observe IT
a **proofpoint**® company

OBSERVEIT V.7.10.X
QUICK START GUIDE

Introduction

The ObserveIT Insider Threat Management software is designed to help security operations and incident response teams easily identify and mitigate Insider threat. This document describes the steps necessary to set up and effectively deploy the ObserveIT software for a self-guided trial.

Product Version

ObserveIT version 7.10.x features includes major improvements.

This document was written for ObserveIT Enterprise version 7.10.x.

Some screenshots and procedures for Windows Server and SQL Express Server may be from earlier versions.

Major Product Enhancements in 7.10.x

- Agent Auto Upgrade: Lets you upgrade Agents directly from the ObserveIT Web Console. You have control over which endpoints to upgrade and you schedule when the endpoints will be upgraded. Agent Auto Upgrade is intuitive and easy to use. From version 7.10, you will no longer need to use a 3rd party deployment tool. The upgrade is completed and deployed from the Web Console.

- Legal Hold: When you schedule archiving to move data from the main ObserveIT database automatically or deletion to remove data automatically, you can choose to exclude all sessions for specific users/endpoints. User activity data that you may not want to include in the scheduled archiving or deletion will remain available. The excluded data will continue to be available from the Web console diaries, alerts, search and reports.

Trial Limitations

ObserveIT will provide a Not for resale (NFR) license viable for a 15-day trial period. All self-guided trials are limited in license scope to:

- 1 Windows Terminal Server License
- 2 Windows Server Licenses
- 5 Windows Desktop Licenses
- 5 Mac Desktop Licenses
- 5 Linux/Unix Multi-Purpose Licenses

System Requirements

Before running the ObserveIT install package, please review the necessary minimum requirements.

OBSERVEIT ALL-IN-ONE MANAGEMENT SERVER

ObserveIT Server side Components	Minimum System Requirements
ObserveIT Application Server Web Console Server Web Categorization Module Database Server	Hardware Requirements • 2 dual-core fast CPU • 8 GB RAM • 80 GB free hard disk space (OS) • 1 Gigabit Ethernet adapter
	Software Requirements • Operating system: Windows Server 2012 R2/ Windows 2016/Windows 2019 (64-bit only) • .NET Framework 4.5.2 or higher • SQL Express bundled installer included • IIS Configuration performed by bundled install script • Domain member (preferred) with typical server configuration

	- Local administrator's permissions - SYSADMIN permissions on the SQL instance - Mixed-mode SQL authentication

Prior to installation, you must have at least **1 virtual Windows Server** with the following specifications and components:

Note: It is the responsibility of the customer to provide all hardware/virtual machines, storage, and all networking requirements for the test environment to be ready for the installation of the ObserveIT platform.
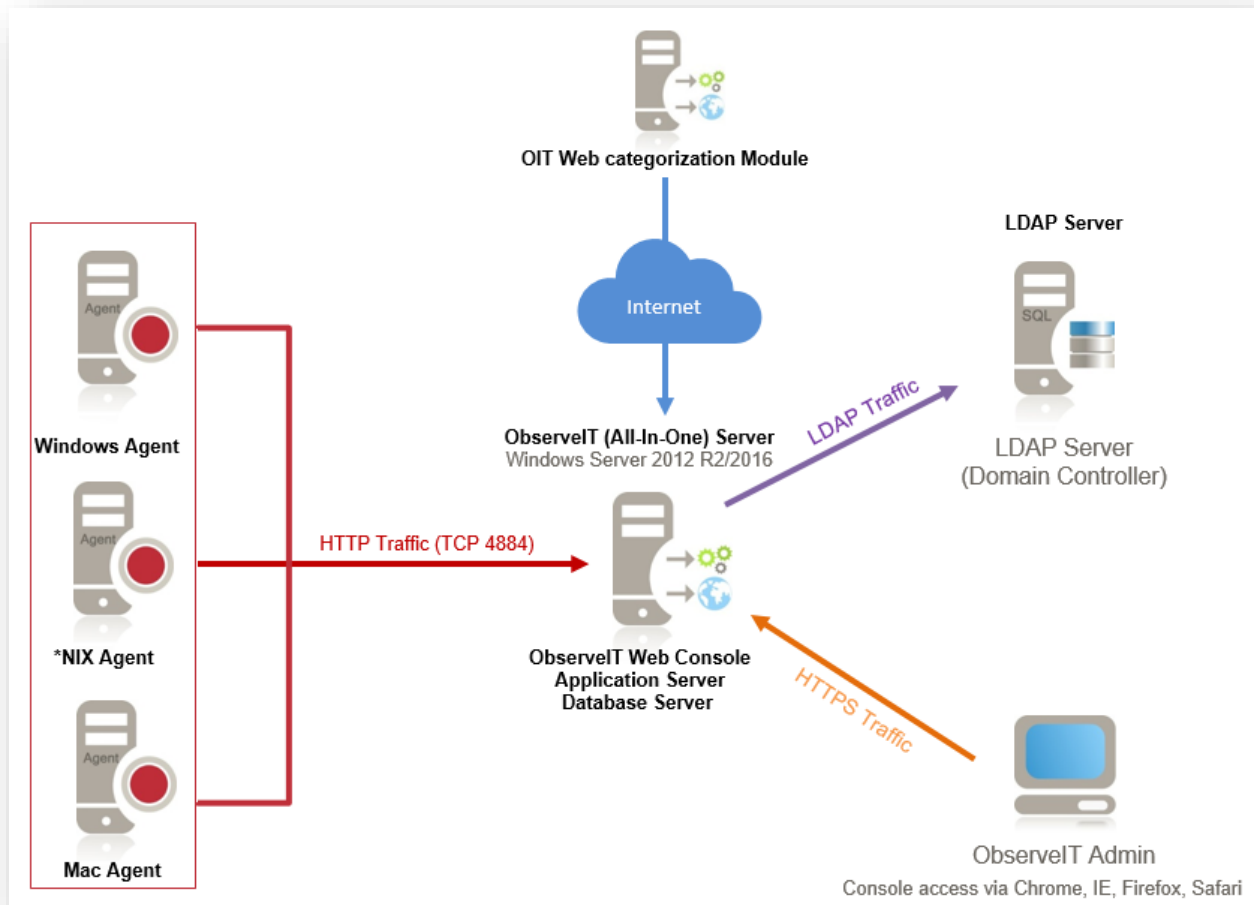
4

ObserveIT Architecture Overview

Figure 1 - All-In-One Architecture Diagram

The ObserveIT software application is comprised of the following components:

- ObserveIT Windows, *NIX, and Mac agents
- ObserveIT Web Categorization Module
- ObserveIT Application Server
- ObserveIT Web Console
- ObserveIT Database Server

Important Considerations

OBSERVEIT COMPONENT NETWORK INTERACTION

1. Each monitored desktop or server runs the ObserveIT Agent which is installed locally on the computer.

2. The Agent captures information about user activity, secures it, and sends it to the Application Server.

3. If high availability is a requirement and there is more than one Application Server, they should be load balanced by using either a software or hardware-based device. In that case the Agents will communicate with the load balancer's virtual IP (VIP).

4. The Application Server analyzes and compresses received data, then it stores it by splitting the textual data in the SQL Server database.

5. An administrator can connect to the Web Console Web-based interface using a web browser, and search for, replay, run reports and inspect alerts based on the captured user activity.

6. Any component of the data transfer or data storage process can be encrypted, if needed.

PERMISSIONS REQUIRED FOR ALL COMPUTERS

1. All computers are members of the same Active Directory domain
2. Logon permissions to these computers with administrative permissions
3. Permissions to access the SQL Server database engine (SYSADMIN permissions)
4. Full network connectivity

FIREWALL PERMISSIONS

On default configuration ObserveIT agents utilize HTTP port 4884 to communicate with the application Server and the Application Server uses port 1433 to communicate with the Database server. If firewalls are enabled, please make sure to create firewall permissions fo these ports.

Opening the firewall ports can be done via Command prompt using the following rules:

1. **For Agent to App Server:** netsh advfirewall firewall add rule name="OIT Application Server (TCP 4884)" dir=in action=allow protocol=TCP localport=4884
2. **For App Server to Database:** netsh advfirewall firewall add rule name="SQL Server (TCP 1433)" dir=in action=allow protocol=TCP localport=1433

OBSERVEIT WINDOWS AGENT

The Windows Agent is a user-mode executable that binds to every user session. As soon as a user logs into a monitored server, the Agent begins recording based on the configured recording policy.

The ObserveIT Windows Agent can be installed on any supported Windows-based operating system (server or desktop) that you want to monitor. For the trial, it is recommended that you manually install the Agent on each system to get familiar with the setup steps required.

Operating System	Minimum System Requirements
Microsoft Windows	Hardware Requirements Processor: Intel i3 or higher and AMD equivalent 4 GB RAM or more At least 1 GB free hard disk space 100 Mb/1Gb Ethernet adapter (1 Gigabit link speed recommended)
	Software Requirements Microsoft Windows Server 2012/2012 R2, 2014, 2016, 2019 Windows Vista, Windows 8.1, Windows 10 (It is recommended that you always use the latest service pack for your operating system) .NET Framework 4.5.2 must always be installed

Note: Local Administrator's permissions required to install the agent.

UNIX/LINUX AGENT

The *NIX Agent runs in user mode and is triggered when an interactive session is created on a monitored machine (connected via SSH, Telnet, Rlogin, etc.) It records user activity inside the sessions, including commands, output and system functions.

The ObserveIT agent can be installed on all Unix or Linux-based systems which require monitoring. The Unix or Linux Agent installer is a self-extracting file which includes the package and an installation script.

You can deploy ObserveIT Agents on the following Unix/Linux-based operating systems:

Operating System	Minimum System Requirements
Unix/Linux	Hardware Requirements Processor: Intel i3 or higher and AMD equivalent 4 GB RAM or more At least 1 GB free hard disk space 100 Mb/1Gb Ethernet adapter (1 Gigabit link speed recommended)
	Software Requirements Solaris 11, updates 1-3; x86/x64 or Sparc Solaris 10, updates 7-11; x86/x64 or Sparc Solaris 11, updates 1-3; x86/x64 or Sparc RHEL/CentOS 6.7-6.9 i386/x86_64/ppc64 RHEL/CentOS 7.0-7.4 x86_64/ppc64 RHEL/CentOS 7.0 7.6 x86_64 RHEL/CentOS 7.2 - 7.6 RHEL/CentOS 6.7 – 6.9 RHEL/CentOS 8.0

Oracle Linux 6.7-6.9 i386/x86_64	
Oracle Linux 7.0-7.4 x86_64	
Oracle Linux 8	
SLES SuSE 11, SP2-SP3 i386/x86_64	
SLES SuSE 12 i386/x86_64	
Ubuntu 14.04 LTS i386/x86_64	
Ubuntu 16.04 LTS i386/x86_64	
Ubuntu 18.04 LTS i386/x86_64	
AIX 7.1 32-bit/64-bit	
AIX 7.2 32-bit/64-bit	
HP-UX 11.31 Itanium architecture (64-bit)	
Debian 8 and 9 32-bit/64-bit	
Amazon Linux AMI	
Amazon Linux 2	

Note: If you require additional *NIX minimum requirements please review our detailed documentation.

MAC OSX AGENT

The ObserveIT mac Agent software can be installed on any supported Mac Platform. The software is a user mode package that will record interactive actions on Mac desktops and laptops. The agent also supports VNC for remote connections and fast user switch for recording multiple users.

The ObserveIT agent can be installed on all Mac based systems which require monitoring. The Agent installer is a self-extracting file which includes the package and an installation script.

Operating System	Minimum System Requirements
Mac OSX	Hardware Requirements 1.6 GHz or faster Intel Core processor

	4 GB RAM or more
	At least 1 GB free hard disk space
	100 Mb/1Gb Ethernet adapter (1 Gigabit link speed recommended)
	Software Requirements
	macOS High Sierra 10.13
	macOS Mojave 10.14
	macOS Catalina 10.15

PRIVACY AND LEGAL CONSIDERATIONS

If the ObserveIT software will be deployed in a production environment, consider the implications of installing monitoring software within your organization. Make sure that you seek all proper management approval and consent.

INSTALLATION PACKAGE OVERVIEW

After you have downloaded the ObserveIT installation package you will need to extract the contents. Following this step go ahead and move the file folder over to the prepared test server.

Once the installation package is transferred, look inside. You will find the following file folders:
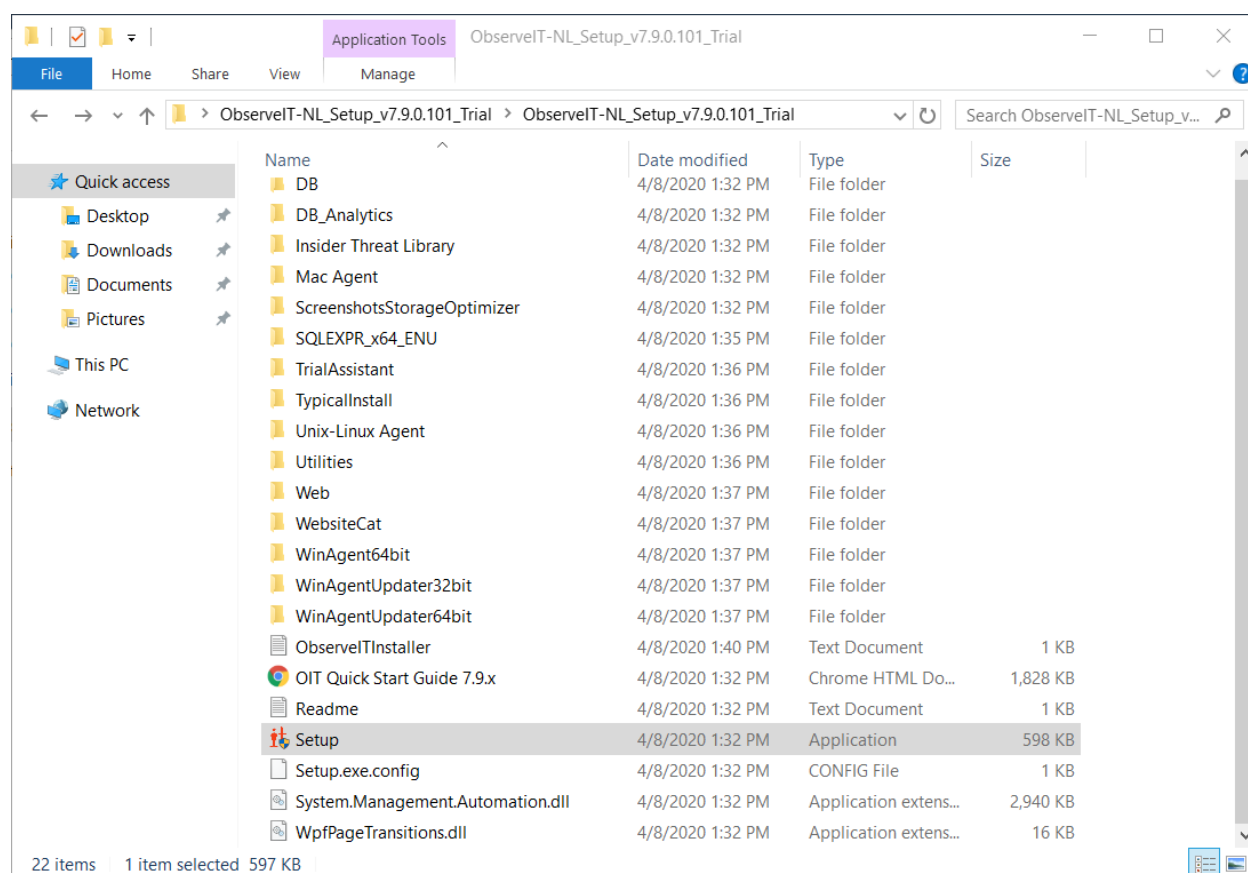
Figure 2 - Installation Folder Contents

- ✓ **DB** – Contains the setup files for the 4 ObserveIT SQL databases
- ✓ **DB_Analytics** – Contains the setup files for the ObserveIT analytics database
- ✓ **Insider Threat Library** – Contains the exported rule library for duplication and review
- ✓ **Mac Agent** – Contains the Mac agent install binaries
- ✓ **ScreenshotsStorageOptimizer** – Optimizes screenshot storage for efficiency
- ✓ **SQLEXPR_x64_ENU** – Installation package for SQLExpress for the purpose of the trial (you can use your own instance of SQL in lieu of SQL Express if you prefer)
- ✓ **TrialAssistant –** Install cleanup scripts
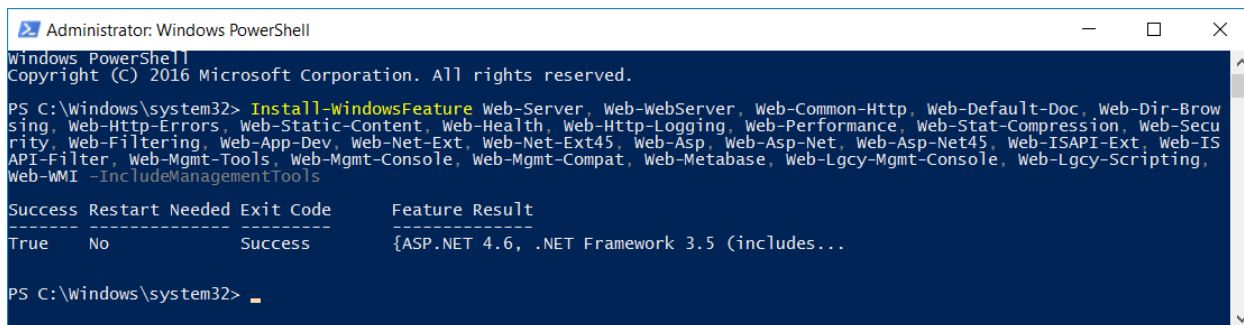
- ✓ **Typical Install** – ObserveIT one-click installation scripts and data
- ✓ **Unix-Linux Agent** – Various unix/linux agent install packages
- ✓ **Utilities** – Several useful tools such as the ObserveIT field-marking utility and Statistics collector
- ✓ **Web** – Contains the web console and application server packages
- ✓ **WebsiteCat** – Contains the new ObserveIT web categorization module
- ✓ **Winagent64bit** - Contains the ObserveIT windows agent for 64 bit systems
- ✓ **OIT Quick Start Guide** – Contains system minimum requirements and helpful notes for the latest version
- ✓ **TypicalInstall** – Folder with **ObserveIT.Installer.exe**
- ✓ **Setup.exe** – The installer that will be used for this trial

Installing SQL Express and IIS Pre-requisites

SQL Express and IIS roles are now installed and configured automatically with the one-click installer. If you already have your own SQL instance, the one-click installer will allow you to specify the location and account required to create new database instances required by the installer. It is important to verify that the account used during the installation process has the required permissions to create a database if using an existing SQL instance.

For IIS You'll want to run the Windows PowerShell as an Administrator and install the following Features with the following PowerShell command:

```
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, NET-WCF-HTTP-Activation45, Web-WMI –
IncludeManagementTools
```

Installing the ObserveIT Software

Now that we have finished the initial setup, it is time to install ObserveIT.

1. Navigate to the extracted Trial folder **ObserveIT-NL_Setup_v7.10.x_Trial** then right click and run the **Setup.exe** file as an Administrator to launch the ObserveIT one-click installer.
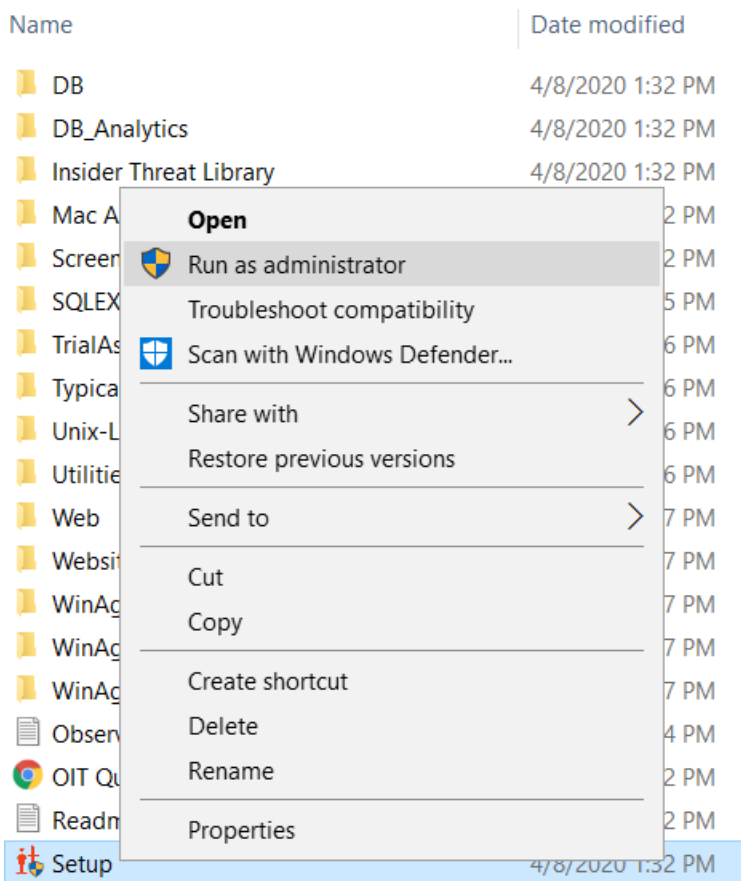
2. The installer will then scan to verify that hardware and operating system settings meet minimum requirements. If IIS is not installed, the ObserveIT installer will install and configure it for you (recommended.)
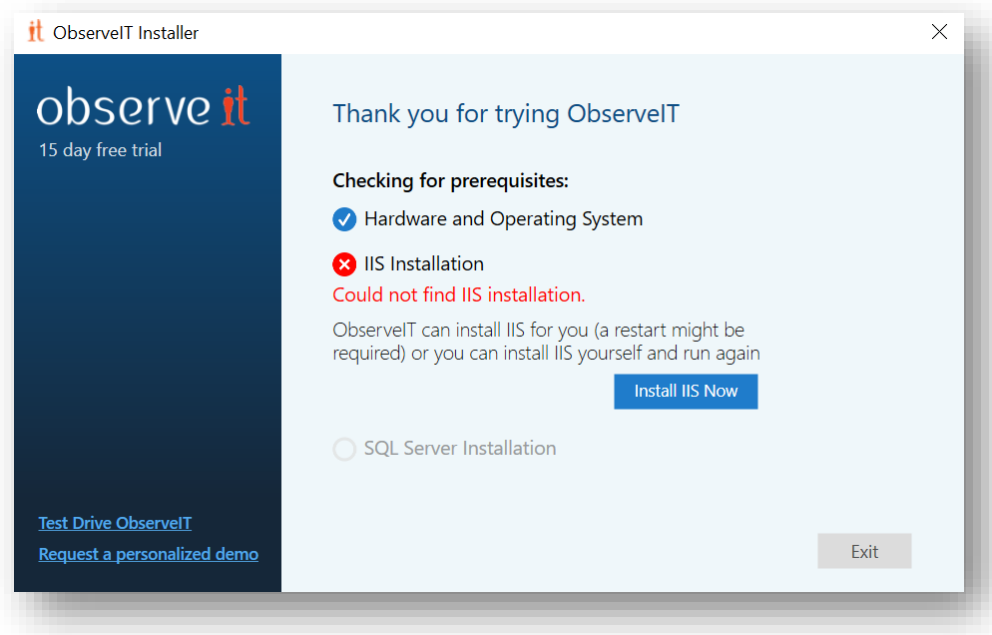
If you ran the PowerShell script above, IIS should be installed, and you are ready to proceed.
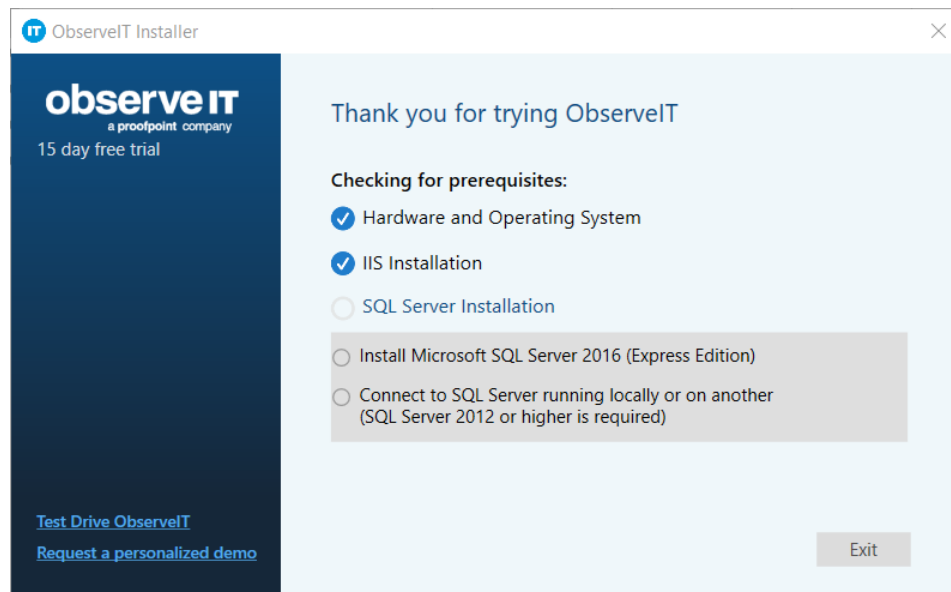
Once IIS is installed and configured, The ObserveIT installer will provide the opportunity to install an instance of SQL Express, or connect to an existing instance within your environment. If connecting to an existing instance, verify that appropriate permissions exist for your account to create a database, such as the db_creator role.

3. Select **Install Microsoft SQL Server 2016 (Express Edition)** and click **Next**
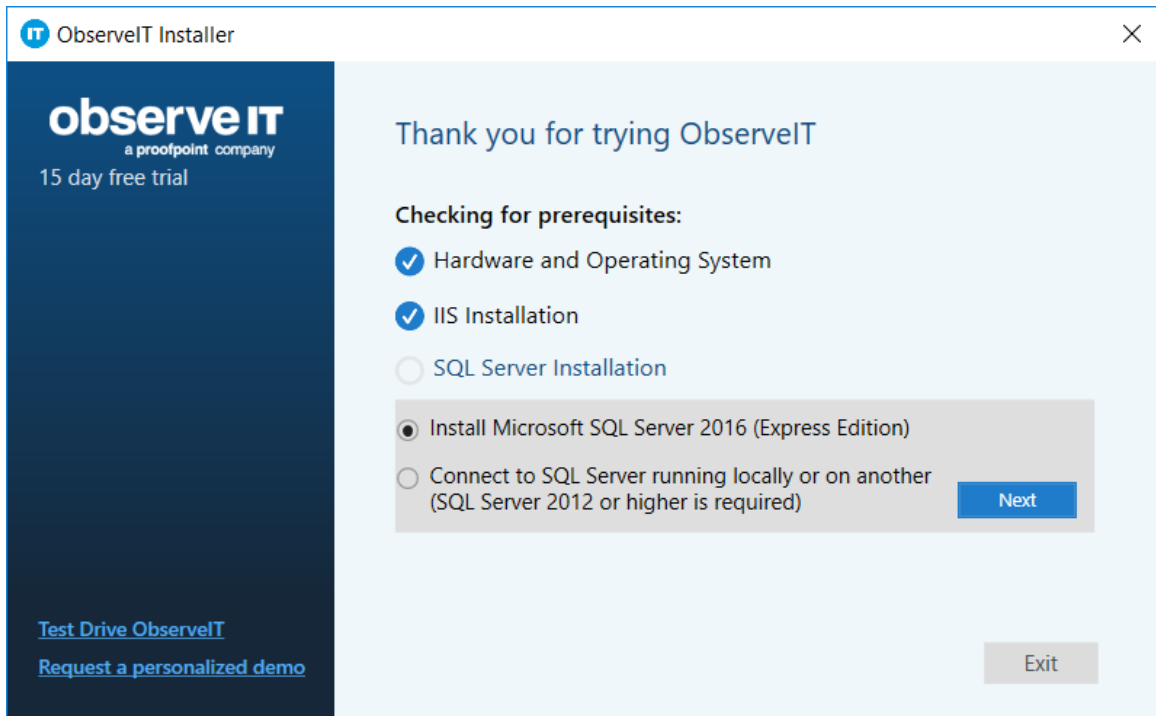
4. If you choose to install a new instance of SQL Express, the installer will use the **sa** account and prompt you to choose a new password. (The password must be at least 16 characters and include an uppercase letter, a number and a special character, for example "P@ssw1rd".)
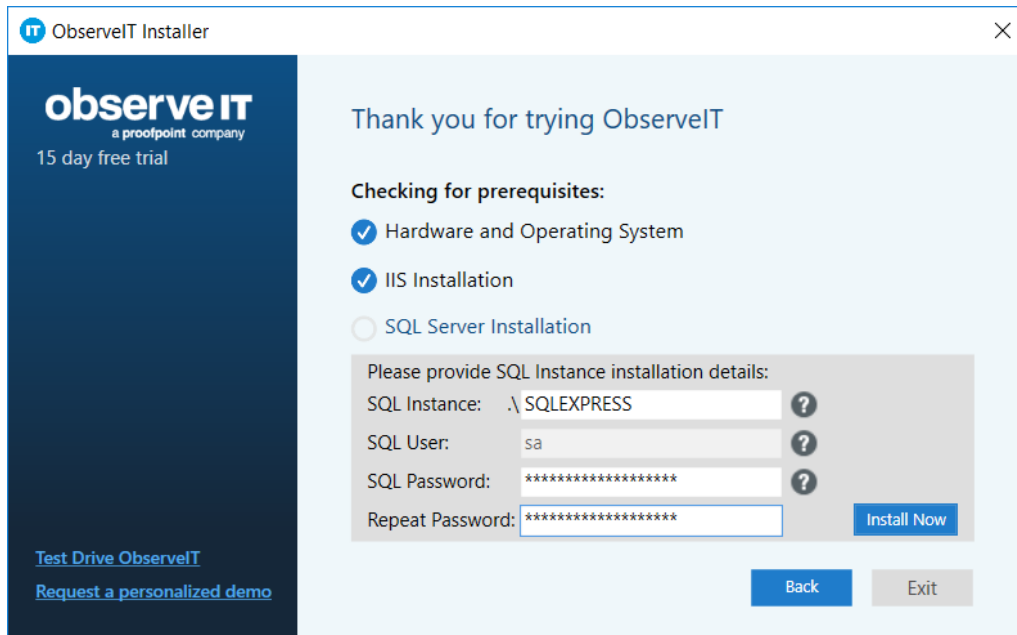
If you receive the following message to install the **PreRequisite_nodeServices.exe**, select **Run.**
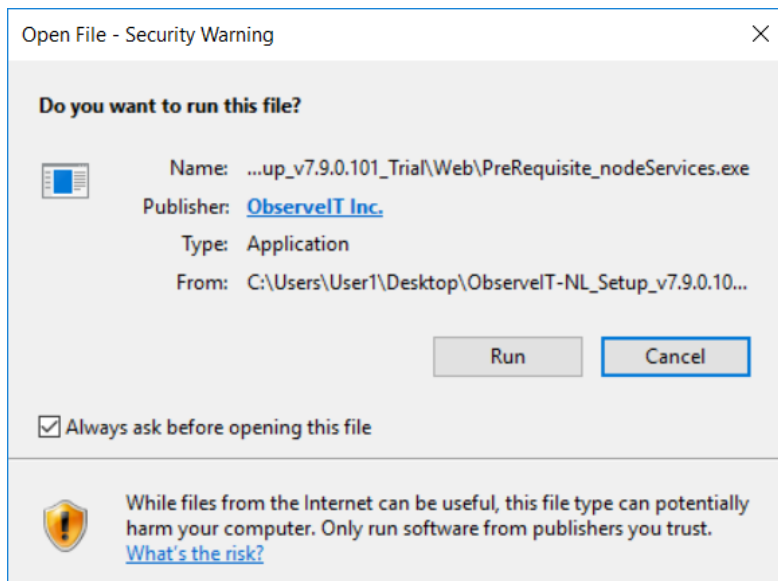
5. Once all of the base requirements are met and configured, Click **Install** to Launch the ObserveIT Installer.
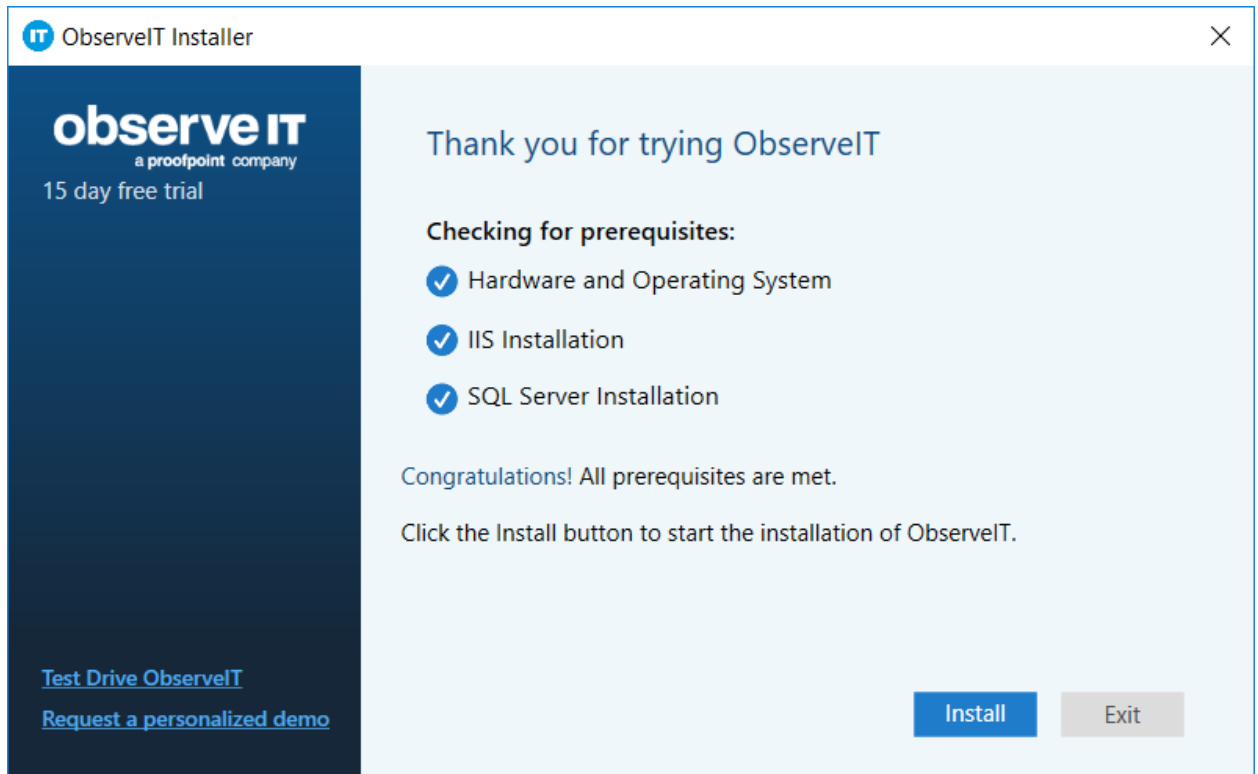
6. Select **Run** when you see the following message:
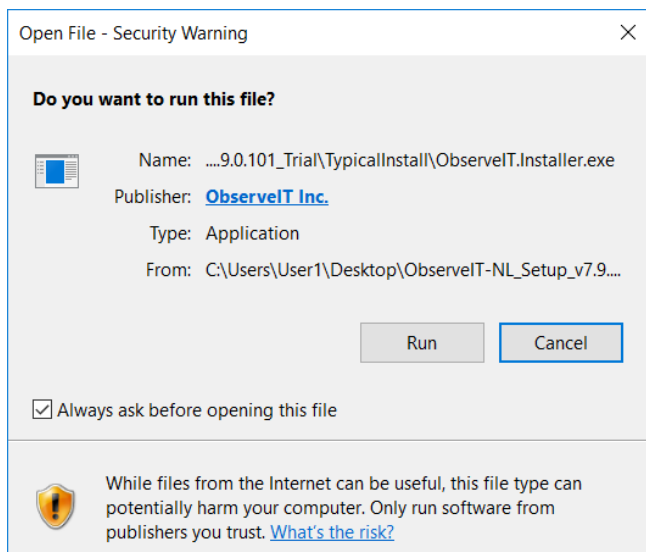
The location of the database should be automatically designated, but you will need to add the **sa** account password, or the account name and password if you manually edited this setting in the previous screens.

7. Make sure you have your ObserveIT license ready (if not you can email licenses@observeit.com) and plug it into the **Insert License** field.
8. As the final step, select **I Agree** for the Terms of Service and click Install. The ObserveIT install process will first deploy the ObserveIT databases, then the Application Server, Web Console, and finally an ObserveIT agent.

Note: If the installation fails or does not go as expected, don't worry! You are not alone. You should reach out to one of our support engineers at oit-support@proofpoint.com .
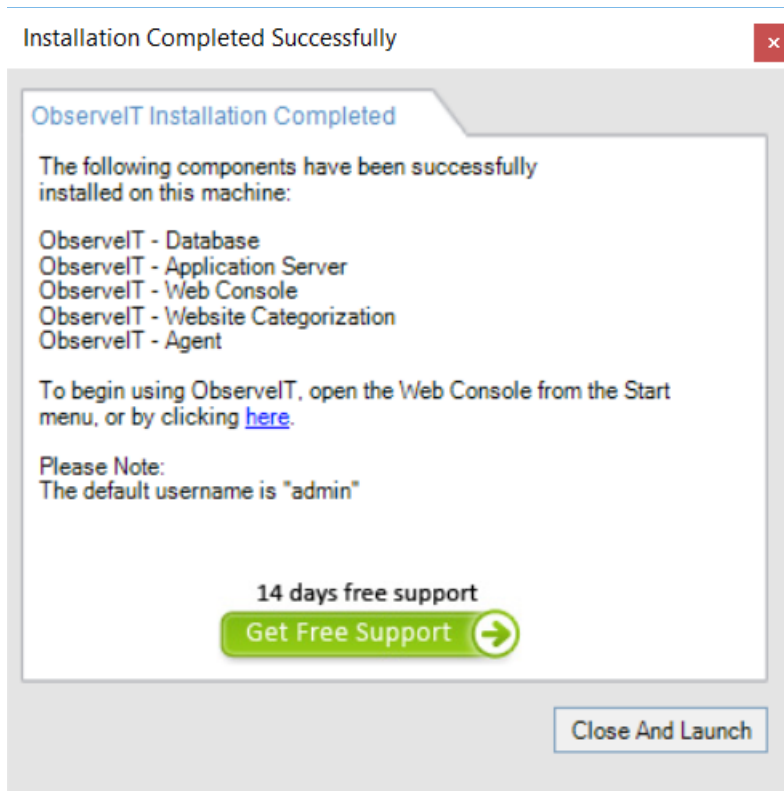
9. Click **Next** to install the Web Categorization Module to continue. The Web Categorization Module provides website categorization and detection capabilities to the ObserveIT agent and console.
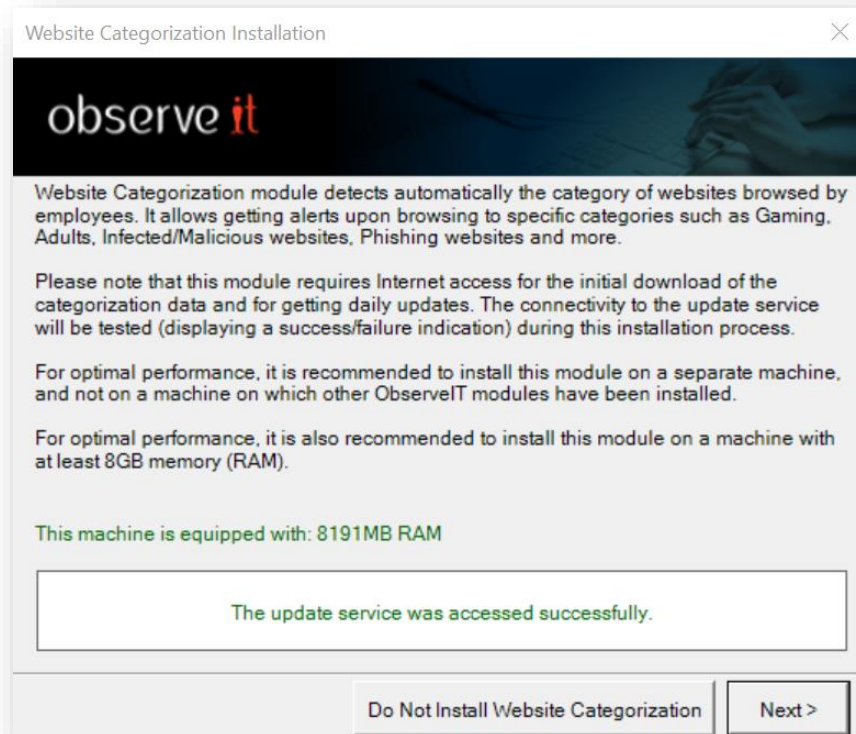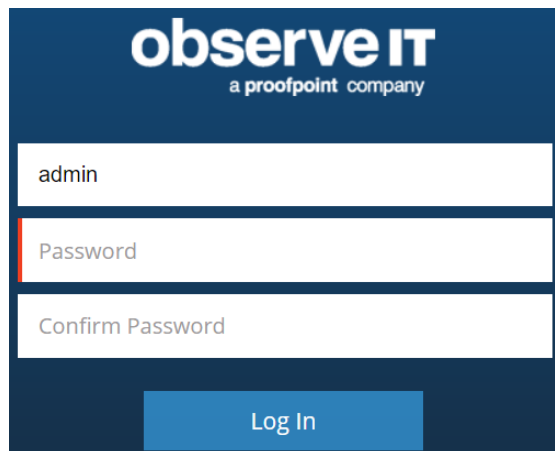
10. If you receive the following notification about installing the FTS module, select **Yes** and then install FTS at a later time.
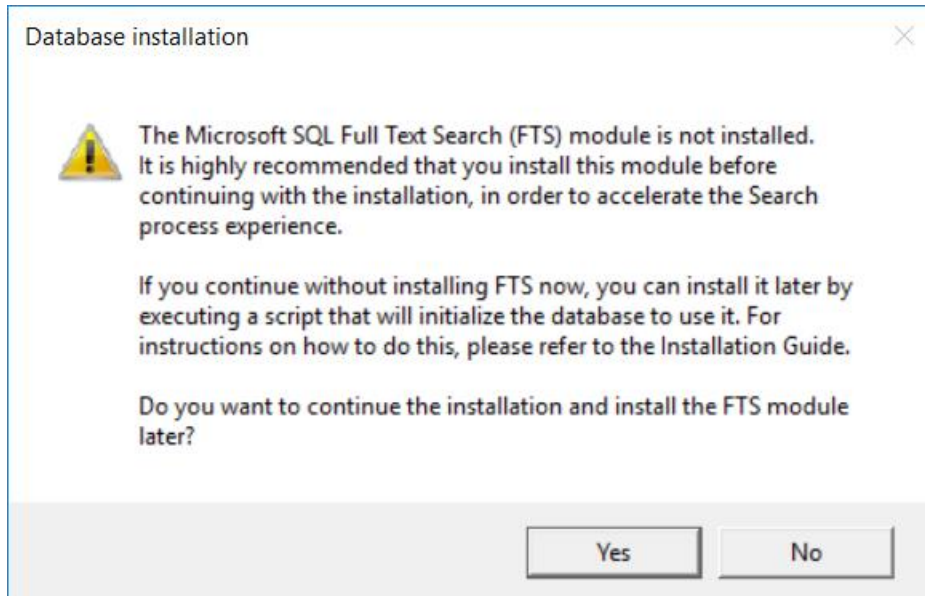
Congratulations! You have completed the installation. Click **Close And Launch** open the web console.

Installation Completed Successfully   ✕

ObserveIT Installation Completed

The following components have been successfully installed on this machine:

ObserveIT - Database
ObserveIT - Application Server
ObserveIT - Web Console
ObserveIT - Website Categorization
ObserveIT - Agent

To begin using ObserveIT, open the Web Console from the Start menu, or by clicking here.

Please Note:
The default username is "admin"

14 days free support
Get Free Support →

Close And Launch

After closing the installation window, the **ObserveIT web console** opens automatically. The login page appears. Login an and configure the initial admin password.
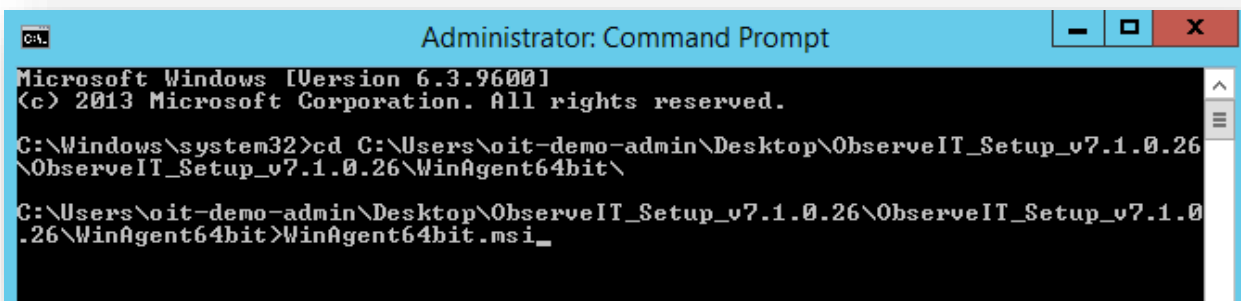
Note: For information about configuration and other settings, see ObserveIT Documentation.

Installing an ObserveIT Agent on a Microsoft Windows-based Computer

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 trial licensing limit. For a small number of monitored servers, it is recommended that you manually install the Agent on each system to familiarize yourself with the process.

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

1. Navigate to the original ObserveIT installation folder and locate the two Windows Agent installation folders. Copy the relevant file folders either manually to a target machine or to an easily accessible network share.
   - On a Windows 64-bit operating system, use the **WinAgent64bit** folder from the ObserveIT installation folder.
2. Once the correct folder has been copied over to the target machine, open an administrator privilege command prompt and navigate to the file folder location.

3. Press enter and wait until the ObserveIT Agent dialogue box initiates, then click **Next.**
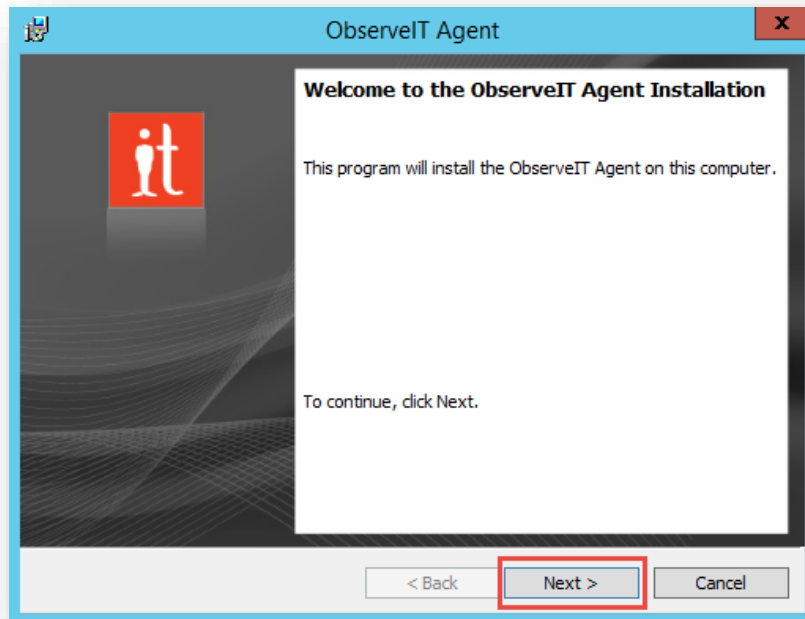
4. Select **I accept** on the End-User License Agreement stage and click **Next**.

5. On the next screen fill-in the **Server** text box, type the name of the **ObserveIT Application Server**. It is preferred that you use the server's fully qualified domain name (FQDN) or IP address.

Enter the TCP port number. By **default**, ObserveIT listens to **TCP port 4884**. When accepting the default settings during the installation of the ObserveIT Application Server. Click **Test Connection** to make sure that the communication is not obstructed by a firewall (if there is no connection, refer to **Firewall permissions** under the **Precautions** section on page 7)

If the configuration was correct, you will be notified that it was successful. Click **Ok**.
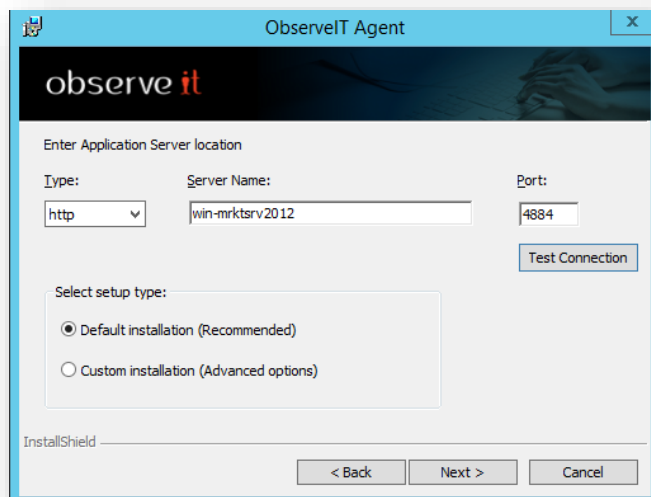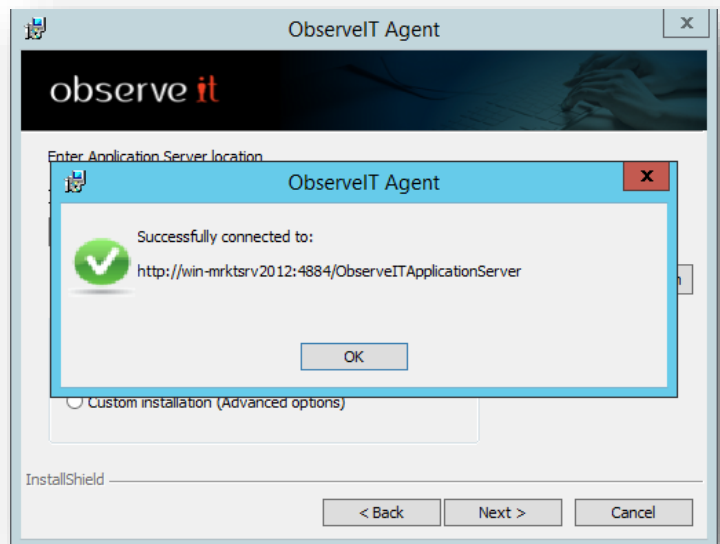
6. It is recommended to select the **Custom installation** radial box to get familiar with the custom settings then Click **Next**.
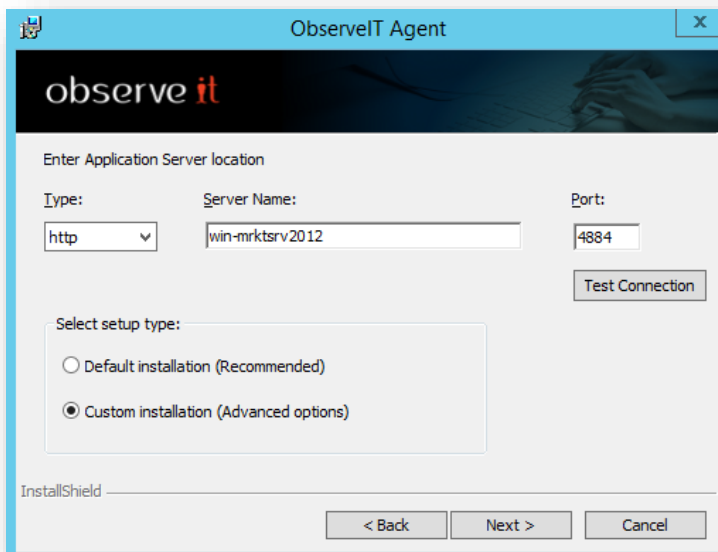
7. Set the Recording Policy to **Default Windows-based Policy.** You can also change other settings such as the installation folder, the registration state, and whether to hide the agent from the **Add/Remove Programs / Uninstall a Program** applet in Control Panel. When you finish configuration click **Next**.
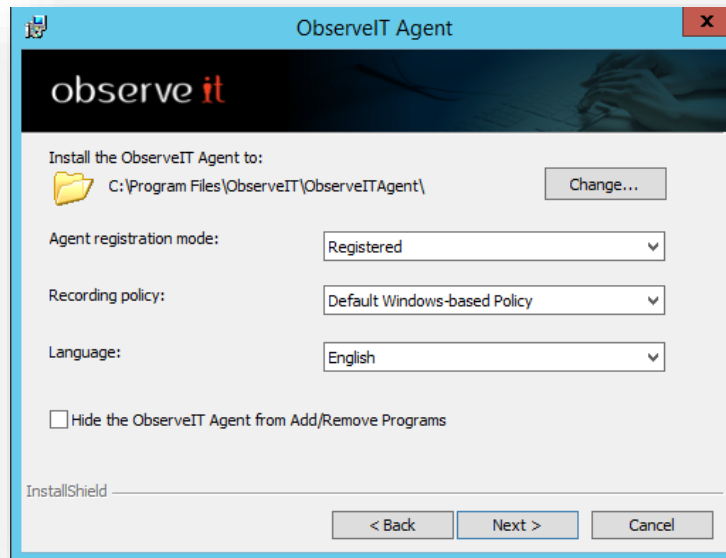

8. Make note of the settings and click **Install.**
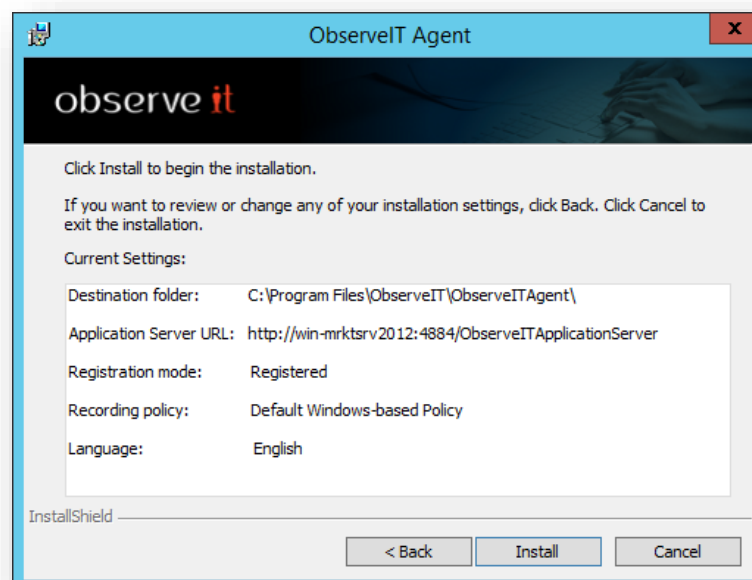
When installation is complete, click **Finish** and note the **Agent's blue** icon in the tray area.
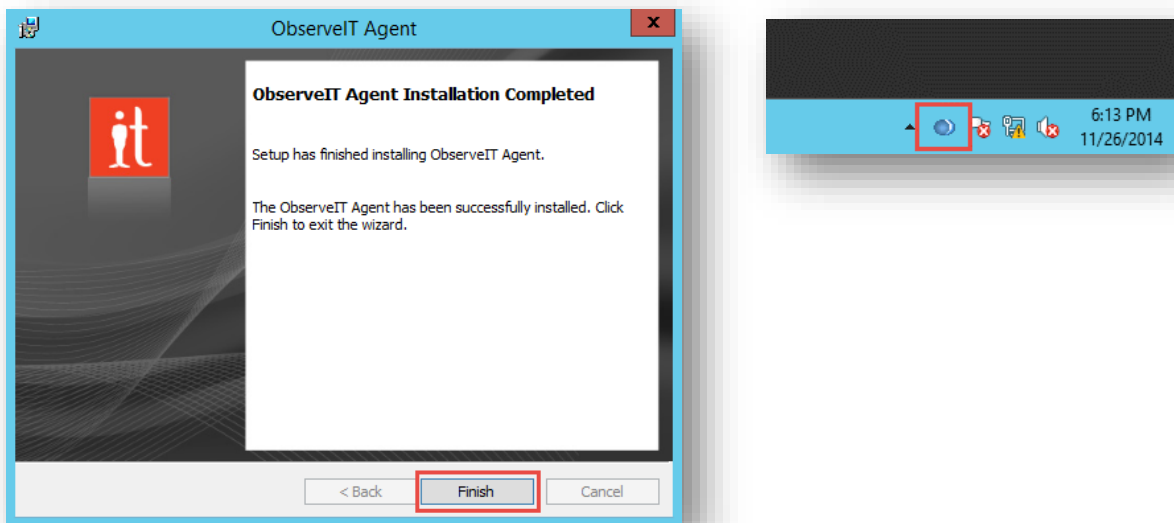
Installing an ObserveIT Agent on a *NIX-based Computer

The Unix or Linux Agent installer is a self-extracting file which includes the package and an installation script.

1. To install the *NIX agent navigate to the Unix-Linux Agent folder in ObserveIT installation package, find the relevant distribution .run file and copy it to the target server(s).
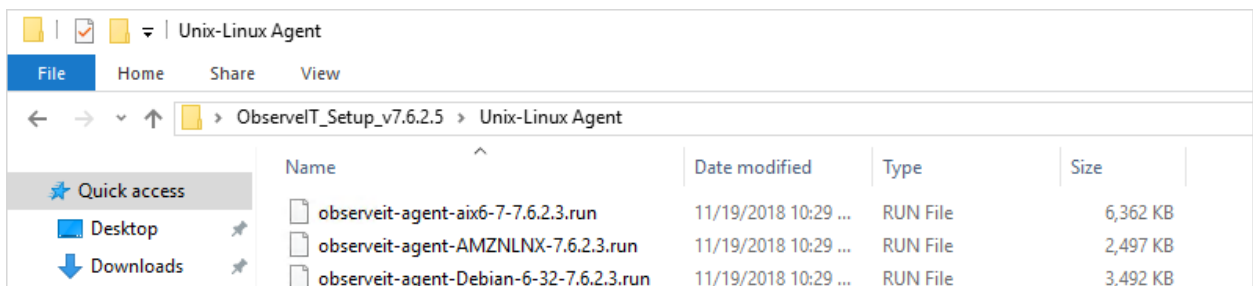
2. Log in to the target server with root permissions; or, alternatively, use the *sudo* command.

3. Run the **ls –l** command and verify that the file has execute permissions (-rwxr-xr-x). Otherwise, use chmod +x for the Agent's file name.

4. Run the command:

./observeit-agent-<*NIX_Distro>-<Dist_ver>-7.6.2.3.run -- -i -s <Application Server IP address>

Installation output:

The oit package was not previously installed; performing clean install

Installing oit agent

Successfully registered this machine and saved configuration

/usr/bin/systemctl start obitd.service

/usr/bin/systemctl restart sshd.service

/sbin/service atd restart

/sbin/service crond restart

After installing the Agent, you should log out from the current session.

Open a new SSH session and check the Agent's registration and health status in the ObserveIT web console.

Important Note!

If there are no execute permissions on the /tmp directory, installation will fail when the self-extracting script attempts to deploy the packages. To prevent installation failure in this case, run the installation command using the ⸺**target** option, as follows:

```
./observeit-agent-Ubuntu-18.04-bionic_Beaver-7.6.2.3.run --target
/work/install -- -i -s 10.3.0.72
```

If there is insufficient space in the **/tmp** folder, then you need to redirect the installation to another directory. In this case, include the **–t** option in the installation command, as follows:

```
./observeit-agent-Ubuntu-18.04-bionic_Beaver-7.6.2.3.run -- -i -s 10.1.1.1 -t
/work/tmp
```

where **/work/tmp** is the location of the new directory, if the /work/directory does not exist you must create it manually.

For registration using SSL see the ObserveIT documentation <u>Configuring a Unix Linux Agent to Use SSL</u>.

Installing an ObserveIT Agent on a Mac Computer

The Mac Agent installer is a self-extracting file which includes the package and an installation script.

1. To install the Mac agent, navigate to the Mac Agent folder in ObserveIT installation package. Find the relevant distribution .dmg file and copy it to the target server(s).
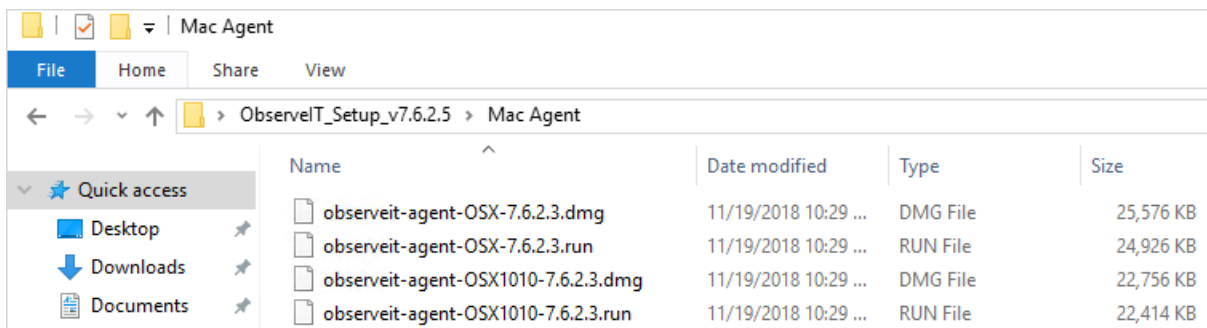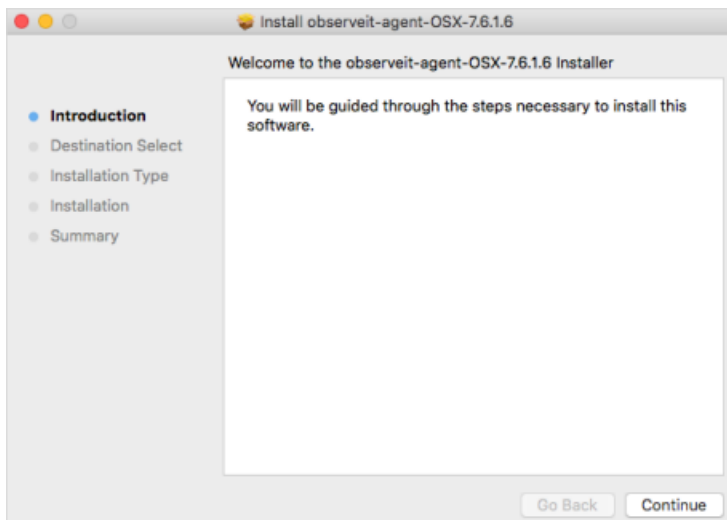

2. Double-click the .dmg file to mount it.
3. Open the mounted ObserveIT OSX agent and then open the remote folder.
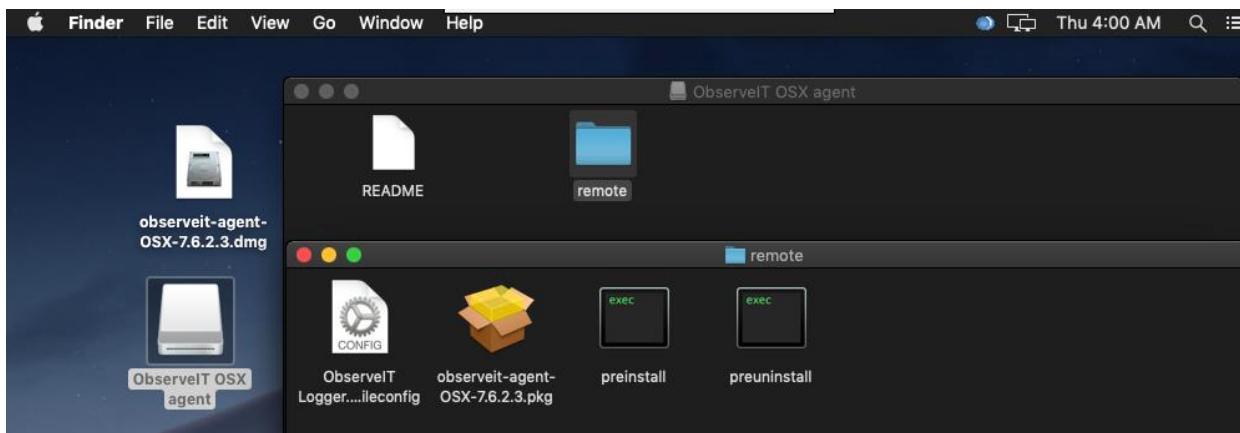
4. Run the observeit-agent-OSX-<version>.pkg package file.

   The ObserveIT Installer opens. Click Continue.

5. The ObserveIT Installer then asks you for the Installation location.

Click Install to perform a standard installation on the disk Macintoch HD.
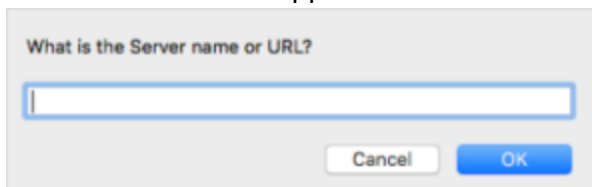
6. The ObserveIT Installer then asks you for the Password.

   Enter your password and click Install Software.
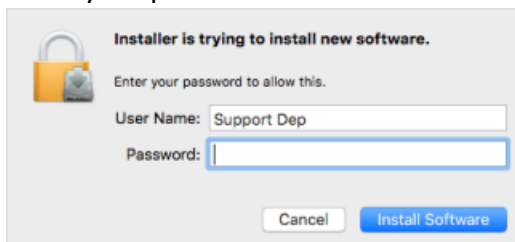
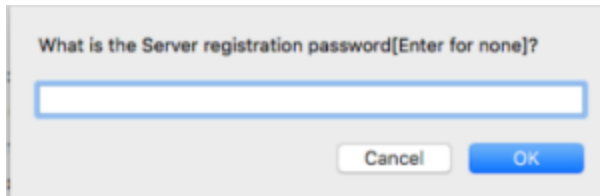7. The ObserveIT Installer then asks you for the Server Name or URL.

   Enter the ObserveIT Application Server hostname or IP address.

If the Agent is connected to the ObserveIT Application Server over SSL, first deploy the SSL certificate, and then in the registration address enter the Fully Qualified Domain Name (FQDN) in the format: https://FQDN:PORT/observeitapplicationserver (the default port for SSL is 443).
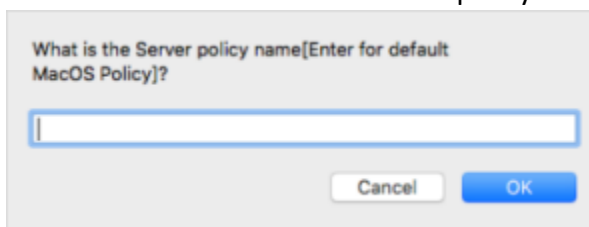
8. The ObserveIT Installer asks you for the Server registration password (optional).

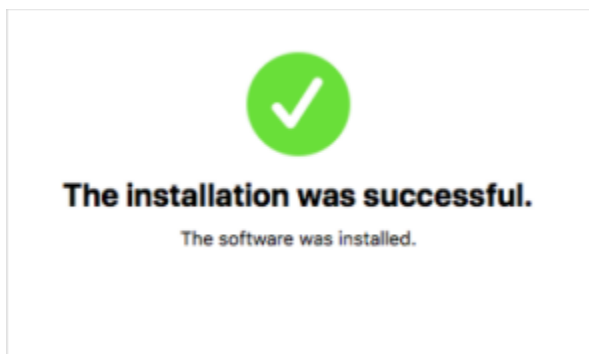Click OK to skip or enter the Server registration password if required.

9. The ObserveIT Installer asks you for the **Server policy name**.

Click **OK** to use the default MacOS policy or enter the relevant Policy ID and click **OK**.

10. The ObserveIT Installer runs.

Verifying Successful User Activity Recording

You should now be able to access the ObserveIT Web console from anywhere on your network by navigating to the url: Https://<Server_Name_FQDN>/ObserveIT

1. By default ObserveIT will open up to the ObserveIT management console, you should immediately see recorded sessions as well as the Trial duration at the top right of the screen.
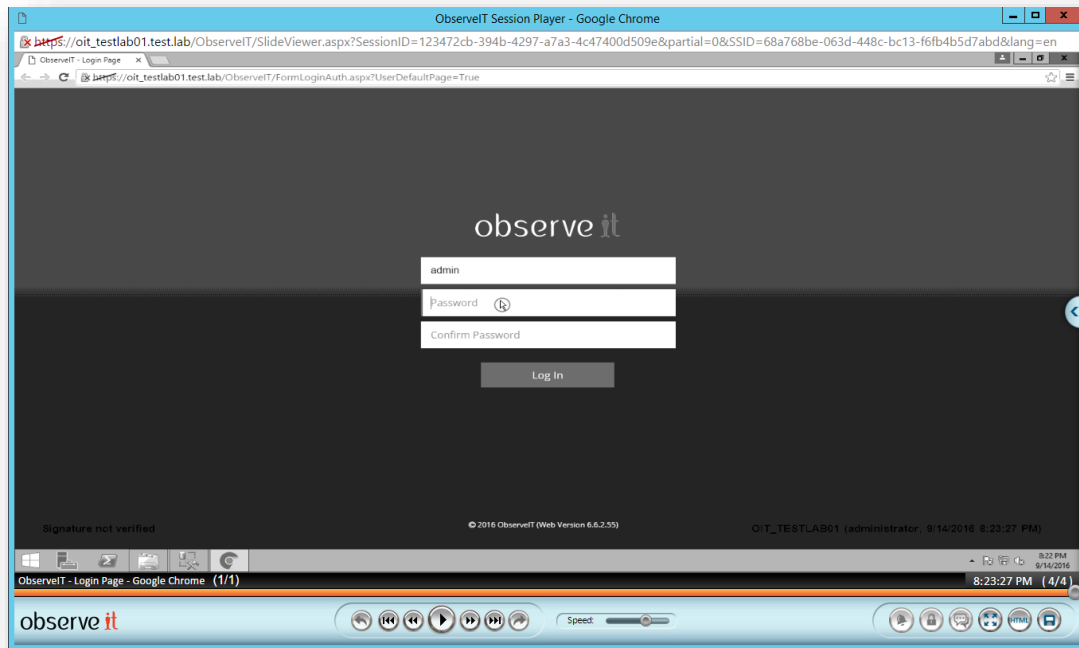
2. Go ahead and familiarze yourself with the layout of the console and expand the recorded sessions by clicking the ⌄ s to make sure metadata is being collected. Then click on the video replay button 🎥 to verify session recording.

Now you're done!

Documentation Feedback

The following online documentation will provide you with guidance for specific aspects, including system requirements and installation procedures:

[ObserveIT documentation](#)

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

ObserveIT Inc. assumes no liability for any damages incurred, directly or indirectly, from any errors, omissions or discrepancies between the software and the information contained in this document.