

observe it MANAGEMENT CONSOLE Welcome, Admin Sign out DER THREAT INTELLIGENCE iod: 5/12/18 12:00 AM - 6/11/18 6:45 Ab ISER ACTIVITY PROFILE WE A 100% 24 RISKY USERS
 1
 | SSMS

 3
 | Microsoft Management
 10 NEW LISERS AT RISK 1 | Adding group membership to Active Directory user Risk level: Critical High Medium RISKY USERS (4) All applications 1 10 1 of1 ◀ ▶ * User name All alerts Sort by: O User risk score B RISKY APPLICATIONS ALERTS TREND 42% Tor Browser \bigcirc 4 $_{-}$ | Running TOR browser, \bigcirc 4 $_{\rm I}$ Clearing browsing history in IE or Firefox 100 USR-00000102 21% Windows Explor ل 5 ا Opening ObserveIT Agent folder, ل 8 ا Accessing system folders 10% Windows PowerShe ⊈ 3 | Ru nning unauthorized command by non-adi () ALERTS RISKY APPLICATIONS 66% SSMS 🗘 8 🛛 Running database managen rkstation, ♀ 11 | Running DBA tools, ♀ 1 | Modify 85 USR-00000105 요 10 | Running Windows management tools, 유 1 | Adding Windows Firewall Rules 11% Microsoft Management Console 11% Windows Explorer △ 1 | Opening ObserveIT Agent folder, △ 3 | Accessing system folders, △ 1 | Installing software on Se RISKY APPLICATIONS ALERTS TREND 79 60% Microsoft Manager \bigcirc 3 $_$) Adding group membership to Active Directory user, \bigcirc 2) Adding r v. 🗘 2 i Running Act 33% Windows PowerShell nd line tools, 🗘 3 | Looking

> 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 selfguided 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	 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.





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
- ObservelT 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
- 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.

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

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



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:

📕 📝 📕 🖛			Application Tools	ObserveIT-NL_Set	up_v7.9.0.101_Trial		_	- 🗆	\times
File Home	Share	View	Manage					,	~ ?
$\leftarrow \rightarrow \checkmark \uparrow$	> Obs	serveIT-NL	_Setup_v7.9.0.101_	Trial > ObservelT-	NL_Setup_v7.9.0.101_Trial	~ Ū	Search Observel1	-NL_Setup_v	Q
			^						^
📌 Quick access		Name			2/8/2020 1:32 PM	Type File folder	Size		
- Desktop	*	DB	Analytics		4/8/2020 1:32 PM	File folder			
Downloads	*	Insi	der Threat Library		4/8/2020 1:32 PM	File folder			
	*	📕 Ma	c Agent		4/8/2020 1:32 PM	File folder			
Pictures	4	Scr	eenshotsStorageOp	otimizer	4/8/2020 1:32 PM	File folder			
i Fictures	~	📜 sqi	LEXPR_x64_ENU		4/8/2020 1:35 PM	File folder			
🧢 This PC		📕 Tria	Assistant		4/8/2020 1:36 PM	File folder			
Network		📜 Тур	icalInstall		4/8/2020 1:36 PM	File folder			
		📜 Uni	x-Linux Agent		4/8/2020 1:36 PM	File folder			
		📜 Util	ities		4/8/2020 1:36 PM	File folder			
		📜 We	b		4/8/2020 1:37 PM	File folder			
		📜 We	bsiteCat		4/8/2020 1:37 PM	File folder			
		📕 Wir	nAgent64bit		4/8/2020 1:37 PM	File folder			
		📕 Wir	nAgentUpdater32b	it	4/8/2020 1:37 PM	File folder			
		📕 Wir	nAgentUpdater64b	it	4/8/2020 1:37 PM	File folder			
		Ob:	servelTInstaller		4/8/2020 1:40 PM	Text Document	1 KB		
		🧿 OIT	Quick Start Guide	7.9.x	4/8/2020 1:32 PM	Chrome HTML Do	1,828 KB		
		📄 Rea	adme		4/8/2020 1:32 PM	Text Document	1 KB		
		🊯 Set	up		4/8/2020 1:32 PM	Application	598 KB		
		🗋 Set	up.exe.config		4/8/2020 1:32 PM	CONFIG File	1 KB		
		Sys	tem.Management.A	Automation.dll	4/8/2020 1:32 PM	Application extens	. 2,940 KB		
		🗟 Wp	fPageTransitions.dl	I	4/8/2020 1:32 PM	Application extens	. 16 KB		\sim
22 items 1 item s	elected	597 KB							

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 ObservelT windows agent for 64 bit systems
- OIT Quick Start Guide Contains system minimum requirements and helpful notes for the latest version
- ✓ **TypicalInstall** Folder with **ObservelT.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.

Nar	me		Date modifi	ed
	DB		4/8/2020 1:3	2 PM
	DB_Analytic	S	4/8/2020 1:3	2 PM
	Insider Threa	at Library	4/8/2020 1:3	2 PM
	Mac A	Open		2 PM
	Screer 🎈	Run as administrator		2 PM
	SQLEX	Troubleshoot compatibility		5 PM
	TrialAs 🖶	Scan with Windows Defender		6 PM
	Туріса —	Share with		6 PM
	Unix-L	Didle with		6 PM
	Utilitie	Restore previous versions		6 PM
	Web	Send to	>	7 PM
	Websit	Cut		7 PM
	WinAg	Сору		7 PM
	WinAg —			7 PM
	WinAg	Create shortcut		7 PM
	Observ	Delete		4 PM
9	OIT QL	Rename		2 PM
	Readn	Properties		2 PM
İţ	Setup		4/8/2020 1:3	2 PM

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".)



ObservelT Installer		×
observe IT a proofpoint company 15 day free trial	Thank you for trying ObserveIT	
	Checking for prerequisites:	
	✓ Hardware and Operating System	
	✓ IIS Installation	
	O SQL Server Installation	
	Please provide SQL Instance installation details:	
	SQL Instance: .\ SQLEXPRESS (2)	
	SQL User: sa 🕜	
	SQL Password: *******************	
	Repeat Password: ************************************	
Test Drive ObservelT		
Request a personalized demo	Back Exit	

If you receive the following message to install the **PreRequisite_nodeServices.exe**, select **Run**.

Open File	- Security War	ning	×
Do you	want to run tl	nis file?	
	Name: Publisher: Type: From:	up_v7.9.0.101_Trial\Web\PreRequisite_nodeServices.es ObserveIT Inc. Application C:\Users\User1\Desktop\ObserveIT-NL_Setup_v7.9.0.10 Run Cancel	«e
🗹 Alwa	ys ask before o	pening this file	
۲	While files fr harm your co <u>What's the ri</u>	om the Internet can be useful, this file type can potential omputer. Only run software from publishers you trust. <u>sk?</u>	ly

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 <u>licenses@observeit.com</u>) 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.

ObserveIT Installer		×
	ipany	
SQL Server		
Server	i.e. "localhost" or "MACHINE,1434" .\SQLEXPRESS	
Authentication	C Windows © SQL Server	
User	sa	
Password		
Web Console	ObservelT Application (part 499.4)	\ \
website	Observent Application (port 4884)	,
License		
• Full Installation	O Upgrade Obtain Trial Licen	se
Insert license:	C:\Users\User1\Desktop\ResellerLicense T Browse for License	e
Installation Log an	d Progress	
Current		
Total	Show Log	
Terms of Service	Aree Support Install Evit	
, , ,		



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 <u>oit-support@proofpoint.com</u>.

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.

observe <u>it</u>	- 1	
Website Categorization module d employees. It allows getting alert Adults, Infected/Malicious website	letects automatically the category of websi s upon browsing to specific categories suc es, Phishing websites and more.	tes browsed by h as Gaming,
Please note that this module requi categorization data and for gettin will be tested (displaying a succe	uires Internet access for the initial downloa g daily updates. The connectivity to the up ss/failure indication) during this installatior	d of the date service process.
For optimal performance, it is rec and not on a machine on which o	ommended to install this module on a sepa ther ObserveIT modules have been install	arate machine, ed.
For optimal performance, it is also at least 8GB memory (RAM).	o recommended to install this module on a	machine with
This machine is equipped with: 8	191MB RAM	
The update	service was accessed successfully.	



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.





After closing the installation window, the **ObserveIT web console** opens automatically. The login page appears. Login an and configure the initial admin password.

a proofpoint company
admin
Password
Confirm Password
Log In

Note: For information about configuration and other settings, see <u>ObserveIT</u> <u>Documentation</u>.



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.

	岁 ObserveIT Agent	x
	observe it	A
	Enter Application Server location	
	<u>Type:</u> <u>S</u> erver Name:	Port:
	http v win-mrktsrv2012	4884
		Test Connection
	Select setup type:	
	InstallShield < Back Next >	Cancel
ight © 2020 observe IT All rij	hts reserved.	



8	ObserveIT Agent x
observe	t
Enter Application Server	location
. 🚽	ObservelT Agent
Mtp://win-	mrktsrv2012:4884/ObserveITApplicationServer
Custom installation	n (Advanced options)
a stall Chield	
194019111210	< Back Next > Cancel

6. It is recommended to select the **Custom installation** radial box to get familiar with the custom settings then Click **Next**.

Enter Application	Server location	
<u>Type</u> :	Server Name:	Port:
http 🗸	win-mrktsrv2012	4884
		Test Connection
-Select setup typ	e:	
O Default inst	allation (Recommended)	
 Custom inst 	allation (Advanced options)	



 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.

ы́	ObserveIT Agent	x		
observe <mark>i</mark> t		-		
Install the ObserveIT Agent to:	eIT\ObserveITAgent\	Change		
Agent registration mode:	Registered	~		
Recording policy:	Default Windows-based Policy	~		
Language:	English	¥		
Hide the ObserveIT Agent from Add/Remove Programs				
InstallShield				
	< Back Next >	Cancel		

8. Make note of the settings and click Install.

9	ObserveIT Agent X
observe <mark>i</mark>	t
Click Install to begin the	e installation.
If you want to review of exit the installation.	or change any of your installation settings, click Back. Click Cancel to
Current Settings:	
Destination folder:	C:\Program Files\ObserveIT\ObserveITAgent\
Application Server URL	: http://win-mrktsrv2012:4884/ObserveITApplicationServer
Registration mode:	Registered
Recording policy:	Default Windows-based Policy
Language:	English
nstallShield	
	< Back Install Cancel



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).

📙 📝 📙 🗢 Unix-Linux Agent					
File Home Share View					
← → ✓ ↑ → ObservelT_Setup_v7.6.2.5 → Unix-Linux Agent					
- Ouisk second	Name	Date modified	Туре	Size	
	observeit-agent-aix6-7-7.6.2.3.run	11/19/2018 10:29	RUN File	6,362 KB	
	observeit-agent-AMZNLNX-7.6.2.3.run	11/19/2018 10:29	RUN File	2,497 KB	
Uownloads	observeit-agent-Debian-6-32-7.6.2.3.run	11/19/2018 10:29	RUN File	3,492 KB	

- 2. Log in to the target server with root permissions; or, alternatively, use the *sudo* command.
- 3. Run the **Is** –**I** 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 selfextracting 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</u> <u>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.



	🥪 Install observeit-agent-OSX-7.6.1.6		
	Welcome to the observeit-agent-OSX-7.6.1.6 Installer		
 Introduction Destination Select Installation Type Installation Summary 	You will be guided through the steps necessary to install this software.		

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.

\cap	Installer is t	rying to install new software.		
	Enter your password to allow this.			
	User Name:	Support Dep		
	Password:			
		Cancel Install Software		

7. The ObserveIT Installer then asks you for the Server Name or URL.

Enter the ObserveIT Application Server hostname or IP address.

What is the Server name or URL?			
	Cancel	ок	

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.

What is the Server registration password[Enter for none]?		
	Cancel	ОК

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.

What is the Server policy nam MacOS Policy]?	e[Enter for default	
[
	Cancel	ОК

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: <u>Https://<Server_Name_FQDN>/ObserveIT</u>

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.



observe <u>it</u>	ISIDER THREAT INTELLIGENCE MANAG	EMENT CONSOLE	Welcome, Admin Sign Out
📲 Admin Dashboard 🛛 6 🕭			Your trial will expire in 364 days. Please contact us for pricing.
ENDPOINT DIARY USER DIARY	FILE DIARY DBA ACTIVITY	ALERTS CONFIGURATION SEAF	ICH REPORTS
Activities	Activities		
Applications Messages	Period: Endoplat:	onths Between 12/02/2018 To: 0 To: 0	1/02/2019 🖶 Print
	Filter by login/user: All	T THE STREET ALTER AND A LEG	Change Descat
	1-12 of 12 20 💌 Items per page		31000 10363
	Session Duration Login	User Endpoint Name	IP Client Name IP Slides Video
	1/2/2019	n/a 🗯 nirs-mbp	console 346
Latest Sessions	 10:26 AM - 11:12 AM nirbarak 	n/a 🗯 nirs-mbp	console 86 K
nirs-mbp nirbarak	 09:32 AM - 09:43 AM nirbarak 	n/a 💼 nirs-mbp	console 79
W12-S12-D Administrator	 08:50 AM - 09:08 AM nirbarak 	n/a 🗯 nirs-mbp	console 168 🖿

Go ahead and familiarze yourself with the layout of the console and expand the recorded sessions by clicking the store store store store store store and expand the recorded sessions by clicking the store st

	Session Duration	Login	User	Endpoint Name 📃 IP	Client Name 🔜 IP	Slides	Video
3/	5/2018						
ŝ	09:35 AM - 09:35 AM	Sean.Keane	n/a	WIN-DSK-POC-10	(local)	8	e 6
				Bbb 月	Comment 🗐 Print summar	v 🕺 Printa	activity
USE	R ACTIVITY (WINDOW TITLES)						
	Application/Website		Activity Details				
	Windows Explorer		OpeDrive				
	Windows Explorer		Onebrive				
			Program Manager				►
	Search and Cortana applicat	ion	Cortana				Þ



	ObservelT Session Player - Google Chrome	_ D X
ttps://oit_testlab01.test.lab/ObserveIT/	SlideViewer.aspx?SessionID=123472cb-394b-4297-a7a3-4c47400d509e&partial=0	&SSID=68a768be-063d-448c-bc13-f6fb4b5d7abd⟨=en
BeservelT - Login Page ×	alT/FormLoginAuth.scnv2llcarDafaultDaga=True	·····································
 C Butteps//on_testiabolitestiab/Observi 	en/PolimboginAdutaspx: oserbeladutrage= inde	= \v
	observe it	
	admin	
	Password 🚯	
	Confirm Password	
	Log In	
	✿ 2016 Observe⊞ (Web Version 6.6.2.55)	
		• 阳 旧 佔 ^{822 PM} 9/14/2016
veIT - Login Page - Google Chrome (1/1)		8:23:27 PM (4/4)
convo it		
	Sheer Charles and the sheer sheer	

Now you're done!

Documentation Feedback

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

ObservelT documentation

ObserveIT is engaged in a continuous effort to improve our documentation. Please help us by sending your comments to: <u>SE@observeit.com.</u>

Copyright

Copyright * 2020, ObserveIT Inc. All rights reserved.

The information in this document is subject to change without notice. No part of this document may be reproduced, stored or transmitted in any form or by any means, electronic or mechanical, for any purpose without the express written permission of:

ObserveIT Inc.



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.