage location during the ObserveIT installation process. If you plan to use the file system for storing the recorded graphic screenshots data, please use the following procedure **before** starting the database installation.

**Note: In this document, we will be using a server called "FILEsrv" to host the graphic images.**

1. Connect to the computer where you downloaded and extracted the ObserveIT installer.
2. Open the Start menu and type in NOTEPAD.
3. Click the File menu and click Open.
4. Navigate to the folder with the extracted ObserveIT installer.
5. Navigate to the DB folder.
6. In the Notepad's Open dialog, change the file type from Text Documents (\*.txt) to All Files (\*.\*).
7. Click the SQLPackage.exe.config file and click the Open button.
8. Find the following line: `<add key="FileSystemPath" value="" />`.
9. Replace the value for the value field with the path to the image store UNC path.

For example:

```
<add key="FileSystemPath" value="//filesrv\OITData\OITImages" />
```

10. Find the following line: `<add key="ArchiveFileSystemPath" value="" />`.
11. Replace the value for the value field with the path to the image store UNC path.

For example:

```
<add key="ArchiveFileSystemPath" value="//filesrv\OITData\OITArchive" />
```

12. Click the File menu and click Save.

```
<!--Where the file system images will storage-->
<add key="FileSystemPath" value="//filesrv\OITData\OITImages"/>
<!--Where the archive file system images will storage-->
<add key="ArchiveFileSystemPath" value="//filesrv\OITData\OITArchive"/>
```

13. Click the File menu and click Open.
14. Navigate to the folder with the extracted ObserveIT installer.
15. Navigate to the DB\_Analytics folder.
16. In the Notepad's Open dialog, change the file type from Text Documents (\*.txt) to All Files (\*.\*).
17. Click the SQLPackage.exe.config file and click the Open button.
18. Find the following line: `<add key="FileSystemPath" value="" />`.
19. Replace the value for the value field with the path to the image store UNC path.

For example:

```
<add key="FileSystemPath" value="//filesrv\OITData\OITImages" />
```

20. Find the following line: `<add key="ArchiveFileSystemPath" value="" />`.
21. Replace the value for the value field with the path to the image store UNC path.

For example:

```
<add key="ArchiveFileSystemPath" value="//filesrv\OITData\OITArchive" />
```

22. Click the File menu and click Save.
23. Close Notepad.

## Installing the ObserveIT databases

Use the following steps to install the database:

**Note:** The database installer requires .NET Framework 3.5. See [Installing prerequisites](#) for more information.

**Note:** The DB install process can also be run directly on the SQL Server machine.

1. Connect to the computer where you downloaded and extracted the ObserveIT installer using the ObserveIT Service Account credentials.
2. Open the Start menu and type in EXPLORER.
3. Navigate to the folder with the extracted ObserveIT installer.
4. Navigate to the DB folder.
5. Double-click the sqlpackage.exe file.
6. In the Run Package window enter the details of the SQL server, in the following format:

**<ServerFQDN>\<InstanceName>,<Port>**

For example:

**SQLsrv.test.lab\ObserveIT,1433**

7. Click the Windows authentication radio button and click the Run button.
8. If the connection is successful, the installation will proceed. If not, check the connectivity to the SQL server and make sure the connection string is correct.

**Hint: Check the Windows Firewall on the SQL Server and either turn it off, or add the relevant rules to allow SQL Server connectivity (TCP port 1433), check protocol bindings (TCP/IP must be enabled), and check the SQL Server listening port. See [Configuring Windows Firewall](#) for more information.**

9. You will receive a message saying that the installation cannot create the "OITServiceAccount" account in SQL Server. The message text is:

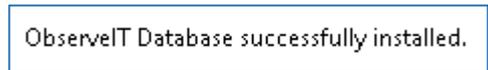
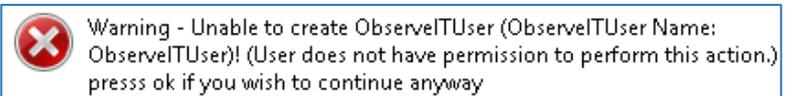
```
Warning - Unable to create OITServiceAccount (OITServiceAccount Name: OITServiceAccount)! (User does not have permission to perform this action.) Press OK if you wish to continue anyway.
```

This error may be ignored. Click OK to acknowledge the message.

**Note:** If you did not receive this

**error, it means that the ObserveIT service account has SYSADMIN permissions on the SQL Server. It is strongly suggested that you stop the installation at this phase, delete the resulting databases, change the ObserveIT service account permissions to DBCREATOR, and then re-execute the database installer program. While, by itself, this is not a problem, the result is that the ObserveIT database and the subsequent connection strings used by all the ObserveIT components will use the "OITServiceAccount" account in SQL Server instead of the ObserveIT service account. To fix this issue you will need to manually change the connection strings and change the SQL Server database settings. Contact support for information on how to perform these changes.**

10. For each of the four ObserveIT databases, you will receive a "successfully installed" message. Acknowledge each message.



After the four databases are created, the installation window will automatically close.

11. Switch to the File Explorer.
12. Navigate to the folder with the extracted ObserveIT installer.
13. Navigate to the `DB_Analytics` folder.
14. Double-click the `sqlpackage.exe` file.
15. In the `Run Package` window enter the details of the SQL server, in the following format:  
**<ServerFQDN>\<InstanceName>,<Port>**

For example:

**SQLsrv.test.lab\ObserveIT,1433**

16. Click the `Windows authentication` radio button and click the `Run` button.
17. If the connection is successful, the installation will proceed. If not, check the connectivity to the SQL server and make sure the connection string is correct.

**Hint: Check the Windows Firewall on the SQL Server and either turn it off, or add the relevant rules to allow SQL Server connectivity (TCP port 1433), check protocol bindings (TCP/IP must be enabled), and check the SQL Server listening port. See [Configuring Windows Firewall](#) for more information.**

18. You will receive a message saying that the installation cannot create the “OITServiceAccount” account in SQL Server. The message text is:

```
Warning - Unable to create OITServiceAccount (OITServiceAccount Name:
OITServiceAccount)! (User does not have permission to perform this action.) Press
OK if you wish to continue anyway.
```

This error may be ignored. Click `OK`.

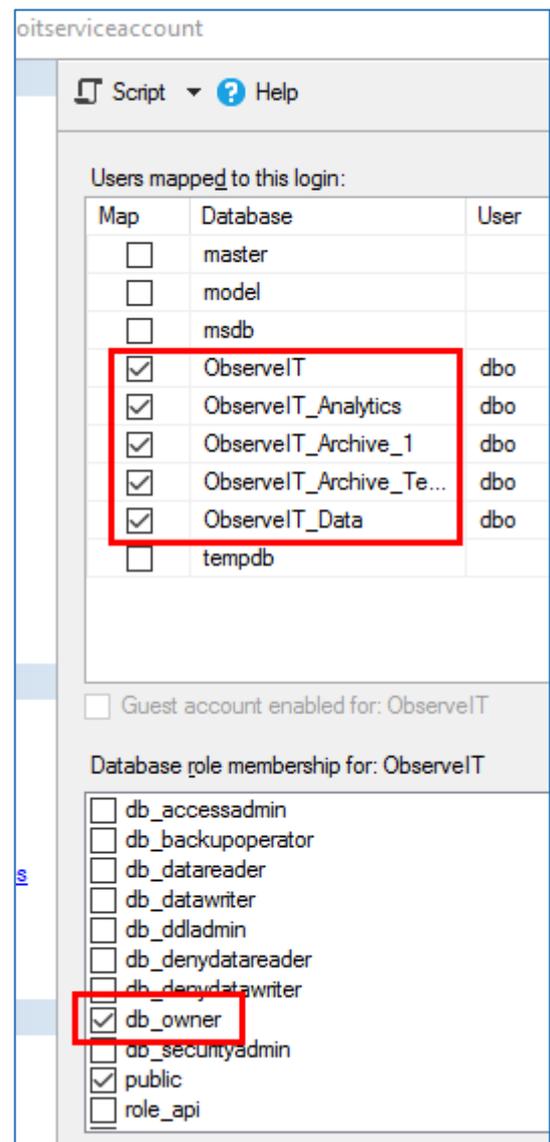
**Note: If you did not receive this error, it means that the ObserveIT service account has SYSADMIN permissions on the SQL Server. It is strongly suggested that you stop the installation at this phase, delete the resulting databases, change the ObserveIT service account permissions to DBCREATOR, and then re-execute the database installer program. While, by itself, this is not a problem, the result is that the ObserveIT database and the subsequent connection strings used by all the ObserveIT components will use the “OITServiceAccount” account in SQL Server instead of the ObserveIT service account. To fix this issue you will need to manually change the connection strings and change the SQL Server database settings. Contact support for information on how to perform these changes.**

19. You will receive a “successfully installed” message. Click `OK` to acknowledge the message.

## Verifying successful database installation

Use the following steps to verify the database installation:

1. Connect to the SQL server or to a computer with SQL Management Studio installed.
2. Open the `Start` menu, expand the Microsoft SQL Server 2016 folder and click `SQL Management Studio`.
3. Type in the SQL server's FQDN or IP address into the `Server name` field.
4. Choose `Windows Authentication` if your account has `sysadmin` permissions on the SQL server. Otherwise, choose `SQL Server Authentication` and log in with a `sysadmin`-level account.
5. Click `OK` to connect.
6. Expand `Databases`. You should see five new `ObserveIT` databases.
7. Expand `Security > Logins`.
8. Right-click the `ObserveIT Service Account` user – in this example, `OITServiceAccount` – and select `Properties`.
9. Click `User Mapping` from `Select a Page` menu.
10. Under `User mapped to this login` click the `ObserveIT` database.
11. Make sure the checkbox in the `Map` column is checked.
12. Make sure that the checkbox for `db_owner` is checked.
13. Repeat steps 10-12 to the other 4 `ObserveIT` databases – 5 total.
14. Click `OK`.
15. Close SQL Management Studio.



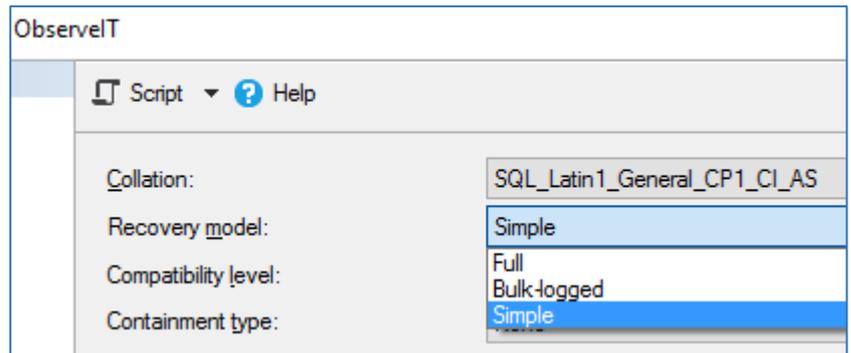
## Configuring Simple Recovery Model for the ObserveIT databases on the SQL Server

A recovery model is a database property that controls how transactions are logged, whether the transaction log requires (and allows) backing up, and what kinds of restore operations are available. It automatically reclaims log space to keep space requirements small, essentially eliminating the need to manage the transaction log space.

**Note:** If you need to use a point in time recovery option – use **Full recovery model** instead, which is the default configuration option. No changes need to be made. For more information, see **Full Database Backups (SQL Server) MSDN article:** <https://msdn.microsoft.com/en-AU/library/ms186289.aspx>.

1. Connect to the SQL server or to a computer with SQL Management Studio installed.
2. Open the `Start` menu, expand the Microsoft SQL Server 2016 folder and click `SQL Management Studio`.
3. Type in the SQL server's FQDN or IP address into the `Server name` field.
4. Choose `Windows Authentication` if your account has `sysadmin` permissions on the SQL server. Otherwise, choose `SQL Server Authentication` and log in with a `sysadmin`-level account.

5. Click OK to connect.
6. Expand Databases.
7. Right-click the ObserveIT database and select Properties.
8. Click Options from Select a Page menu.
9. Under Recovery model select Simple.
10. Click OK.
11. Repeat steps 7-10 for the remaining 4 ObserveIT databases – 5 total.



**Note:** simple recovery mode may be configured via an automated query. See [Setting the ObserveIT databases to a simple recovery mode for more information](#).

## Placing the database files on designated drives

The best practice for SQL databases is to place the database data files (.mdf) and the database log files (.ldf) on designated, separate drives. This guide will guide you on moving the ObserveIT database files to designated drives.

**Note:** the following steps assume two designated drives are present at the SQL machine. This guide assumes that the database drive is assigned the drive letter E:, while the log drive is assigned the drive letter F:. This guide also assumes the SQL Management Studio is installed on the SQL server machine.

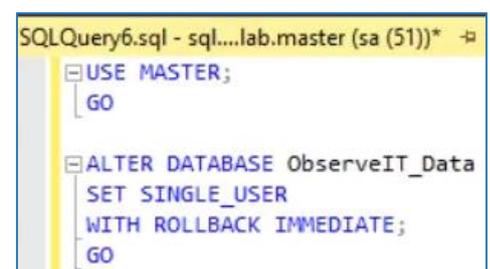
1. Connect to the SQL server machine.
2. Click the Start menu, expand the Microsoft SQL Server 2016 folder and click the SQL Management Studio.
3. At the SQL Management Studio, specify the Server name, authentication type and Login and Password to the ObserveIT SQL instance (if connecting via SQL Server Authentication). Click Connect.
4. Click the **New Query** button.
5. Paste the following code into the New Query window:

**Note:** This action will stop all ObserveIT databases and will cause downtime for all ObserveIT services.

```
USE MASTER;
GO
ALTER DATABASE ObserveIT_Data
SET SINGLE_USER
WITH ROLLBACK IMMEDIATE;
GO
EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Data'
GO

USE MASTER;
GO
ALTER DATABASE ObserveIT
SET SINGLE_USER
WITH ROLLBACK IMMEDIATE;
GO
EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT'
GO

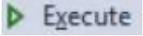
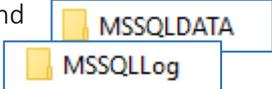
USE MASTER;
GO
```



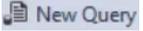
```
ALTER DATABASE ObserveIT_Archive_1
SET SINGLE_USER
WITH ROLLBACK IMMEDIATE;
GO
EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Archive_1'
GO

USE MASTER;
GO
ALTER DATABASE ObserveIT_Archive_Template
SET SINGLE_USER
WITH ROLLBACK IMMEDIATE;
GO
EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Archive_Template'
GO

USE MASTER;
GO
ALTER DATABASE ObserveIT_Analytics
SET SINGLE_USER
WITH ROLLBACK IMMEDIATE;
GO
EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Analytics'
GO
```

6. Click the  button. Wait for the query to finish.
7. Follow the [Formatting a disk for graphic images store](#) guide in this document to correctly format the two new disks in the machine, in this example: disk *E*: for the database data files and disk *F*: for the database log files.
8. Open the Start menu and type in EXPLORER. Press the Enter key.
9. Navigate to disk E:.
10. Right-click the empty space inside the File Explorer window, expand the *New* menu and select *Folder*. 
11. Type in MSSQLDATA. Press the Enter key.
12. Navigate to disk F:.
13. Right-click the empty space inside the File Explorer window, expand the *New* menu and select *Folder*.
14. Type in MSSQLLog. Press the Enter key.
15. Open the *Start* menu and type in POWERSHELL.
16. Right-click the PowerShell shortcut and choose *Run as administrator*.
17. If prompted *Do you want to allow this app to make changes to your device?* click *Yes*. 
18. Paste the following code into the PowerShell window:
 

```
Get-ChildItem 'C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\' | Where-Object {$_.Name -like "*observeit*" -and $_.Name -like "*mdf"} | Move-Item -Destination E:\MSSQLDATA\

Get-ChildItem 'C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\' | Where-Object {$_.Name -like "*observeit*" -and $_.Name -like "*ldf"} | Move-Item -Destination F:\MSSQLLog\
```
19. Press the Enter key at the final prompt.
20. Return to the SQL Management Studio.
21. Click the  button.

22. Paste the following code into the New Query window:

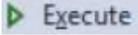
```
CREATE DATABASE [ObserveIT_Data] ON
( FILENAME = N'E:\MSSQLDATA\ObserveIT_Data_Data.mdf' ),
( FILENAME = N'F:\MSSQLLog\ObserveIT_Data_Log.ldf' )
FOR ATTACH
GO

CREATE DATABASE [ObserveIT] ON
( FILENAME = N'E:\MSSQLDATA\ObserveIT_Data.mdf' ),
( FILENAME = N'F:\MSSQLLog\ObserveIT_Log.ldf' )
FOR ATTACH
GO

CREATE DATABASE [ObserveIT_Analytics] ON
( FILENAME = N'E:\MSSQLDATA\ObserveIT_Analytics_Data.mdf' ),
( FILENAME = N'F:\MSSQLLog\ObserveIT_Analytics_Log.ldf' )
FOR ATTACH
GO

CREATE DATABASE [ObserveIT_Archive_1] ON
( FILENAME = N'E:\MSSQLDATA\ObserveIT_Archive_1_Data.mdf' ),
( FILENAME = N'F:\MSSQLLog\ObserveIT_Archive_1_Log.ldf' )
FOR ATTACH
GO

CREATE DATABASE [ObserveIT_Archive_Template] ON
( FILENAME = N'E:\MSSQLDATA\ObserveIT_Archive_Template_Data.mdf' ),
( FILENAME = N'F:\MSSQLLog\ObserveIT_Archive_Template_Log.ldf' )
FOR ATTACH
GO
```

23. Click the  button. Wait for the query to finish.

24. Close the SQL Management Studio.

## Setting initial MDF and LDF file size for the ObserveIT databases on the SQL Server

Setting the initial size for the database files and database log files assures that the database writing is optimized.

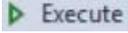
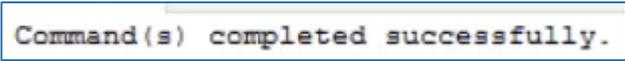
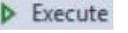
1. Connect to the SQL server or to a computer with SQL Management Studio installed.
2. Open the `Start` menu, expand the `Microsoft SQL Server 2016` folder and click `SQL Management Studio`.
3. Type in the SQL server's FQDN or IP address into the `Server name` field.
4. Choose `Windows Authentication` if your account has `sysadmin` permissions on the SQL server. Otherwise, choose `SQL Server Authentication` and log in with a `sysadmin`-level account.

5. Click OK to connect.
6. Expand Databases.
7. Right-click the ObserveIT database and select Properties.
8. Click Files from Select a Page menu.
9. Change the Initial Size (MB) value for the ObserveIT\_Data logical name to 102400MB.  
Change the Initial Size (MB) value for the ObserveIT\_Log logical name to 51200MB.
10. Click OK.
11. Right-click the ObserveIT\_Archive\_1 database and select Properties.
12. Click Files from Select a Page menu.
13. Change the Initial Size (MB) value for the ObserveIT\_Data logical name to 10240MB.  
Change the Initial Size (MB) value for the ObserveIT\_Log logical name to 5120MB.
14. Click OK.
15. Right-click the ObserveIT\_Archive\_Template database and select Properties.
16. Click Files from Select a Page menu.
17. Change the Initial Size (MB) value for the ObserveIT\_Data logical name to 10240MB.  
Change the Initial Size (MB) value for the ObserveIT\_Log logical name to 5120MB.
18. Click OK.

Logical Name	File Type	Filegroup	Initial Size (MB)
ObserveIT_Data	ROWS...	PRIMARY	102,400
ObserveIT_Log	LOG	Not Applicable	51,200

## Installing the automated maintenance procedure

To ensure optimal database health and performance, please perform the following steps to add the automated maintenance procedure for your ObserveIT databases:

1. Connect to the machine containing the ObserveIT database or the machine at which SQL Management Studio is installed.
2. Download the following file: <http://files.observeit.com/support/OIT-DB-Maintenance.zip>
3. Open the Start menu and type in EXPLORER. Press the Enter key.
4. Navigate to the folder you have downloaded the file in step 2 to.
5. Right-click the *OIT-DB-Maintenance.zip* file and click Extract All.
6. In the new window, check the Show extracted files when complete checkbox and click Extract. A new File Explorer window will open.
7. Double-click the *dbmaintprepare.sql* file.
8. If prompted How do you want to open this file? choose SQL Management Studio or SSMS. Click OK.
9. At the SQL Management Studio, specify the Server name, authentication type and Login and Password to the ObserveIT SQL instance (if connecting via SQL Server Authentication). Click Connect.
10. Click inside the query window.
11. Click the  button. If successfully completed, a confirmation message will appear in the Messages pane. 
12. Return to the previous File Explorer window.
13. Double-click the *OIT-DB-Maint-Create-Jobs.sql* file.
14. Click inside the query window.
15. Click the  button. If successfully completed, a confirmation message will appear under the Messages pane. Ignore any warnings received. 
16. Close the SQL Management Studio.
17. Open the Start menu and type in RUN. Press the Enter key.
18. Type in SERVICES.MSC. Press the Enter key.
19. Locate the SQL Server Agent service.
20. Right-click the service and click Properties.
21. Change the value for Startup Type field to **Automatic (Delayed Start)**.
22. Click the Start button.
23. Click OK.
24. Close the window.

# CONFIGURING THE INTERNET INFORMATION SERVICES

## Preparing IIS to install the ObserveIT web applications

The following steps describe how to create and configure the Application Pool and website on the ObserveIT server machine in preparation for the application installation.

If you have multiple Application Servers and/or a separate Web Console machine, you need to repeat this process for each machine.

## Assigning a digital certificate for the Web Console

ObserveIT strongly recommends encrypting the Web Console traffic by using HTTPS.

**Note: If you plan on using unencrypted HTTP for the Web Console traffic – skip to the next section.**

**Note: In most instances, the Web Console is deployed on the only ObserveIT Application Server in a smaller deployment or one of the ObserveIT Application Servers in case of a larger deployment. It is also possible to deploy the ObserveIT Web Console on a separate server.**

It is strongly recommended a certificate to be issued by a Certificate Authority, either 3<sup>rd</sup>-party (such as Verisign, Thawte, GoDaddy, Rapid SSL, or other), or from an internal Enterprise Certificate Authority. Windows Server operating systems have a built-in CA role that you can install and use.

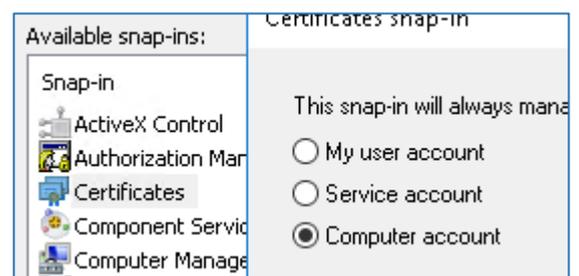
When it is not possible to acquire a Certificate Authority certificate, a self-signed certificate may be used.

**Note: Please consult with your organization's security team to learn what type of digital certificate best fits your environment. In this guide, we assume an Enterprise Certificate Authority certificate is used.**

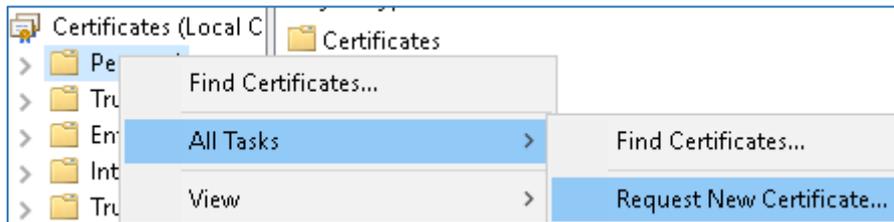
## Option 1: Creating an internal Enterprise Certificate Authority certificate for the Web Console

To obtain a certificate from a local Enterprise Certificate Authority follow these steps:

1. Connect to the ObserveIT Web Console machine.
2. Open the Start menu and type in RUN. Press the Enter key.
3. Type in MMC and press the Enter key.
4. If prompted Do you want to allow this app to make changes to your device? click Yes.
5. Click the File menu and click Add/Remove Snap-in.
6. From Available snap-ins choose Certificates and click Add.
7. In the Certificates snap-in window choose Computer account and click Next.
8. Under Select the computer you want this snap-in to manage select Local computer and click Finish.
9. Click OK.
10. Expand the Certificates (Local Computer) node.



- Right-click the `Personal` node, click `All Tasks` and then `Request New Certificate`.

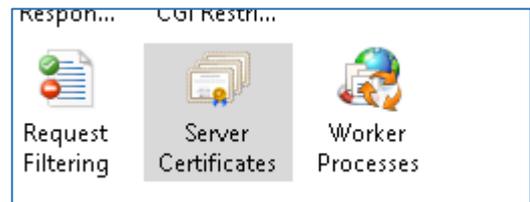


- Click `Next`.
- At the `Select Certificate Enrollment Policy` page select your enrollment policy (usually – `Active Directory Enrollment Policy`) and click `Next`.
- At the `Request Certificates` page select the certificate type (usually – `Computer`) and click `Enroll`.
- Click `Finish` when the enrollment is successfully completed to close the window.
- Under `Personal` node, click the `Certificates` note.
- Confirm the newly-created certificate exists and has the FQDN of the current server under the `Issued To` column.



### Option 2: Creating a self-signed certificate for the Web Console

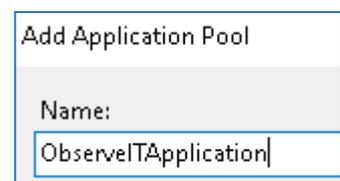
- Connect to the `ObserveIT Web Console` machine.
- Open the `Start` menu and type in `Run`. Press the `Enter` key.
- Type in `IIS`, select the `Internet Information Services (IIS) Manager` and press the `Enter` key.
- At the `Connections` pane, expand the server node and double-click the `Server Certificates` icon at the main page.
- At the `Actions` pane, click `Create Self-Signed Certificate`.
- At the new window, under `Specify a friendly name for the certificate` enter a descriptive name for the certificate. Click `OK`.



### Creating and configuring the ObserveIT Application Pool

- Connect to the `ObserveIT Web Console` machine.
- Open the `Start` menu and type in `Run`. Press the `Enter` key.
- Type in `IIS`, select the `Internet Information Services (IIS) Manager` and press the `Enter` key.
- At the `Connections` pane, expand the server node and double-click the `Server Certificates` icon at the main page.
- Right-click the `Application Pools` node and choose `Add Application Pool`.
- In the `Add Application Pool` window, in the `Name` field, type in `OBSERVEITAPPLICATION`. Click `OK`.
- Right-click the `ObserveITApplication` Application Pool and select `Advanced Settings`.

**Note: The Application Pool name must not contain spaces.**



8. Under the `Process Model` section, click `Identity` and click the  button.
9. Click the `Custom Account` radio button, and click `Set`.
10. In the `Set Credentials` window, fill out the details:
  - a. In the `User name` field enter the username in the `DOMAIN\username` format. In our case: `OIT-DEMO\OITSERVICEACCOUNT`.
  - b. In the `Password` and `Confirm password` fields enter the password for the `OITServiceAccount` account.
11. Click `OK`, click `OK` again and then click `OK` once more to save all settings.

If you have multiple Application Servers and/or a separate Web Console machine, you need to repeat this process for each machine.

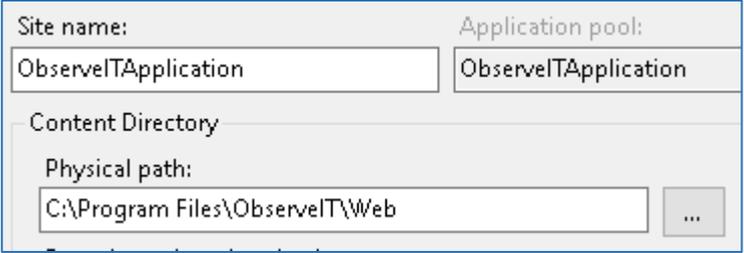
For example, if you plan to use the following setup:

- OITsrv1 – Application Server #1
- OITsrv2 – Application Server #2
- OITweb – Web Console

The result would be to have an identical application pool using the same name and identity settings on all 3 machines.

## Creating the website for the ObserveIT Application Server

On the machine that is assigned for the ObserveIT Application Server role, perform the following steps:

1. Connect to the ObserveIT Web Console machine.
2. Open the `Start` menu and type in `EXPLORER`.
3. Navigate to the following path: `C:\Program Files`.
4. Click the `Home` tab and click `New Folder`.
5. Type in `OBSERVEIT`. Press `Enter`.
6. Double-click the new `ObserveIT` folder.
7. Click the `Home` tab and click `New Folder`.
8. Type in `WEB`. Press `Enter`.
9. Open the `Start` menu.
10. Type in `IIS`, select the `Internet Information Services (IIS) Manager` and press the `Enter` key.
11. At the `Connections` pane, expand the server node and expand `Sites`.
12. Right-click `Sites` and choose `Add Website`.
13. At the `Site Name` field type in `OBSERVEITAPPLICATION`.
14. Click the `Select` button next to the `Application Pool` field.
15. Select the `ObserveITApplication` Application Pool. Click `OK`.
16. At the `Physical path` field click the  button.
 
17. Navigate to the following path: `C:\Program Files\ObserveIT\Web`. Click the `Web` folder. Click `OK`.
18. Click the `Select` button next to the `Application Pool` field.

**Note: If you cannot find the “ObserveITApplication” application pool please go back to the previous topic and make sure you properly created the application pool before creating the website.**

19. Under Binding, at the Port field, change the port value from 80 to 4884.
20. Click OK to save the changes and create the new website.

If you have multiple Application Servers, you need to repeat this process for each machine.

For example, if you plan to use the following setup:

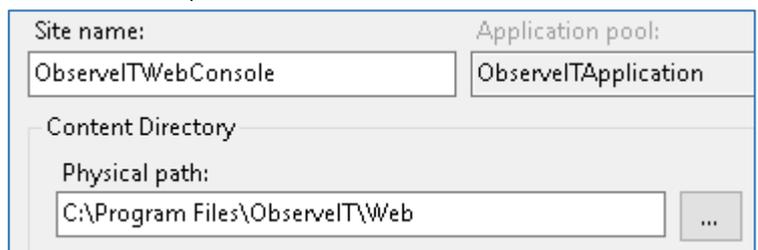
- OITsrv1 – Application Server #1
- OITsrv2 – Application Server #2
- OITweb – Web Console

The result would be to have an identical website using the same name and application pool on the 2 machines that will act as the Application Servers.

## Creating the website for the ObserveIT Web Console

On the machine that is assigned for the ObserveIT Web Console role, perform the following steps:

1. Connect to the ObserveIT Web Console machine.
2. Open the Start menu.
3. Type in IIS, select the Internet Information Services (IIS) Manager and press the Enter key.
4. At the Connections pane, expand the server node and expand Sites.
5. Right-click Sites and choose Add Website.
6. At the Site Name field type in OBSERVEITWEBCONSOLE.
7. Click the Select button next to the Application Pool field.
8. Select the ObserveITApplication Application Pool. Click OK.
9. At the Physical path field click the  button.
10. Navigate to the following path: C:\Program Files\ObserveIT\Web. Click the Web folder. Click OK.
11. Click the Select button next to the Application Pool field.



**Note: If you cannot find the “ObserveITApplication” application pool please go back to the previous topic and make sure you properly created the application pool before creating the website.**

12. Under Binding, at the Type field, change the value from http to https. The value of the Port field will be automatically changed from 80 to 443.
13. At the SSL certificate field choose a certificate you have previously created at the steps [Option 1: Creating an internal Enterprise Certificate Authority certificate for the Web Console](#) or [Option 2: Creating a self-signed certificate for the Web Console](#).
14. Click OK to save the changes and create the website.

# INSTALLING THE OBSERVEIT COMPONENTS

## Installing the ObserveIT Application Server

Depending on the sizing and architecture of the product deployment, you must install one or more ObserveIT Application Server(s). This topic describes how to install the ObserveIT Application Server component on the first server. If you have multiple Application Servers, you need to repeat this process for each machine.

**Note: Do not attempt to install ObserveIT server-side components over the network. Always use a local copy of the installation files.**

Use the following steps to install the ObserveIT Application Server:

1. Connect to the computer where you downloaded and extracted the ObserveIT installer using the ObserveIT Service Account credentials.
2. Open the Start menu and type in `COMMAND PROMPT`.
3. Right-click the Command Prompt shortcut found and choose `Run as administrator`.
4. If prompted `Do you want to allow this app to make changes to your device?` click `Yes`.
5. Navigate to the folder with the extracted ObserveIT installer. Navigate to the Web folder.

For example:

```
cd c:\Users\OITServiceAccount\Desktop\ObserveIT_Setup_v7.1.0.136\Web\AppServer
```

6. Type in `OBSERVEIT.APPSERVERSETUP.MSI` and press Enter.
7. At the ObserveIT Application Server window click Next.
8. At the Site field choose `ObserveITApplication`.
9. At the Application Pool choose `ObserveITApplication`. Click Next.
20. At the Server field enter the details of the SQL server, in the following format:

```
<ServerFQDN>\<InstanceName>,<Port>
```

For example:

```
SQLsrv.test.lab\ObserveIT,1433
```

10. Click the Windows Authentication radio button and enter the password for the current account – the ObserveIT Service Account - at the Password field. Click the Test Connection button

If the test is successful, a success message will be displayed and the Next button will become available.

11. Click Next. The installation will begin.
12. After successful installation, click Close.

## Verifying the ObserveIT Application Server installation

1. Connect to the ObserveIT Web Console machine.
2. Open the Start menu and type in `RUN`. Press the Enter key.
3. Type in `%USERPROFILE%\APPDATA\LOCAL\TEMP`. Press the Enter key.
4. Locate the `AppServer_CA_Log.txt` file. Double-click the file to open it.
5. Press `CTRL+F` on the keyboard to open the Find dialog.

6. Type in REGISTERAPPLICATIONSERVER and press Find Next.
7. Locate the following line: RegisterApplicationServer: Done.

**Note: If the line does not exist or the word Done does not exist – the installation failed. Please make re-check the installation requirements, particularly the permissions for the SQL logins created previously in this guide.**

```

---server url: http://OITsrv.oit-demo.local|:4884
---RegisterApplicationServer: Trying using SSPI.
---RegisterApplicationServer: Done.---
---dict curr val : ObserveIT is ObserveIT?---
    
```

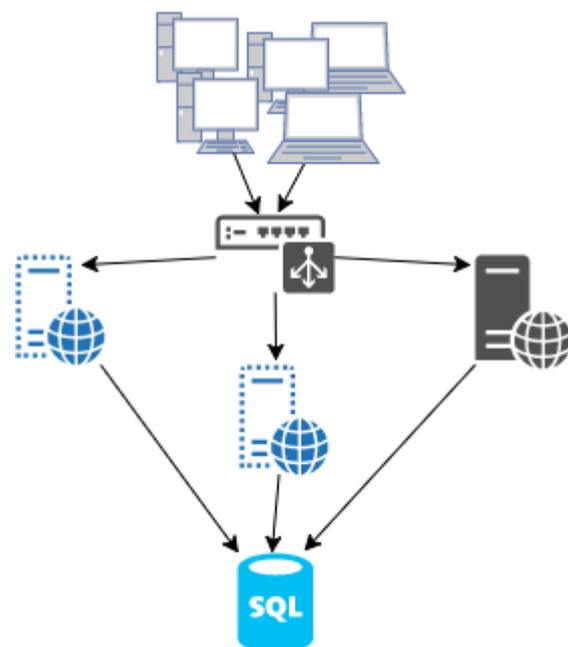
## Installing Additional ObserveIT Application Servers

Depending on your deployment design and the number of concurrent recorded sessions, you may need to deploy additional ObserveIT Application Servers.

**Note: Before installing an additional Application Server, you must obtain a valid license from the ObserveIT Sales team.**

When deploying more than one Application Server, you need to load balance the Agent connections with the multiple Application Servers. You may use software-based load balancing solutions, such as Microsoft Network Load Balancing (NLB), or hardware-based solutions, such as F5, Citrix NetScaler, or others. Configuring steps for these solutions is a task that is beyond the scope of this document.

The steps required to install additional Application Server(s) and verify its successful installation are identical to the steps required for installing and verifying the first Application Server.



## Installing the ObserveIT Web Management Console

The ObserveIT Web Console is the component that is used to configure, administer and use the product. Only one Web Console can be installed per environment. This topic describes how to install the ObserveIT Application Server component on the first server.

**Note: In most cases, the Web Console is installed on the same machine as the Application Server (the first one, in case of multiple Application Servers). However, it's also possible that a separate dedicated machine will be used for this role.**

Use the following steps to install the Web Management Console:

1. Connect to the computer where you downloaded and extracted the ObserveIT installer using the ObserveIT Service Account credentials.
2. Open the Start menu and type in COMMAND PROMPT.
3. Right-click the Command Prompt shortcut found and choose Run as administrator.
4. If prompted Do you want to allow this app to make changes to your device? click Yes.
5. Navigate to the folder with the extracted ObserveIT installer. Navigate to the Web folder.

For example:

**cd c:\Users\OITServiceAccount\Desktop\ObserveIT\_Setup\_v7.1.0.136\Web\WebConsole**

6. Type in `OBSERVEIT.WEBCONSOLESETUP.MSI` and press Enter.
7. At the ObserveIT Console window click Next.
8. At the Site field choose ObserveITWebConsole.
9. At the Application Pool choose ObserveITApplication. Click Next.
10. At the Server field enter the details of the SQL server, in the following format:

**<ServerFQDN>\<InstanceName>,<Port>**

For example:

**SQLsrv.test.lab\ObserveIT,1433**

11. Click the Windows Authentication radio button and enter the password for the current account – the ObserveIT Service Account - at the Password field. Click the Test Connection button  
If the test is successful, a success message will be displayed and the Next button will become available.
12. Click Next. The installation will begin.
13. After successful installation, click Close.

Site:	ObserveITWebConsole
Virtual directory:	ObserveIT
Application Pool:	ObserveITApplication

## Verifying the Web Management Console installation

1. Connect to the ObserveIT Web Console machine.
2. Open the Start menu and type in `RUN`. Press the Enter key.
3. Type in `%USERPROFILE%\APPDATA\LOCAL\TEMP`. Press the Enter key.
4. Locate the `WebConsole_CA_Log.txt` file. Double-click the file to open it.
5. Press CTRL+F on the keyboard to open the Find dialog.
6. Type in `REGISTERAPPLICATIONSERVER` and press Find Next.
7. Locate the following line:  
**RegisterWebConsole: Done.**

```
---RegisterWebConsole: Trying using SSPI.---
---RegisterWebConsole: Done.---
```

**Note: If the line does not exist or the word Done does not exist – the installation failed. Please make re-check the installation requirements, particularly the permissions for the SQL logins created previously in this guide.**

## Configuring the ObserveIT services

The ObserveIT installation creates 4 services. You need to modify them so that they use the AD-based service account:

On the ObserveIT Application Server machine(s):

- "ObserveIT Activity Alerts Service"

On the Web Console machine:

- "ObserveITNotificationService"
- "ObserveIT Health Monitoring Service"
- "ObserveIT Analytics Service"

Use the following steps to configure the *ObserveIT Activity Alerts Service* service to use the ObserveIT service account user:

1. Connect to the ObserveIT Application Server machine.
2. Open the Start menu and type in **RUN**. Press the Enter key.
3. Type in **SERVICES.MSC** and press the Enter key.
4. Find the *ObserveIT Activity Alerts Service* in the list.
5. Right-click the service and click **Properties**.
6. Click the **Log On** tab.
7. Click the **This account** radio button. Click **Browse**.
8. Click **Locations** and ensure your Active Directory domain is selected.
9. In the **Enter the object name to select** box type in **OITSERVICEACCOUNT**. Click **OK**.
10. In the **Password** and **Confirm password** fields enter the password for the ObserveIT Service Account user.
11. Click **OK**. If a message pops up that the user **OITServiceAccount** has been granted the **Log on as a service** rights click **OK**.
12. Right-click the *ObserveIT Activity Alerts Service* service and click **Restart**.
13. Perform steps 5-12 on the remaining 3 ObserveIT services – 4 total – named *ObserveIT Health Monitoring Service*, *ObserveIT Notification Service* and *ObserveIT User Analytics Service*.

## Installing the Web Categorization module

The ObserveIT Website Categorization module automatically detects categories of Websites that end users are browsing, enabling alerts to be generated on browsing categories such as Gaming, Adults, Infected or Malicious Websites, Phishing Websites, and more.

To trigger alerts on Internet browsing, the Website Categorization module must be installed. Note that the Website Categorization module can be installed on the same machine as the Web Console or on a separate dedicated machine (recommended).

### Prerequisites for installing the Website Categorization module

- To download the initial data and receive updates directly from NetSTAR cloud service, your machine (that is, the server on which the Website Categorization module is installed) must have Internet access.  
**Note: If you don't have Internet access you can use an HTTP proxy that will provide Internet access and allow the data download.**
- Make sure that port number 443 is open, and that the URL <https://nsv10.netstar-inc.com/gcfus/get.cgi> (that the module needs to access NETSTAR for initial data download and daily database updates) is not blocked by the Firewall.
- 8 GB minimum memory requirement is recommended. If you install the Website Categorization module on a machine with less than 8 GB RAM, the first time that the module detects the categorized browsed URLs, alerts will not be generated. Upon subsequent browsing, alerts will be generated on these URLs.

## Performing the Website Categorization module installation

Note: It is recommended, though not required, to install the Website Categorization module on a separate Windows Server machine. Please also make sure you meet the prerequisites listed in the previous section.

1. Connect to the computer where you downloaded and extracted the ObserveIT installer using the ObserveIT Service Account credentials.
2. Click the `Start` menu and type in `RUN`.
3. Type in `CMD`. Right-click the `Command Prompt` shortcut and click `Run as administrator`.
4. If prompted `Do you want to allow this app to make changes to your device?` click `Yes`.
5. Navigate to the folder with the extracted ObserveIT installer. Navigate to the `Web` folder.

For example:

```
cd c:\Users\OITServiceAccount\Desktop\ObserveIT_Setup_v7.1.0.136\WebsiteCat
```

6. Type in `WEBSITECAT_SETUP.MSI` and press `Enter`. A new window will open.
7. Ensure the installer confirms you have enough RAM for the Website Categorization module. Click `Next`.
8. On the path selection screen click `Next`.
9. At the `Please fill in the required SQL Server details` window:
  - a. At the `Server` field enter the details of the SQL server, in the following format:

```
<ServerFQDN>\<InstanceName>,<Port>
```

For example:

```
SQLsrv.test.lab\ObserveIT,1433
```

- b. At the `Authentication method` field choose `Windows Authentication` and supply the password for the current user, in our case – `OITServiceAccount`.

10. Click `Test Connection`. If successful, the `Next` button will become available. Click `Next`.
11. If no Internet connectivity detected, a message will notify you of an issue, and if you continue with the installation, it will fail. Please check for Internet connectivity and/or [configure the Internet proxy access](#).
12. If the Internet connectivity check succeeds, click `Install Website Categorization`.
13. After the installation completes, click `Close` to close the installer window.

For optimal performance, it is also recommended to install on a machine with 8GB memory (RAM).  
This machine is equipped with: 10812 MB of RAM.



sqlsrv.oit-demo.local\Observeit,1433

Installer Authentication (ObserveITUser)

Windows Authentication

The update service could not be accessed. Please check Internet connectivity. If this machine will never have Internet access, an HTTPS Proxy can be configured. Please refer to Installation Guide.

The update service was accessed successfully.

## Configuring Internet proxy settings for Website Categorization module

This section describes configuration of the Internet proxy for the Website Categorization module, allowing the Website Categorization module component to access the Internet and automatically update the internal website list.

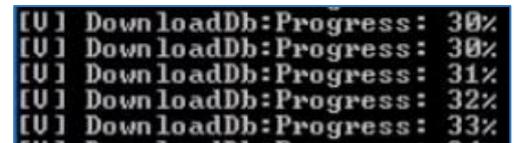
**Note: Website Categorization module does not support proxy authentication.**

1. Connect to the ObserveIT Website Categorization module machine.
2. Open the `Start` menu and type in `RUN`. Press the `Enter` key.
3. Right-click the `Notepad` shortcut and click `Run as administrator`.
4. If prompted `Do you want to allow this app to make changes to your device?` click `Yes`. Click the `File` menu and click `Open`.
5. Navigate to the following folder: `C:\Program Files\ObserveIT\WebsiteCat\Adapters\NetStar\db\etc\`.

6. In the Notepad's Open dialog, change the file type from **Text Documents (\*.txt)** to **All Files (\*.\*)**.
7. Locate the *gcf1.conf* file, click it, and click the Open button.
8. At the # `Proxy Settings` section, locate the `PROXY_HOST=` string. Enter the IP address or the FQDN of the proxy server after the = sign.
9. Locate the `PROXY_PORT=` string. Enter the port of the HTTP or HTTPS proxy after the = sign.
10. Click the `File` menu and click `Save`.
11. Close Notepad.
12. Open the `Start` menu and type in `POWERSHELL`.
13. Right-click the PowerShell shortcut and choose `Run as administrator`.
14. If prompted `Do you want to allow this app to make changes to your device?` click `Yes`.
15. Paste the following command into the PowerShell window and press the Enter key:

```
Get-Service WebsiteCat.Manager,GCF1Service | Restart-Service -Force  
&"C:\Program Files\ObserveIT\WebsiteCat\WebsiteCat.Manager.exe" -dw
```

It is safe to close the PowerShell window now. A download window may appear. Please do not close the new window until the operation is complete.



```
[U] DownloadDb:Progress : 30%  
[U] DownloadDb:Progress : 30%  
[U] DownloadDb:Progress : 31%  
[U] DownloadDb:Progress : 32%  
[U] DownloadDb:Progress : 33%
```

# CONFIGURING OBSERVEIT INSTALLATION

## Configuring the default *ObserveIT Admin* password

When accessing the ObserveIT Web Console for the first time, you will need to configure the password for the default *ObserveIT Admin* user account. Please follow these steps to do so:

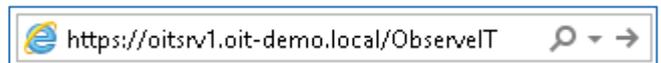
1. Open your preferred web browser, click the address bar and type in the URL address of your ObserveIT Web Console in the following format:

**https://<WebConsoleServerAddressFQDN>/ObserveIT**

For example:

**https://oitsrv1.oit-demo.local/ObserveIT**

2. You are prompted to set the password for the *admin* user.
3. At the Password and Confirm Password fields enter the password for the *ObserveIT Admin* user account.
4. Click **Log In**. Your password is now set.



admin
Confirm Password

## Generating the license registration key (for non-trial installations only)

When you install the ObserveIT server-side components using the ObserveIT Custom Installation, your product will not be licensed. The first time that you access the Web Management Console, you will need to install a license to be able to use the product.

When installing the product with a trial license, your trial license will be provided for you. However, full installations of ObserveIT require a license file that is tied to your current ObserveIT infrastructure.

To receive your non-trial license key, please perform the following steps:

1. Contact your Account Manager at ObserveIT to receive your ObserveIT serial number.
2. When you have the serial number, paste it into the Web Console's *Serial Number* field and click *Generate Registration Key*. A new window will open.
3. Right-click inside the text box in the new window and click *Select all*.
4. Right-click the selected text and click *Copy*.
5. Click the *Start* menu and type in *NOTEPAD*. Press *Enter*.
6. Right-click inside the Notepad and click *Paste*.
7. Click the *File* menu and click *Save*.
8. Navigate to your desktop.
9. At the *File name* field enter *ObserveIT License Request* and click *Save*.
10. Create a new email, attach the file from step 9 to it, and send the email to [licenses@observeit.com](mailto:licenses@observeit.com).

## Installing the ObservelT license

After receiving your license file from ObservelT Licensing Department, use the following steps to install the ObservelT license:

1. Open your preferred web browser, click the address bar and type in the URL address of your ObservelT Web Console in the following format:  
**https://<WebConsoleServerAddressFQDN>/ObservelT**  
 For example:  
**https://oitsrv1.oit-demo.local/ObservelT**
2. Log into the ObservelT Web Console.
3. At the `License File` section of the screen, click the `Browse` button.
4. Navigate to the folder you have saved your ObservelT license file to.
5. Locate the license file, click it, and click the `Open` button.
6. Click the `Activate` button. Your ObservelT installation is now activated.

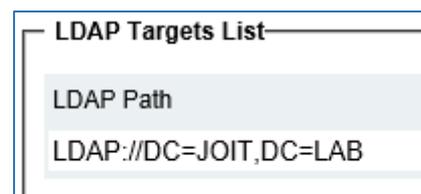
## Configuring LDAP settings

Unlike the ObservelT 1-Click Installer, custom installation of ObservelT requires manual configuration of the LDAP connector. The LDAP connector enables usage of Active Directory-based users and groups for various system settings, such as:

- Usage of AD groups in Console Users
- Usage of AD users in Secondary Authentication
- Filtering of AD groups on Secondary Authentication
- Displaying of logon messages to specific AD users
- Recording/no recording of AD users and groups
- DNS integration for Agent auto-configuration
- Usage of AD users in Identity Theft

To configure the LDAP connector, perform the following steps:

1. Open your preferred web browser, click the address bar and type in the URL address of your ObservelT Web Console in the following format:  
**https://<WebConsoleServerAddressFQDN>/ObservelT**  
 For example:  
**https://oitsrv1.oit-demo.local/ObservelT**
2. Log into the ObservelT Web Console.
3. Click `Management Console` at the top of the screen, click `Configuration`, and click `LDAP Settings`.
4. Click `Detect Domain Membership`.
5. The domain in which the ObservelT Application Server is installed will be added to the list of LDAP targets, and can now be used.



## Configuring SMTP settings

If you would like to receive email notifications from your ObserveIT installation, such as notifications, reports and alerts, configure SMTP settings.

**Note: The Web Console is responsible for sending emails from ObserveIT. Please allow the Web Console to send email via your email server.**

Use the following steps to configure the LDAP connector:

1. Open your preferred web browser, click the address bar and type in the URL address of your ObserveIT Web Console in the following format:  
**https://<WebConsoleServerAddressFQDN>/ObserveIT**  
For example:  
**https://oitsrv1.oit-demo.local/ObserveIT**
2. Log into the ObserveIT Web Console.
3. Click **Management Console** at the top of the screen, click **Configuration**, and click **SMTP Settings**.
4. At the **SMTP Server** field enter the FQDN of your email server. Adjust the **Port** field value if necessary.
5. At the **Mail From** field enter the email address which will identify the sender of ObserveIT notifications.
6. Optional: At the **User Name** and **Password** fields enter credentials for the account authorized to send emails using the specified email server.
7. Click the **Update** button to save the details.
8. To verify ObserveIT can successfully send emails, enter a working email address at the **Email Address** field and click **Send**.
9. If the verification is successful, a *Successfully Verified* message will appear and you should receive an email from an email address specified in the **Mail From** field.

## CONFIGURING ENCRYPTION

By default, ObserveIT Agents communicate with the ObserveIT Application Server by using the HTTP protocol. As a built-in security mechanism, the ObserveIT Agents and Application Server use a token exchange mechanism to prevent session hijacking and replay, and to encrypt the data communication. The security mechanisms for this communication include encryption (Rijndael), digital signing, and token exchange.

If needed, encryption can be enabled to further secure the communications:

- Between the Agents and the Application Server (HTTPS)
- Between the Application Server and the Database Server (HTTPS)
- Between the Application Server and the file share holding the graphic images (IPsec)

**Note: If you followed the custom installation guide, the ObserveIT Web Console should already be using HTTPS.**

### Data in transit encryption overview and requirements

HTTPS can be used on the ObserveIT website (either optional or mandatory) to protect the data transferred by the Agents to the ObserveIT Application Server.

**Note: This guide assumes you are only using one Application Server. If you plan to deploy more than one Application Server, you must use a network load balancing product. This can be a software-based load balancing solution such as Microsoft Network Load Balancing (NLB), or hardware-based solutions such as F5, Citrix NetScaler, or others. In that case, the digital certificate used for this traffic must be identical for all Application Servers, which can be achieved by creating it on the first Application Server, exporting it (including the private key), and importing it to the other Application Servers.**

Required steps to enable traffic encryption between the ObserveIT Agents and the Application Server:

1. Obtain a digital certificate.
2. Encrypt the traffic from ObserveIT Agents to ObserveIT Application Server.
3. Configure ObserveIT Agent for Windows to use SSL.
4. Configure the ObserveIT Agent for Unix/Linux to use SSL.

### Configuring ObserveIT Application Server for data in transit encryption

1. Connect to the ObserveIT Web Console machine.
2. Request or create a digital certificate. You can use the steps [outlined previously](#) in this guide.  
**Note: if ObserveIT Web Console is installed on this ObserveIT Application Server you can skip this step.**
3. Open the Start menu and type in `Run`. Press the Enter key.
4. Type in `IIS`, select the Internet Information Services (IIS) Manager and press the Enter key.
5. Expand the server node and expand `Sites`.
6. Right-click the `ObserveITApplication` website, and click `Edit Bindings`.
7. Click `Add`.
8. Change the value for `Type` field from `http` to `https`.
9. Make sure the value for `Port` field is set at `443`.
10. Under `SSL certificate` select the certificate you have created or acquired at step 2.

11. Click **OK** to create the bindings. Click **Close** to close the window.

**Note:** When enabling HTTPS encryption on an existing ObserveIT installation, with existing ObserveIT Agents, remember that removing an existing, non-encrypted binding, will cause existing ObserveIT Agents to cease communications with the ObserveIT Application Server. It is recommended to leave as-is the previous, non-encrypted binding at this point.

## Configuring ObserveIT Agents for Windows to use SSL

After configuring the ObserveIT Application Server to require usage of HTTPS, you will need to configure the ObserveIT Agent to use HTTPS when communicating with the ObserveIT Application Server.

### New ObserveIT Agent installations

While configuring HTTPS during deployment of new Agents, remember the following:

- During the ObserveIT Agent installation, at the Enter Application Server location screen, set the value for **Type** field from **http** to **https**. Specify the server's FQDN at the **Server Name** field. If a non-default HTTPS port is used, specify it in the **Port** field.
- If using self-signed certificates, ensure the certificates are trusted by both parties. You can skip this step if certificates from Enterprise Certificate Authority are used.
- If a firewall is enabled on the ObserveIT Application Server, ensure the correct incoming port is allowed in the firewall settings.

Type:	Server Name:	Port:
https	oitsrv1.oit-demo.local	10443

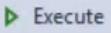
### Existing ObserveIT Agent installations

In existing ObserveIT Agent installations, when configuring HTTPS traffic between the ObserveIT Application Server and ObserveIT Agents, you must make changes in the ObserveIT Database, which will propagate to the existing ObserveIT Agents, and will configure them to use SSL when communicating with the ObserveIT Application Server.

To make changes to the ObserveIT Database for enabling HTTPS on the Agents:

1. Connect to the SQL server or to a computer with SQL Management Studio installed.
2. Open the **Start** menu, expand the **Microsoft SQL Server 2016** folder and click **SQL Management Studio**.
3. Type in the SQL server's FQDN or IP address into the **Server name** field.
4. Choose **Windows Authentication** if your account has *sysadmin* permissions on the SQL server. Otherwise, choose **SQL Server Authentication** and log in with a *sysadmin*-level account.
5. Click **OK** to connect.
6. Click the **File** menu, click **New** and **Query with Current Connection**.
7. To Check the current connection URL, paste the following code into the query window:

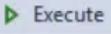
```
Use ObserveIT
select * from dbo.ServerConfiguration
WHERE PropertyId = 4
```

8. Click the  button to run the query.
9. Paste the following code into the query window, where *NEW\_APP\_SERVER\_URL* is the new address, with the HTTPS connectivity specified, and *OLD\_APP\_SERVER\_URL* is the address currently in use.

```
Use ObserveIT
UPDATE dbo.ServerConfiguration
SET PropertyValue = '<NEW_APP_SERVER_URL>'
WHERE PropertyId = 4
AND PropertyValue = '<OLD_APP_SERVER_URL>'
```

For example:

```
Use ObserveIT
UPDATE dbo.ServerConfiguration
SET PropertyValue = 'https://oitsrv1.oit-demo.local:10443/ObserveITApplication'
WHERE PropertyId = 4
AND PropertyValue = 'http://oit-srv1.oit-demo.local:4884/ObserveITApplication'
```

10. Click the  button to run the query.

## Configuring ObserveIT Agent for Unix/Linux to use SSL

Following is the overview steps required to configure OpenSSL and the Agent, to register the ObserveIT Unix/Linux Agent to an Application Server over HTTPS, using a self-signed digital certificate or a trusted internal CA certificate.

**Note: These steps apply to ObserveIT Agents that are deployed on Unix/Linux-based operating systems: Solaris, AIX, HP-UX, RHEL/CentOS, Oracle Linux, SLES (SuSE Linux Enterprise Server), and Ubuntu.**

1. Check the Agent's status.
2. Find the path to the trusted certificates.
3. Install the certificate (self-signed digital or trusted internal CA).
4. Verify reachability to the Application Server.
5. Register the Agent with the Application Server.
6. Enable the ObserveIT Service.
7. Verify the Agent's registration and health status.

For detailed instructions on how to perform the above steps, please refer to the [product documentation](#).

## Encrypting the ObserveIT Application Server to Database Server traffic

To enhance database security, communication to and from the ObserveIT database may be encrypted. This topic describes how to secure communication between the ObserveIT server-side components (Application Server, Web Management Console, and Notification Services) and the SQL database server, by using HTTPS.

The following overview outlines steps required to secure communications to and from the SQL server:

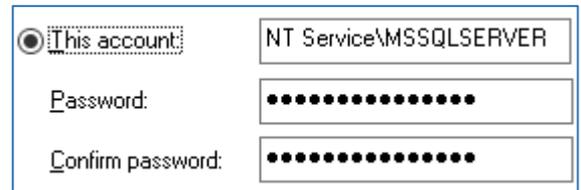
- Obtain a digital certificate.
- Configure a database server to work with the certificate.
- Configure ObserveIT server-side components to use SSL when communicating with the SQL server.

**Note: As previously, this guide assumes you are employing an Enterprise Certificate Authority certificates.**

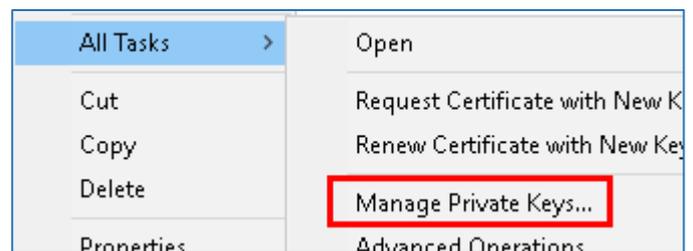
Follow this procedure:

1. Connect to the ObserveIT SQL Server machine.
2. Request or create a digital certificate. You can use the steps [outlined previously](#) in this guide.
3. Open the `start` menu and type in `Run`. Press the Enter key.

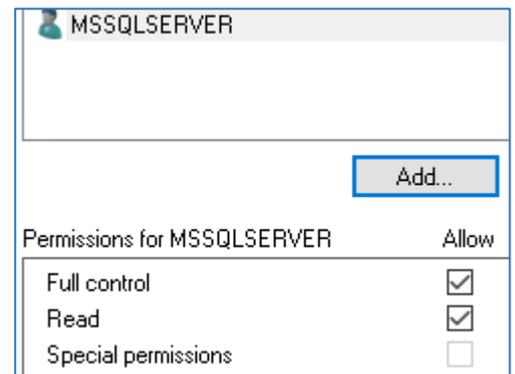
4. Type in `Services.msc` and press the Enter key.
5. Find the SQL Server service (by default - SQL Server (MSSQLSERVER)), right-click it, and click Properties.
6. Click the Log On tab and note which account starts the service. By default - NT Service\MSSQLSERVER. Copy this account name.
7. Click Cancel to close the window.
8. Open the Start menu and type in `Run`. Press the Enter key.
9. Type in `MMC` and press the Enter key.
10. If prompted Do you want to allow this app to make changes to your device? click Yes.
11. Click the File menu and click Add/Remove Snap-in.



12. From Available snap-ins choose Certificates and click Add.
13. In the Certificates snap-in window choose Computer account and click Next.
14. Under Select the computer you want this snap-in to manage select Local computer and click Finish.



15. Click OK.
16. Expand the Certificates (Local Computer) node.
17. Expand the Personal node, and click Certificates.
18. Right-click the certificate obtained in step 2, click All Tasks and click Manage Private Keys.
19. Click the Add button and click Locations. Set the location to the local server.
20. Paste the full account name you copied in step 6 into the Enter the object names to select box. Click OK.
21. Ensure that at the Permissions section, the Full Control and Read permissions are granted.
22. Click OK to save the changes and close the window.



23. Open the Start menu, navigate to the Microsoft SQL Server 2016 folder, and click SQL Server 2016 Configuration Manager.
24. Expand the SQL Server Network Configuration node, and right-click the configuration node for your current SQL instance. For example: Protocols for MSSQLSERVER. Click Properties.
25. At the Flags tab, under General, change the value for Force Encryption from No to Yes.
26. Click the Certificate tab. At the Certificate list, choose your correct certificate.
27. Click the OK button to save the changes and close the window.
28. Click the SQL Server Services node, right-click the SQL Server service and click Restart.
29. Connect to the ObserveIT Application Server.
30. Open the Start menu and type in `NOTEPAD`. Press the Enter key.
31. Click the File menu and click Open.
32. Navigate to the following path:  
`C:\Program Files\ObserveIT\Web\ObserveITApplicationServer.`
33. Next to the File Name field, change the file type value from **Text Documents (\*.txt)** to **All Files**.
34. Click the `web.config` file and click the Open button.
35. Locate the following string: **add name="ConnectionString"**.

36. Append the following value at the end of the string, before the `" />` characters: `;Encrypt=YES`

```
Info=False;Integrated Security=SSPI;Encrypt=YES" />
```

For example:

```
<add name="ConnectionString" connectionString="Data Source=SQLsrv1.oit-demo.local;Initial Catalog={0};Persist Security Info=False;Integrated Security=SSPI;Encrypt=YES" />
```

37. Click the `File` menu and click `Save`.
38. Perform steps 31 to 37 for the following additional paths:
- C:\Program Files\ObserveIT\web\ObserveIT\web.config
  - C:\Program Files\ObserveIT\NotificationService\ObserveIT.WinService.exe.config
  - C:\Program Files\ObserveIT\RuleEngineService\bin\ActivityAlerts.Service.exe.config
  - C:\Program Files\ObserveIT\HealthMonitor\bin\ObserveIT.HealthMonitor.Service.exe.config
39. Click the `Start` menu and type in `RUN`.
40. Type in `cmd`. Right-click the `Command Prompt` shortcut and click `Run as administrator`.
41. If prompted `Do you want to allow this app to make changes to your device?` click `Yes`.
42. Type in `IISRESET` and press the `Enter` key.

## Configure ObserveIT Image Security

To ensure any screenshots saved – either to the database or to the file share – are encrypted and accessible only via ObserveIT Web Console, you can configure ObserveIT Image Security. When configured, any received image is encrypted and then saved in an encrypted state.

To enable the Image Security, follow these steps:

1. Use a [previous guide](#) in this document to obtain a certificate from an Enterprise Certificate Authority.
 

**Note: to configure ObserveIT Image Security your certificate must support the *Encrypting File System* Enhanced Key Usage.**

**Note: The certificate obtained in this step must not be removed from the ObserveIT machine even after expiration. If the certificate is removed, ObserveIT will no longer be able to decrypt the stored images.**
2. Open your preferred web browser, click the address bar and type in the URL address of your ObserveIT Web Console in the following format:
 

```
https://<WebConsoleServerAddressFQDN>/ObserveIT
```

For example:

```
https://oitsrv1.oit-demo.local/ObserveIT
```
3. Log into the ObserveIT Web Console.
4. Click `Management Console` at the top of the page, click `Configuration`, and click `Security & Privacy`.
5. Click `Off` at the `Image Security` tab. New window will appear.
6. Check the `Enable Image Security` checkbox.
7. Select the appropriate certificate.
8. Click `Update`.
9. When asked `You are about to update Application Server Configuration. Are you sure?` click `OK`. The window will close and the `Off` link will change to `On`. `Changes have been saved successfully` message will appear at the top of the page.

Changes have been saved successfully.

Image Security

On

# INSTALLING OBSERVEIT AGENTS

## Installing ObserveIT Agent for Windows

An ObserveIT Agent must be installed on any computer that you want to monitor and record. You can deploy as many ObserveIT Agents as required up to the licensing limit. For a small number of monitored servers, it is recommended that you manually install the Agent on each system. For larger deployments, you may use Group Policy Software policies in conjunction with the DNS auto-configuration to deploy the ObserveIT Agents.

**Note:** for detailed system requirements for the ObserveIT Agent software, please consult the [product documentation](#).

**Note:** for detailed procedure on configuring the DNS auto-configuration, please consult the [product documentation](#).

The following steps describe how to install an ObserveIT Agent on a Microsoft Windows-based machine:

1. Connect to the computer where you downloaded and extracted the ObserveIT installer using the ObserveIT Service Account credentials.
2. Click the Start menu and type in RUN.
3. Type in CMD. Right-click the Command Prompt shortcut and click Run as administrator.
4. If prompted Do you want to allow this app to make changes to your device? click Yes.
5. Navigate to the folder with the extracted ObserveIT installer. Navigate to the Web folder.

For example:

```
cd c:\Users\OITServiceAccount\Desktop\ObserveIT_Setup_v7.1.0.136\WinAgent64bit
```

**Note:** If installing on a 32-bit system, navigate to the WinAgent32bit folder.

6. Type in WINAGENT64BIT.MSI and press Enter.

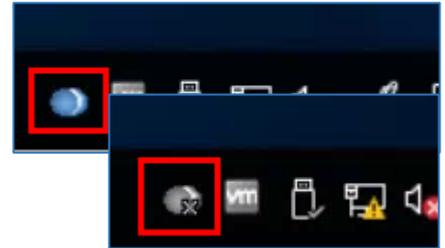
**Note:** If installing on a 32-bit system, type in WinAgent32bit.MSI.

7. At the first screen, click Next.
8. Click the I accept the terms in the license agreement if you accept the ObserveIT's End-User License Agreement and click Next.
9. At the Enter Application Server location:
  - a. At the Type field choose the connectivity type, either **http** or **https**.
  - b. At the Server Name field enter the FQDN of the ObserveIT Application Server.
  - c. At the Port field enter the correct port to which the ObserveIT Agent will connect on the ObserveIT Application Server.
10. Click Test Connection. If the connectivity test is successful, a message confirming the successful test will appear, also specifying the full connection string of the ObserveIT Application Server.
11. Click the Custom installation (Advanced options) radio button.
12. At the Recording policy drop-down list, choose Default Windows-based Policy. Click Next.
13. Review installation settings and click Install to begin the installation.

Type:	Server Name:	Port:
http	oitsrv1.oit-demo.local	4884

Type:	Server Name:	Port:
https	oitvip.oit-demo.local	10443

14. Click **Finish** to close the installer.
15. Unless otherwise specified in the recording policy, successful installation will produce the ObserveIT Agent icon in the system tray.
16. If the installation on the endpoint was successful, but the connection to the ObserveIT Application Server is not established, the icon will change accordingly.



## Installing ObserveIT Agent for Unix/Linux

**Note:** This guide assumes you are familiar with managing and administering a Unix/Linux endpoint. The example in this guide is detailed to the level of familiarity expected. If you are not familiar with Unix/Linux management and administration, please contact your systems administrator.

**Note:** This guide will install ObserveIT Agent on a CentOS 7 Operating System as an example. However, ObserveIT Agent supports all major Unix/Linux distributions. For detailed system requirements for the ObserveIT Agent software, please consult the [product documentation](#).

To deploy ObserveIT Agent for Unix/Linux please follow these steps:

1. Connect to the computer where you downloaded and extracted the ObserveIT installer.
2. Navigate to the folder with the extracted ObserveIT installer. Navigate to the `Unix-Linux Agent` folder.
3. Upload the Agent installer package for the correct Unix/Linux distribution to the Unix/Linux machine. In this example, the folder is `/tmp` and the package name is `observeit-agent-RHEL7-7.0.0.15.run`.
4. Run the installer command in the following format:

```
sudo sh observeit-agent-RHEL7-7.0.0.15.run -- -i -s
<Protocol>://<ObserveITApplicationServerFQDN>:<Port>/ObserveITApplicationServer -z
```

For example, for HTTP:

```
sudo sh observeit-agent-RHEL7-7.0.0.15.run -- -i -s http://oitsrv1.oit-demo.local:4884/
ObserveITApplicationServer -z
```

For example, for HTTPS:

```
sudo sh observeit-agent-RHEL7-7.0.0.15.run -- -i -s https://oitsrv1.oit-demo.local:10443/
ObserveITApplicationServer -z
```

5. You should receive output like this:

```
Verifying archive integrity... Done.
```

```
Uncompressing ....
```

```
The oit package was not previously installed; performing clean install
```

```
Installing observeit agent
```

```
Successfully registered this machine and saved configuration
```

```
auditing service started/running
```

```
ssh stop/waiting
```

```
ssh start/running, process 26529
```

6. Run the following command to check for the successful registration and communication with the ObserveIT Application Server: `SUDO /OPT/OBSERVEIT/AGENT/BIN/OITCHECK`

You should receive output like this:

```
Detected platform: Linux - "CentOS Linux release 7.3.1611 (Core) "
```

```
Check for oit package: PASS
oit-7.0.0.15-1.x86_64
```

```
Check for obitd service: PASS
STATUS: obitd (pid 12593 12599 12600 12603) is running...
```

```
Check that obitd daemon running: PASS
```

```
Check for /opt/observeit/agent/run directory: PASS
```

```
Check for /opt/observeit/agent/conf/obit.conf: PASS
HostURL: http://oitsrv1.oit-demo.local:4884/observeitapplicationserver
WebConsoleURL: http://oitsrv1.oit-demo.local/ObserveIT
```

```
Checking for registration by remote app server: PASS
```

```
Checking for Obit basic interception linkage: PASS
```

```
Checking SELinux status:
STATUS: enabled
MODE: enforcing
Warning: "enforcing" mode may interfere with session recording.
Selinux policy adjustment may be required.
```

This output indicates the installation ObserveIT Agent for Unix/Linux was completed successfully.

## Verifying successful user activity recording

After successful installation, you can begin using the machine. All user actions will now be recorded. You can view the recorded sessions using the ObserveIT Web Management Console.

The following steps provide an example of how to verify user activity recording and replaying. For detailed use cases, please refer to the [product user guide](#).

1. Log on to a monitored endpoint.
2. Perform several actions such as opening an application or two, typing some text in a Notepad window, running a command or two in a Command Prompt window, and opening a Control Panel applet or two.
3. Open your preferred web browser, click the address bar and type in the URL address of your ObserveIT Web Console in the following format:  
**https://<WebConsoleServerAddressFQDN>/ObserveIT**  
 For example:  
**https://oitsrv1.oit-demo.local/ObserveIT**
4. Log into the ObserveIT Web Console.
5. Click **Management Console** at the top of the page and click **Endpoint Diary**.
6. Open the drop-down list and find the endpoint in question. Click it and click **Go**.
7. Determine whether the ongoing session appears in the session list.
8. Click the  button to replay the session. Verify you can see the images.
9. Open the metadata pane by clicking the  button at the right of the player window and verify window titles and correct timestamps appear at the **User Activities List**.

# APPENDIXES

## Setting the ObserveIT databases to a simple recovery mode

Simple recovery mode is the recommended ObserveIT databases mode for a stand-alone, non-clustered SQL server. Simple recovery mode may be configured manually (as previously described in this document), or may be configured automatically via a query. Follow these steps to configure the simple recovery mode for all ObserveIT databases via a query.

1. Connect to the SQL server or to a computer with SQL Management Studio installed.
2. Open the `Start` menu, expand the `Microsoft SQL Server 2016` folder and click `SQL Management Studio`.
3. Type in the SQL server's FQDN or IP address into the `Server name` field.
4. Choose `Windows Authentication` if your account has `sysadmin` permissions on the SQL server. Otherwise, choose `SQL Server Authentication` and log in with a `sysadmin`-level account.
5. Click `OK` to connect.
6. Click the `File` menu, click `New and Query with Current Connection`.
7. Paste the following code into the `New query` window:  

```
USE master ;  
ALTER DATABASE ObserveIT SET RECOVERY SIMPLE ;  
ALTER DATABASE ObserveIT_Analytics SET RECOVERY SIMPLE ;  
ALTER DATABASE ObserveIT_Archive_1 SET RECOVERY SIMPLE ;  
ALTER DATABASE ObserveIT_Archive_Template SET RECOVERY SIMPLE ;  
ALTER DATABASE ObserveIT_Data SET RECOVERY SIMPLE ;
```
8. Click the  button to run the query.