

Quick Start Guide Overview

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.

This document was written for ObserveIT Enterprise version 7.12.x. Some screenshots and procedures for Windows Server and SQL Express Server may be from earlier versions.

ObserveIT version 7.12.x features includes major improvements including:

MIP Labels: The Agent detects MIP label changes on tracked files. This provides additional visibility when monitoring suspicious activity on sensitive files. Using label change detection when a file is exfiltrated lets you fine tune alerts, reduce noise and gives you a more comprehensive view of file activity. Label changes display in the File Diary and File History, User and Endpoint Diary and in the Session Player views.

Linux Desktop UI Monitoring: This feature is now GA and provides a graphical view for Linux systems that support a graphical environment. The Linux Desktop Agent captures screenshots and metadata for application usage and Web browsing.

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

The table shows the minimum requirements you'll need to run the ObserveIT install package.

Before running the ObserveIT install package, review the necessary minimum requirements. It is the responsibility of the customer to provide all hardware/virtual machines,

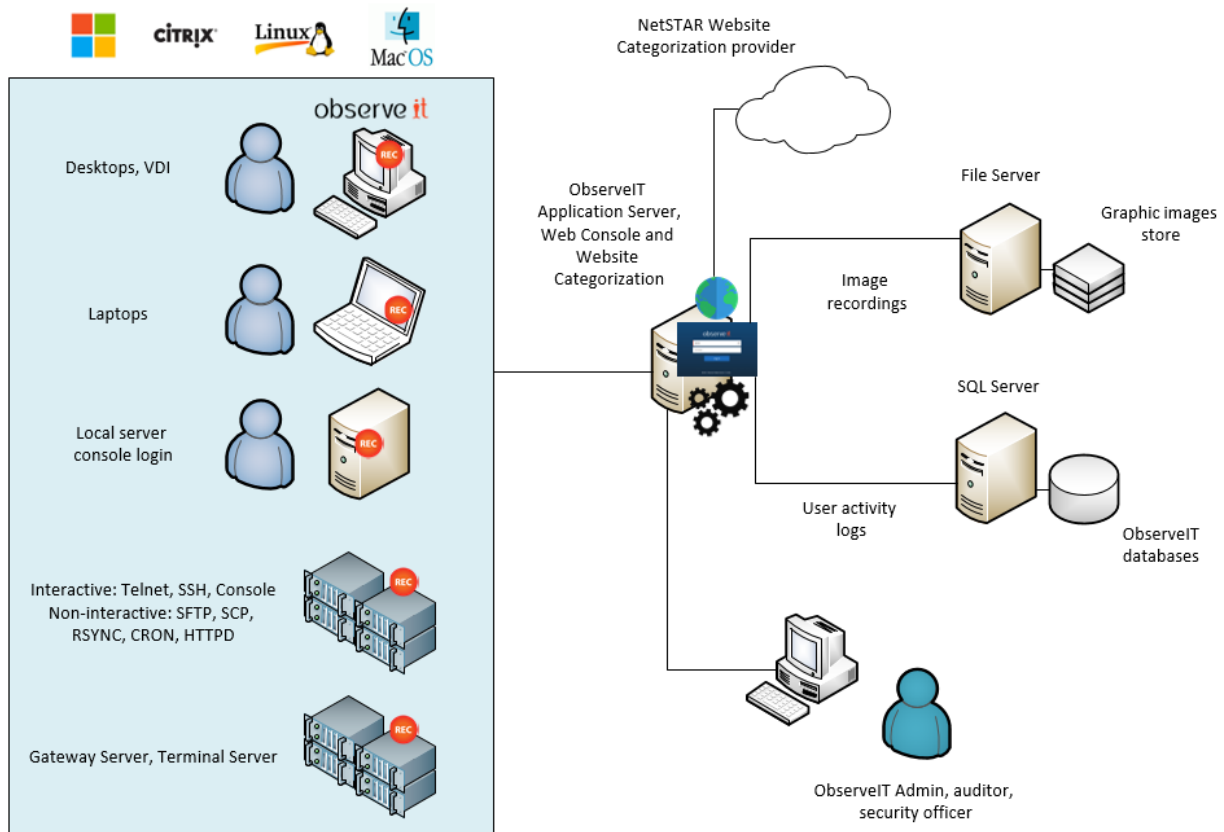
storage, and all networking requirements for the test environment to be ready for the installation of the ObserveIT platform.

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

ObserveIT Server side Components	Minimum System Requirements
ObserveIT Application Server Web Console Server Web Categorization Module Database Server	Hardware Requirements <ul style="list-style-type: none"> • 2 dual-core fast CPU • 8 GB RAM • 80 GB free hard disk space (OS) • 1 Gigabit Ethernet adapter
	Software Requirements <ul style="list-style-type: none"> • Operating system: Windows Server 2012 R2/ Windows 2016/Windows 2019 (64-bit only) • NET Framework 4.7.2 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

ObserveIT Architecture Overview

The diagram illustrates the product architecture and flow of communication between the components.



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

For more information, see [System Requirements](#) in the ObserveIT documentation.

Network and Security Requirements

Network Requirements

The following are the ObserveIT component network interaction requirements:

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

- The Agent captures information about user activity, secures it, and sends it to the Application Server.
- 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).
- The Application Server analyzes and compresses received data, then it stores it by splitting the textual data in the SQL Server database.
- 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.

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

Permission Requirements

The following are permissions required for all computers:

- All computers are members of the same Active Directory domain
- Logon permissions to these computers with administrative permissions
- Permissions to access the SQL Server database engine (SYSADMIN permissions)
- 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 for these ports.

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

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

Privacy and Legal Requirements

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.

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.

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

You can deploy ObserveIT Agents on the following Windows operating systems:

Operating System	Minimum System Requirements
Microsoft Windows	<p>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)</p> <p>Software Requirements Microsoft Windows Server 2102 2016 2019 Windows 8.1, Windows 10 (It is recommended that you always use the latest service pack for your operating system) Win 10 Enterprise Multi-Session Windows Virtual Desktop Win10 Win 10 V1903, V1909, V2004 .NET Framework 4.7.2 or higher must always be installed (or higher)</p>

ObserveIT 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.

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

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

Operating System	Minimum System Requirements
Unix/Linux	<p>Hardware Requirements</p> <p>Processor: Intel i3 or higher and AMD equivalent</p> <p>4 GB RAM or more</p> <p>A t least 1 GB free hard disk space</p> <p>100 Mb/1Gb Ethernet adapter (1 Gigabit link speed recommended)</p>
	<p>Software Requirements</p> <p>Solaris 10/11</p> <p>RHEL/CentOS 8.3</p> <p>RHEL/CentOS 8.2</p> <p>RHEL/CentOS 7.X</p> <p>RHEL/CentOS 6.7-6.10 i386/x86_64/ppc64</p> <p>Oracle Linux 6.7-6.9 i386/x86_64</p> <p>Oracle Linux 7.0-7.4 x86_64</p> <p>Oracle Linux 8.0; x86_64</p> <p>SLES SuSE 11, SP2-SP3 i386/x86_64</p> <p>SLES SuSE 12 i386/x86_64</p> <p>SLES SuSE 15.2 - 32 & 64 bit4</p> <p>Ubuntu 14.04 LTS i386/x86_64</p> <p>Ubuntu 16.04 LTS i386/x86_64</p> <p>Ubuntu 18.04 LTS i386/x86_64</p> <p>Ubuntu 20.04 LTS i386/x86_64</p> <p>AIX 6.1 32-bit/64-bit</p> <p>AIX 7.1 32-bit/64-bit</p>

	<p>AIX 7.2 32-bit/64-bit</p> <p>HP-UX 11.31 Itanium architecture (64-bit)</p> <p>Debian 8, 9,10 32-bit/64-bit</p> <p>Amazon Linux AMI 2015.03, 2017.09</p> <p>Amazon Linux 2</p>
--	--

ObserveIT macOS 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.

You can deploy ObserveIT Agents on the following macOS operating systems:

Operating System	Minimum System Requirements
Mac OSX	<p>Hardware Requirements</p> <p>1.6 GHz or faster Intel Core processor or Apple M1 Chip CPU</p> <p>4 GB RAM or more</p> <p>A t least 1 GB free hard disk space</p> <p>100 Mb/1Gb Ethernet adapter (1 Gigabit link speed recommended)</p> <p>MacBook / iMac / Mac mini</p> <p>Software Requirements</p> <p>macOS Mojave 10.14</p> <p>macOS Catalina 10.15</p> <p>macOS Big Sur 11</p>

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:

The following folders and files are included:

- 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
- SQLEXPRESS_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
- TypicalInstall folder: Contains **ObserveIT.Installer.exe**, a self-contained one-click ObserveIT installer
- observeIT.Installer.exe: The installer that will be used for this trial

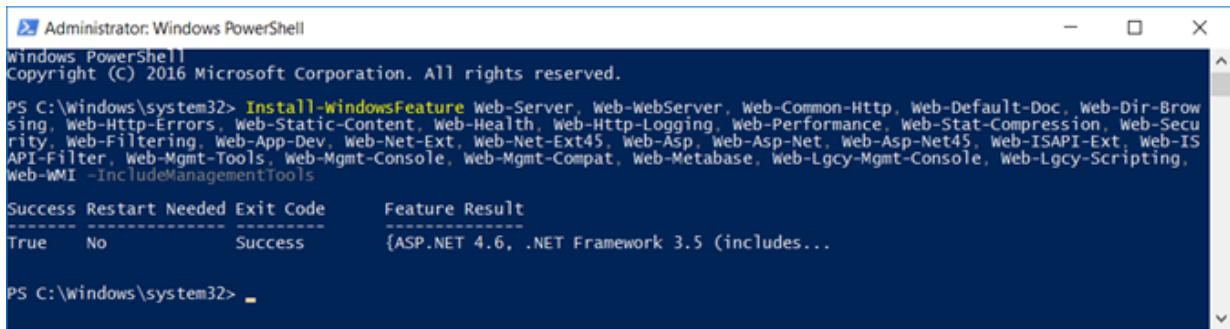
Installing IIS Pre-requisites

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



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> Install-WindowsFeature Web-Server, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-Dir-Brow
sing, Web-Http-Errors, Web-Static-Content, Web-Health, Web-Http-Logging, Web-Performance, Web-Stat-Compression, Web-Secu
rity, Web-Filtering, Web-App-Dev, Web-Net-Ext, Web-Net-Ext45, Web-Asp, Web-Asp-Net, Web-Asp-Net45, Web-ISAPI-Ext, Web-IS
API-Filter, Web-Mgmt-Tools, Web-Mgmt-Console, Web-Mgmt-Compat, Web-Metabase, Web-Lgcy-Mgmt-Console, Web-Lgcy-Scripting,
Web-WMI -IncludeManagementTools

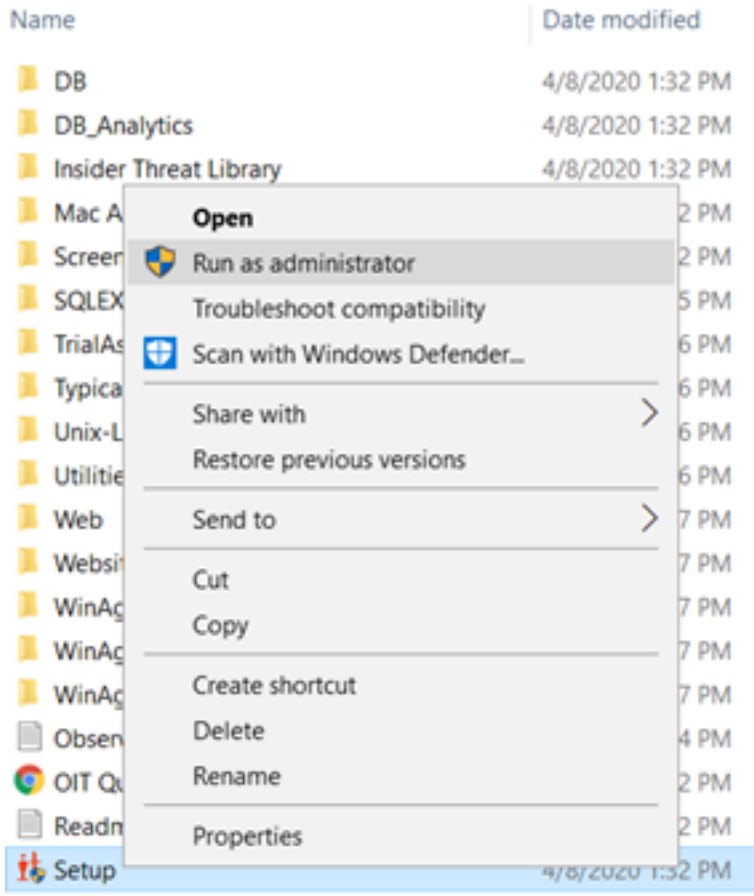
Success Restart Needed Exit Code      Feature Result
-----
True      No          Success          {ASP.NET 4.6, .NET Framework 3.5 (includes...

PS C:\windows\system32>
```

Installing the ObserveIT Software

This topic describes how to install ObserveIT One-Click installer.

1. Download the **Trial** folder **ObserveIT-NL_Setup_vX.X.x_Trial** and extract the contents.
2. Right-click and run the **Setup.exe** as an administrator.

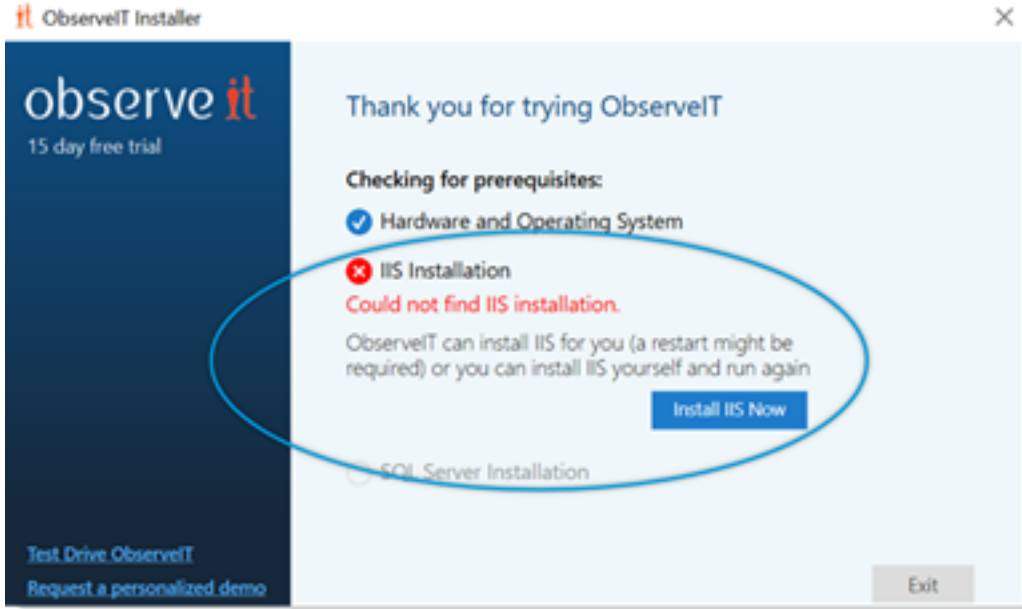


The ObserveIT One-Click installer is launched.

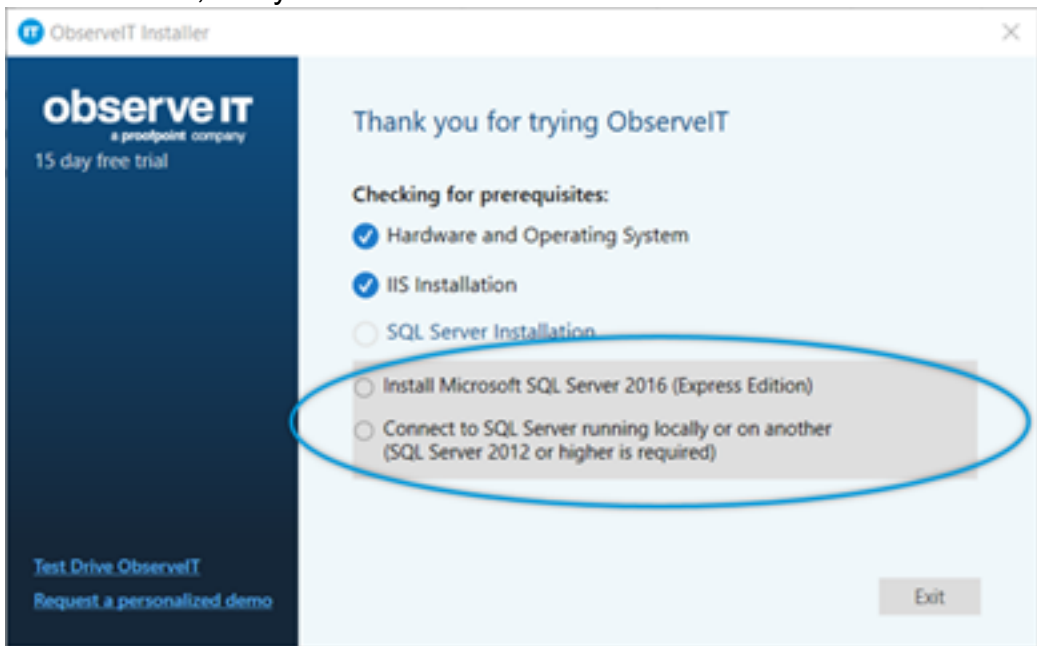
3. The installer scans to verify that your hardware and operating system settings meet the minimum requirements. (See [System Requirements](#).)

Do one of the following:

- If IIS is not installed, you'll be prompted to let the ObserveIT installer install and configure it for you. It is recommended that you click **Install IIS Now**.



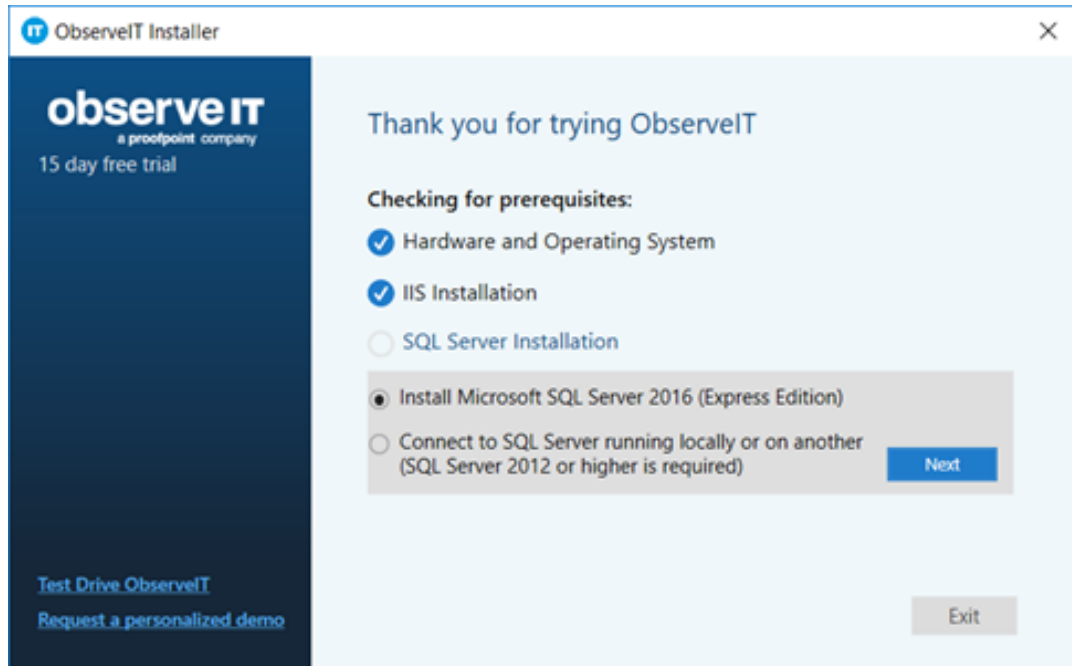
- If you ran the PowerShell script described in [Installing IIS Pre-requisites](#), IIS is installed, and you can continue.



4. The ObserveIT installer will prompt you to install Microsoft SQL Server Express or connect to an existing SQL Server in your environment.

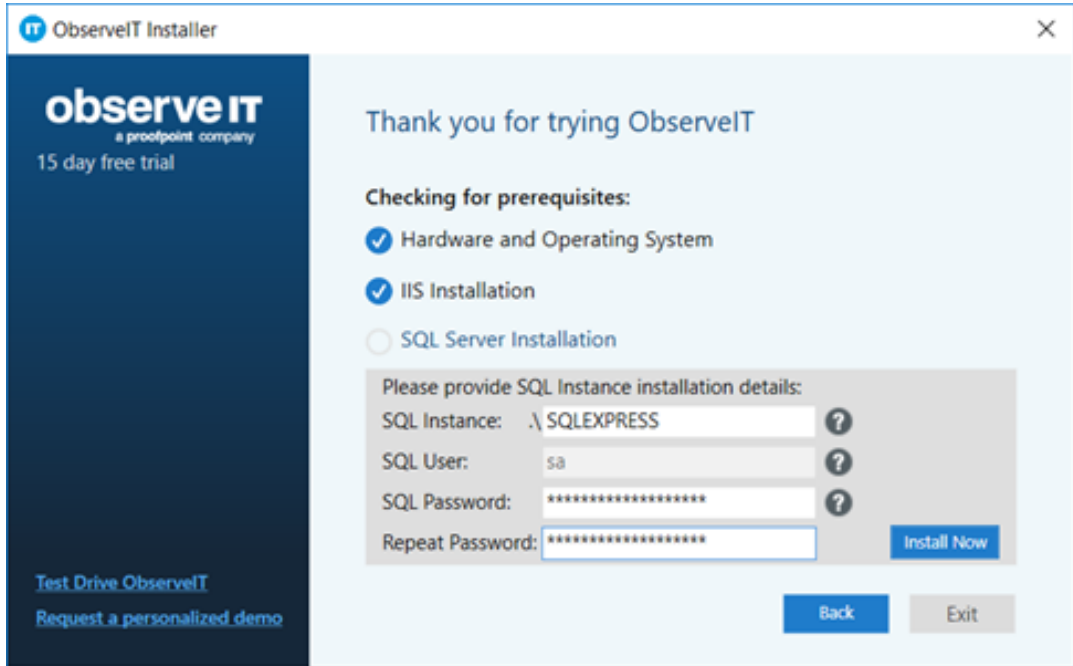
Do one of the following:

- If you are connecting to an existing SQL Server, verify that appropriate permissions exist for your account to create a database, such as the db_creator role.
Select **Install Microsoft SQL Server 2016 (Express Edition)** and click **Next**.

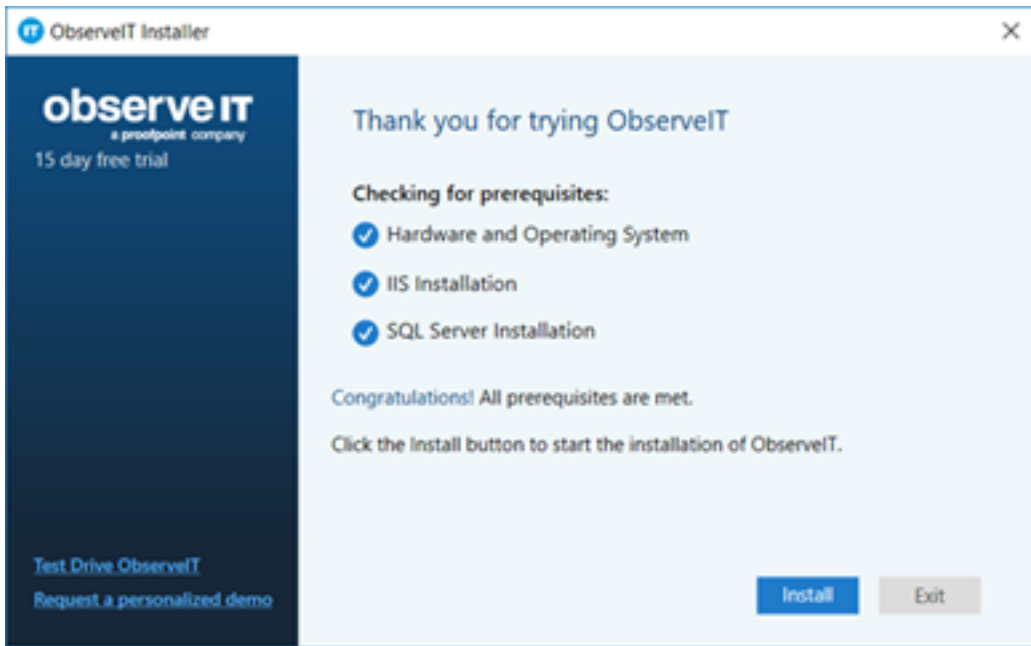


- If you choose to install a new instance of SQL Express, select **Connect to SQL Server running locally or on another**. The installer will use the “sa” account and prompt you to choose a new password. (The password must be at least 16 characters and include an uppercase letter, a number and a special

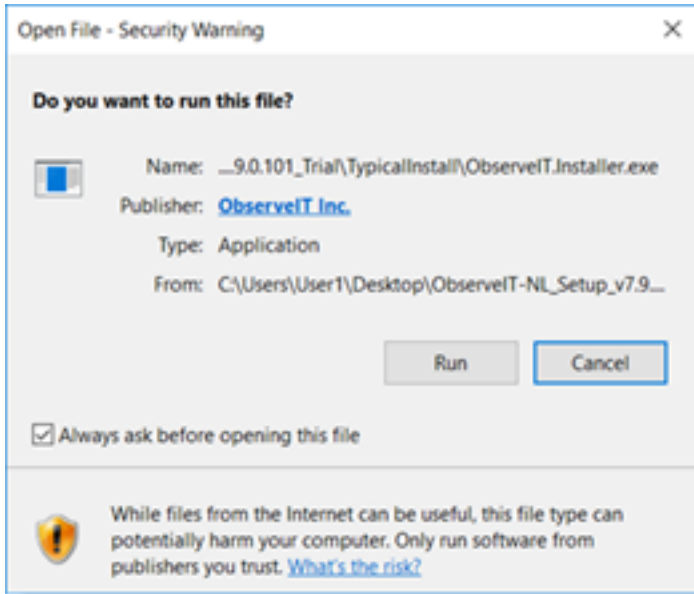
character, for example “P@ssw1rd”).



5. When the prerequisites are met, click **Install** to start the installation.



6. When prompted, click **Run**.

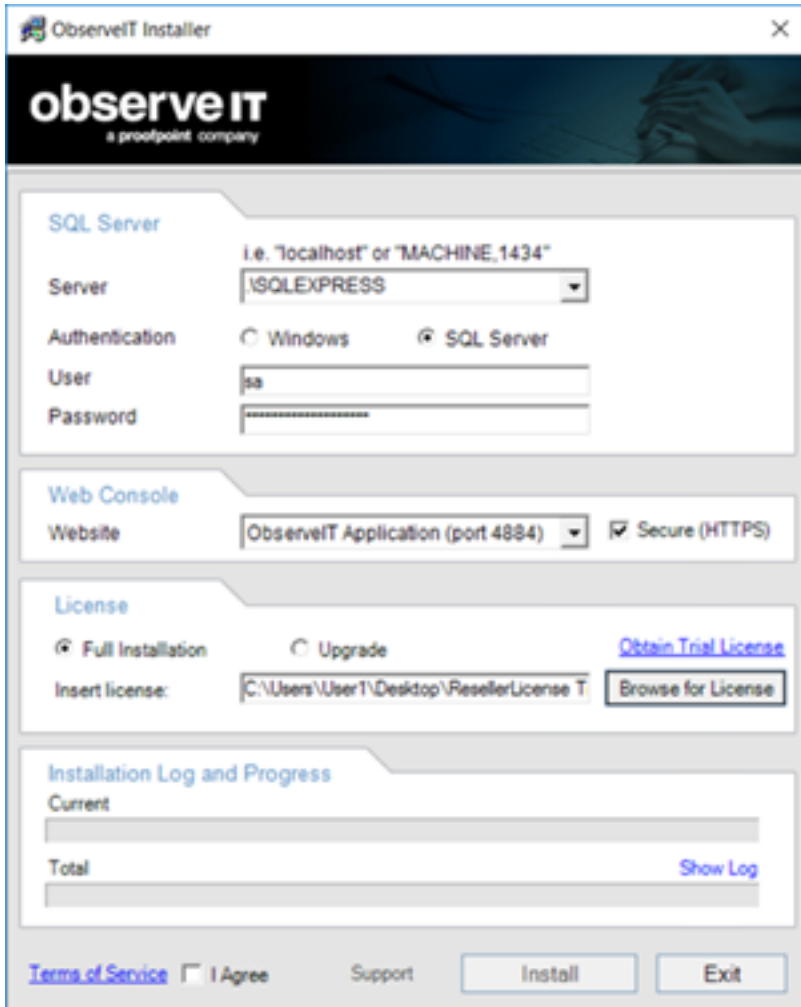


The location of the database should be automatically designated, but you will need to add the “sa” account password, or the account name and password if you manually edited this setting previously.

7. Make sure you have your ObserveIT license ready. When prompted complete the **Insert license** field.

(If you do not have your license, email licenses@observeit.com.)

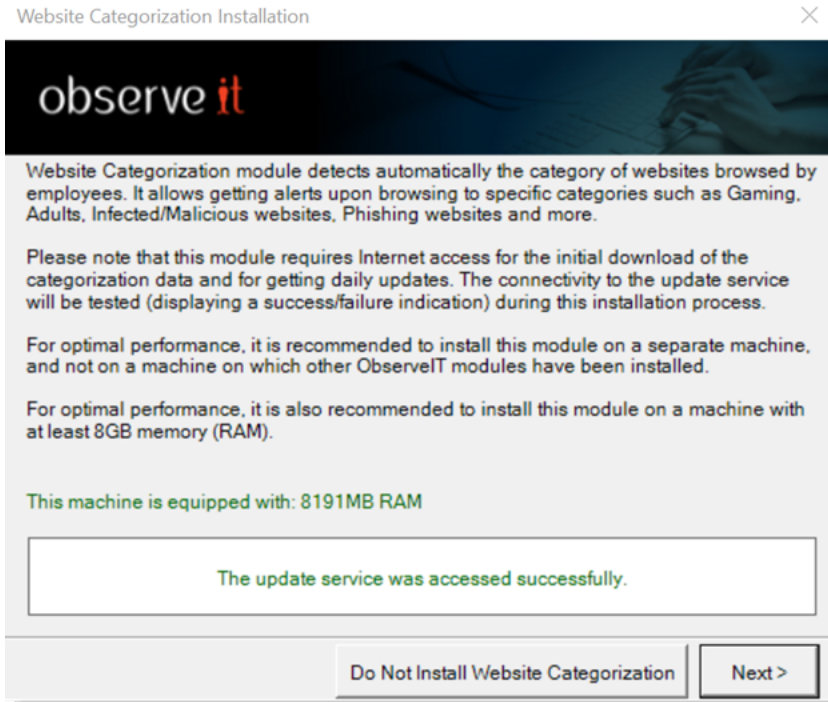
8. Select **I Agree** in the **Terms of Service** and click **Install**.



The ObserveIT install process deploys the ObserveIT databases, then the Application Server, Web Console, and finally an ObserveIT Agent.

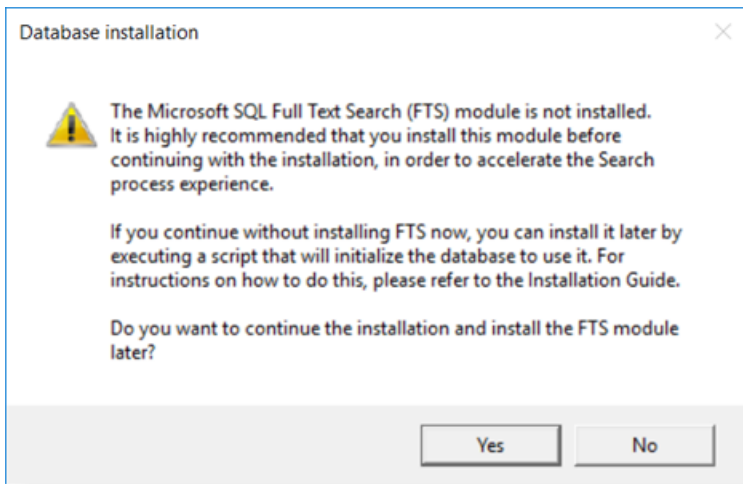
If the installation fails or does not go as expected, contact **support@ObserveIT.com**.

9. You are prompted to install the **Web Categorization Module**. The **Web Categorization Module** provides website categorization and detection capabilities to the ObserveIT Agent and console.

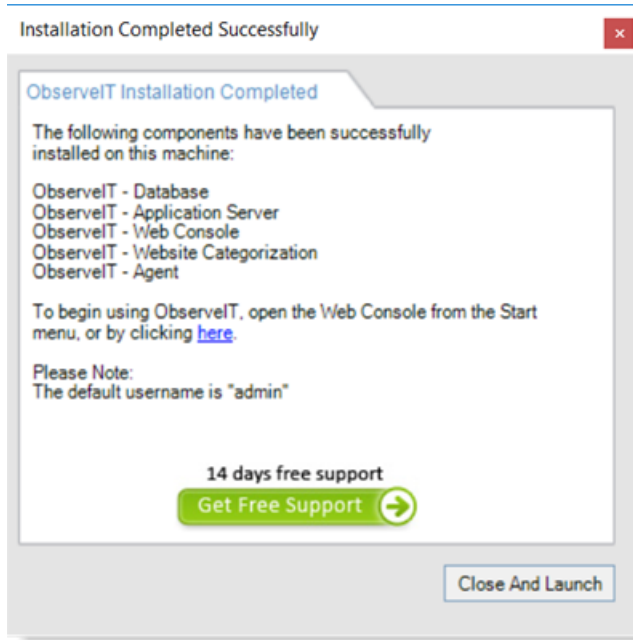


10. Click **Next** to install.

If you receive notification about installing the FTS module, select **Yes** and then install FTS at a later time.



11. The installation is complete. Click **Close and Launch**.



Congratulations! You can now open the ObserveIT Web console.

12. Click **Close And Launch** and the ObserveIT Web console opens to the login page. Log in and configure the initial admin password.
13. From version 7.12.0, before deploying the Agent, you must download the JWT file with authentication details. (See [Configuring Service Settings](#).)

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.

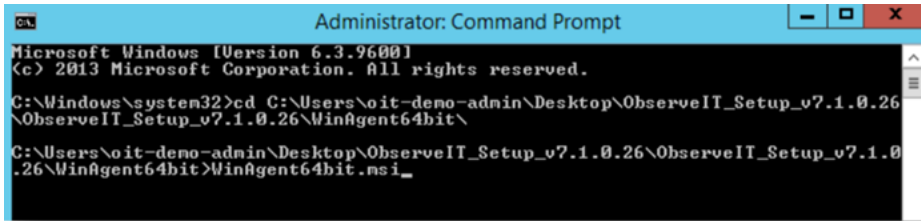
Note: Before installing a Window or Mac agent, you must download a JWT File that you will provide during the installation. This file can be downloaded from the **Configuration > Settings > Service Settings**.

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.

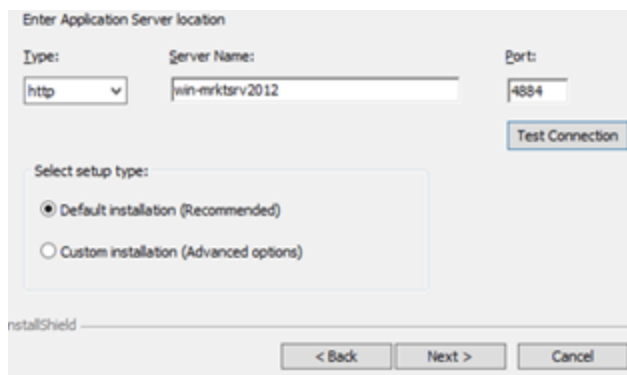
On a Windows 64-bit operating system, use the “WinAgent64bit” folder from the ObserveIT installation folder.

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.



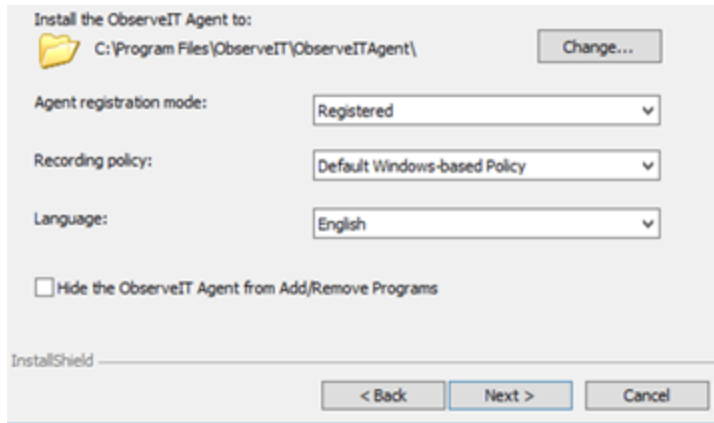
3. Enter and wait until the ObserveIT Agent dialogue box initiates, then click **Next**.
The ObserveIT Agent wizard opens.

4. Accept the End-User License Agreement and click **Next**.

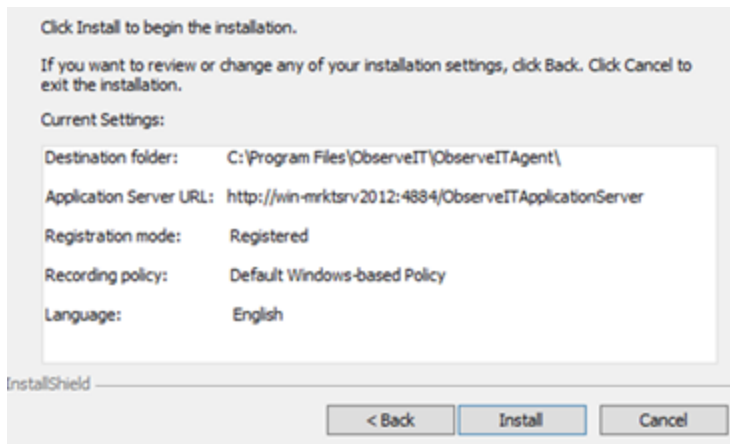


5. In the **Server Name** field, enter the name of the ObserveIT Application Server. It is preferred that you use the server’s fully qualified domain name (FQDN) or IP address.
6. In the **Port** field, enter the TCP port number. By default, ObserveIT listens to TCP port 4884. When accepting the default settings during the installation of the ObserveIT Application Server.

7. Click **Test Connection** to make sure that the communication is not obstructed by a firewall.
8. If the configuration was correct, you will be notified that it was successful. Click **OK**. Click **Next**.
(If there is no connection, see [Firewall Permissions](#)).
9. Select **Custom installation** and click **Next**. This is recommended to help you get familiar with the custom settings.



10. From the dropdown **Recording Policy**, select **Default Windows-based Policy**.
11. If you want to change other settings such as the installation folder, the registration state, and whether to hide the agent from the Add/Remove Programs, click **Change**.



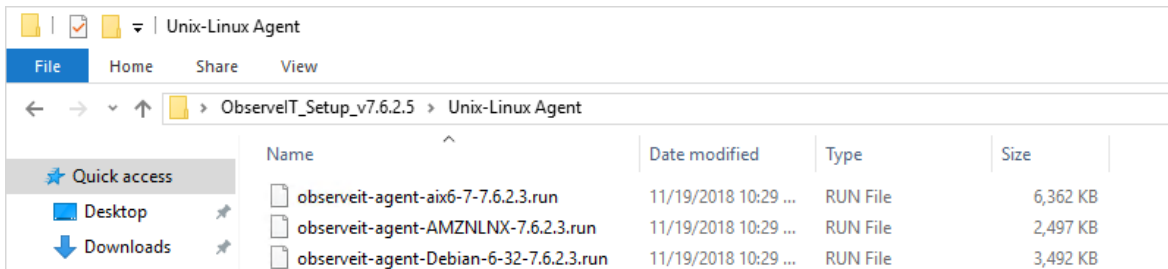
12. Make a note of the settings and click **Install**.

13. When installation is complete, click **Finish** and you'll see 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>
```

The following output should appear:

```
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
```

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

6. 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.

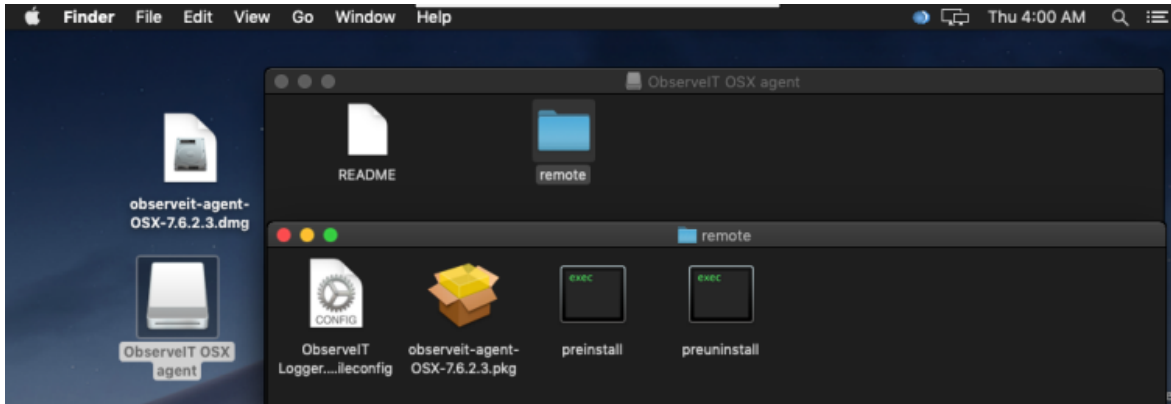
For registration using SSL see the ObserveIT documentation [Configuring a Unix Linux Agent to Use SSL](#).

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.

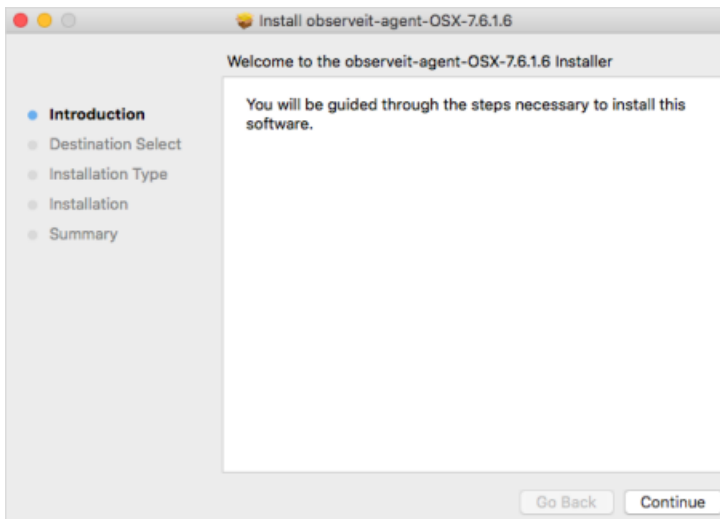
Note: Before installing a Window or Mac agent, you must download a JWT File that you will provide during the installation. This file can be downloaded from the **Configuration > Settings > Service Settings**.

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. Open the mounted **ObserveIT OSX agent** and then open the **remote** folder.

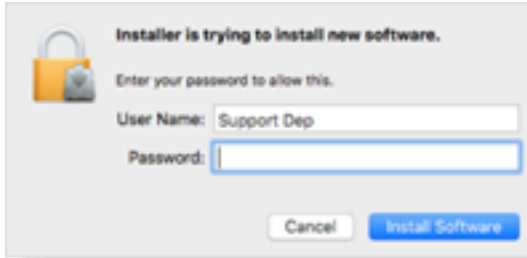


3. Run the observeit-agent-OSX-<version>.pkg package file.

The **ObserveIT Installer** opens.



4. Click **Continue**.
5. The ObserveIT Installer asks you for the **Installation location**.
Click **Install** to perform a standard installation on the disk "macintosh HD".
6. The ObserveIT Installer asks you for the **Password**. Enter your password and click **Install Software**.

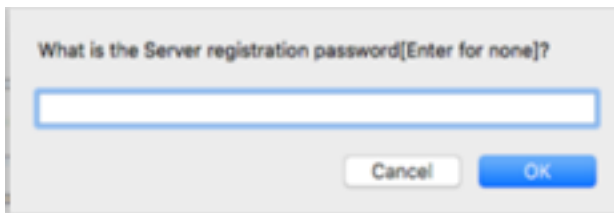


7. The ObserveIT Installer asks you for the **Server name or URL**. Enter the ObserveIT Application Server hostname or IP address.

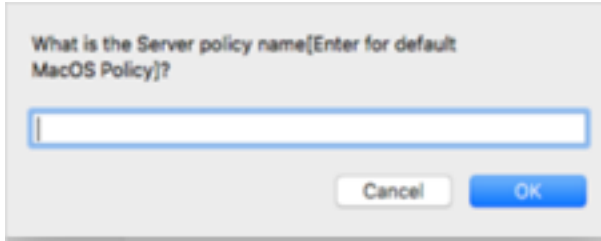


If the Agent is connected to the ObserveIT Application Server over SSL, first deploy the SSL certificate, and then in the registration address enter the Fully Qualified Domain Name (FQDN) in the format: `https://FQDN:PORT/observeitapplicationserver` (the default port for SSL is 443).

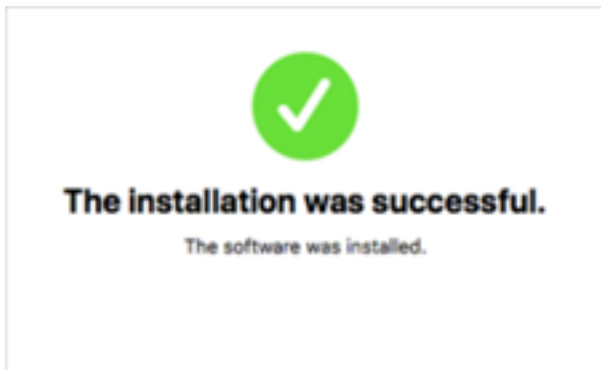
8. The ObserveIT Installer asks you for the **Server registration password** (optional). Click **OK** to skip or enter the Server registration password if required.



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. Access the ObserveIT Web console.

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.

The screenshot shows the observeIT Management Console interface. The top navigation bar includes 'observeIT INSIDER THREAT INTELLIGENCE MANAGEMENT CONSOLE' and a user profile 'Welcome, Admin | Sign Out'. Below this is a search bar and a notification: 'Your trial will expire in 29 days. Please contact us for pricing.' The main navigation menu contains: ENDPOINT DIARY, USER DIARY, FILE DIARY, EMAIL DIARY, DBA ACTIVITY, ALERTS, CONFIGURATION, SEARCH, and REPORTS. The 'Activities' section is active, displaying a filter panel with options for 'Period' (Last 1 Months, Between 08/15/2020 to 09/16/2020), 'Endpoint' (W19-S14-QA01, 10.2.0.64), and 'Filter by login/user' (All). A table of activities is shown below, with columns for Session Duration, Login, User, Endpoint Name, Client Name, Slides, and Video. The first row is highlighted, and red circles indicate the expand and video buttons.

Session Duration	Login	User	Endpoint Name	Client Name	Slides	Video
02:12 PM - 03:52 PM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	385	[Video]
01:36 PM - 02:12 PM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	112	[Video]
01:35 PM - 01:35 PM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	4	[Video]
01:32 PM - 01:35 PM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	13	[Video]
01:09 PM - 01:10 PM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	2	[Video]
12:34 PM - 12:40 PM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	11	[Video]
11:18 AM - 11:19 AM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	2	[Video]
11:17 AM - 11:18 AM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	5	[Video]
10:36 AM - 10:37 AM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	5	[Video]
09:34 AM - 10:20 AM	Administrator	n/a	W19-S14-QA01	OIT-INBAL-LAP	176	[Video]

2. Go ahead and familiarize yourself with the layout of the console and expand the recorded sessions by clicking  to make sure metadata is being collected. Then click on the video replay button  to verify session recording.