ObserveIT Custom Installation

In a custom installation, each of the ObserveIT components can be installed separately and you can distribute the components and use advanced configuration options as needed. This is the most common type of installation.

Custom Installation is often used in environments with higher security procedures, requiring each component of the ObserveIT product to be installed separately and using dedicated service accounts; or in large-scale environments requiring custom modifications of some of the server-side components.

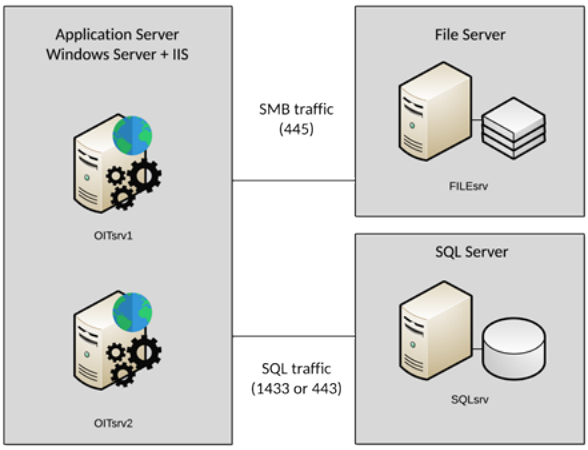
Active Directory Domain membership is not mandatory, although ideally all components should be placed on domain members. This enables usage of AD groups for Console Users; filtering of AD groups for Privileged Identity Management; DNS integration for Agent auto-configuration; and GPO-based installation.

Assumptions

This section describes the assumptions for examples included in the Custom Installation steps.

SYSTEM REQUIREMENT ASSUMPTIONS

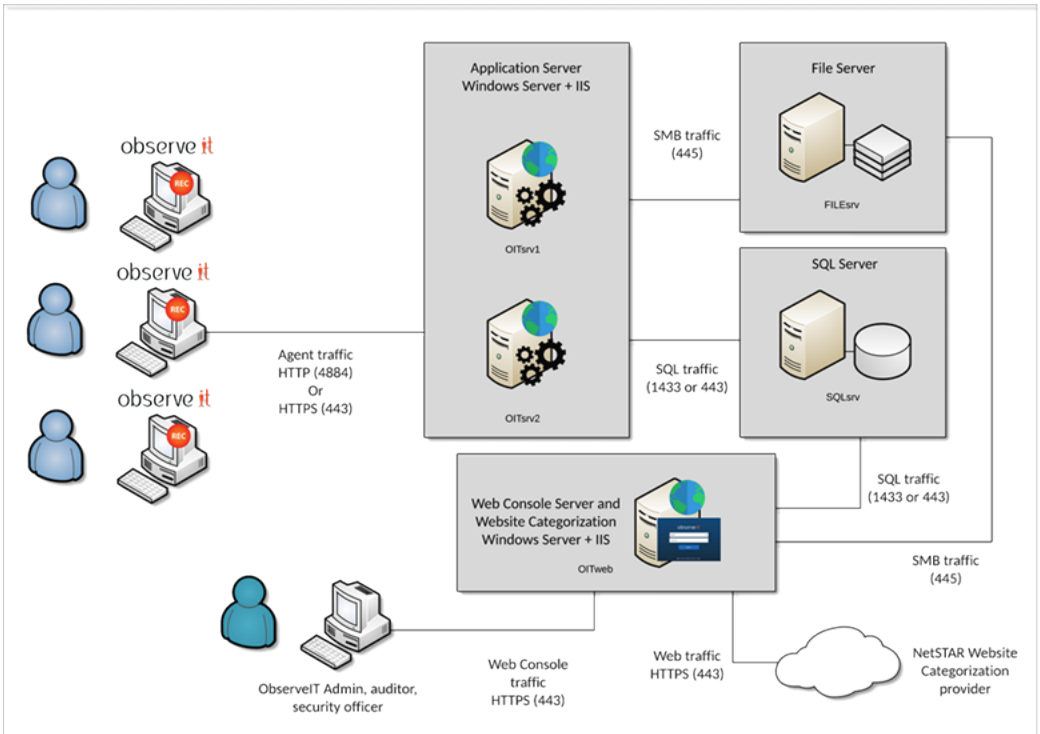
The diagram below shows the system requirements for the Custom Installation that is described in this documentation.



In the Custom Installation examples in the documentation, the following is assumed.

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

The diagram below is an example If you use a more complex installation.



The following is assumed:

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

SYSTEM PREREQUISITES ASSUMPTIONS

For the system requirements in a custom installation, the following is required:

- All computers must be members of the same Active Directory domain
- Logon permissions to the computers must be defined with administrative permissions (local administrator)
- Permissions to create a service account user in Active Directory

You must prepare the following in a custom installation:

- Permissions to access the SQL Server database engine (SYSADMIN permissions)
- Permissions to grant the service account DBCREATOR permissions on the SQL Server
- Permissions to create folder(s) and share(s) on the server acting as the file server
- Permissions to grant the service account MODIFY permissions on the file share(s)
- Full network connectivity with no firewall restrictions between the components of the deployment, or permissions to create the appropriate firewall rules to allow the requested traffic type
- For data encryption (data in transit, data at rest, Web Console traffic):
- An internal Certificate Authority (CA) capable of issuing the correct digital certificates (it is possible to use self-signed certificates, however that may add complexity to the deployment)
- For detailed instructions, hardware recommendations and sizing refer to the ObserveIT General Prerequisites and Recommendations document which can be obtained by contacting ObserveIT's professional Services team at proserv@observeit.com.

ADDITIONAL ASSUMPTIONS FOR CUSTOM INSTALLATION

The server hosting the ObserveIT server-side website application is a member of an Active Directory domain, but not a domain controller (DC). Hosting IIS on a domain controller may cause adverse security issues and should be avoided. However, it may be possible when installing in an isolated lab environment. When installing on a DC, you need to use the "Active Directory Users and Computers" MMC snap-in and add the ObserveIT service account to the "Administrators" group found in the "Builtin" container, but this will affect all the DCs in the domain.

The reader has prior knowledge of Public Key Infrastructure (PKI) and its related terminology.

Your organization has an SQL server administrator who follows best practices for deploying and maintaining SQL server.

Your organization has a backup administrator, who follows best practices for backing up databases, Operating Systems, and file shares.

Table of Contents

ObserveIT Custom Installation 1
Assumptions 2
System Requirement Assumptions 2
System Prerequisites Assumptions 4
Additional Assumptions for Custom Installation 4
Downloading the Latest Version 9
Custom Installation Steps 11
Preparing the Environment 13
Formatting a Disk for Graphic Images Storage and the Database 13
Storage Types 13
Format the Disk Using Computer Management 14
Validating Compression and Indexing Settings 17
Creating and Sharing the Graphics Image Folders 18
Installing Prerequisites for a Custom Installation 19
Configuring Windows Firewall 20
Configuring Windows Firewall on SQL server 20
Configuring Windows Firewall on ObserveIT Application Server 21
Preparing Permissions 21
Creating a Service Account User in Active Directory 22
Assigning SQL Permissions to the Service Account User 22
Adding the Service Account User to the Local Administrators Group 25
Adding the Service Account User to the Local IIS_IUSRS Group 27
Installing and Configuring Databases 29
Configuring Location for Recorded Screenshots 30
Installing the ObserveIT Databases 31

Installing the Databases 31
Installing the Analytics Database 33
Verifying Database Installation 34
Moving Database File to Drives 35
Installing Database Maintenance 41
Configuring Microsoft Internet Information Server (IIS) 43
Obtaining a Digital Certificate 44
Digital Certificate Source 44
Assigning a Digital Certificate 47
Using Microsoft Management Console 47
Using Internet Information Services (IIS) Manager 50
Creating a New Application Pool in IIS 8.X 51
Creating a New Website in IIS 8.X for the ObserveIT Application Server 56
Creating a New Website in IIS 8.X for the ObserveIT Web Console 58
Installing ObserveIT Components 60
Installing ObserveIT Application Server 60
Verifying Application Server Installation 62
Installing Additional ObserveIT Application Servers 63
Load Balancing 63
Installing ObserveIT Web Management Console 63
Installing the SQL Native Client 66
Verifying the Web Management Console installation 67
Obtaining a Commercial License 67
Installing the Screenshots Storage Optimizer 72
Screenshot Storage Optimizer Wizard 73
Installing the Website Categorization Module 75

Website Categorization Prerequisites 76
Installing the Website Categorization Module 76
Installing the module using a Custom installation 76
Configuring Internet proxy settings for Website Categorization module 85
Verifying the ObserveIT Services Identity 86
Configuring ObserveIT Installation 88
Configuring the Admin Password 88
Configuring LDAP Settings 89
Configuring SMTP Settings 90
Configuring Screen Capture Data Storage 91
Configuring Traffic Security 93
Requirements 93
Configuring ObserveIT Application Server for Data Transit Encryption 94
Configuring Windows Agents to Use SSL 94
New ObserveIT Agent Deployment 95
Existing ObserveIT Agent Deployment 95
Configuring a Mac Agent to use SSL 96
Obtaining and Importing a Certificate 96
Copy the Certificate to your Mac 99
Configuring a Unix Linux Agent to Use SSL 101
Obtain and Import a Trusted Internal CA Certificate 101
Copy the Certificates to a Linux Server 104
Configuring Simple Recovery Mode 105
Configuring Simple Recovery Model for the ObserveIT Databases on the SQL Server 105
Configuring Simple Recovery Model for the ObserveIT Databases via SQL Query 106
Formatting NTFS 107

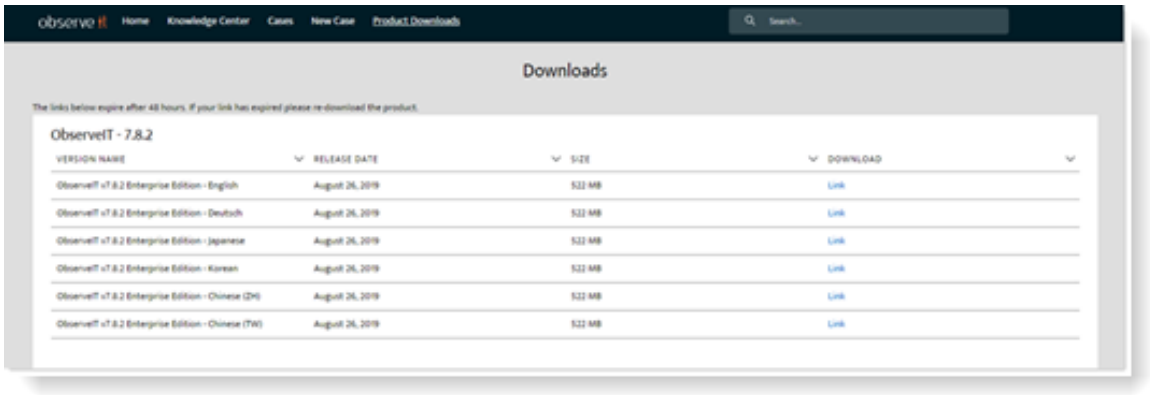
Using PowerShell 109
Running Elevated Windows PowerShell Prompt as a Different User 109

Downloading the Latest Version

When you're ready to install or update to a new version, you can download the files you need. Files are located in the **Downloads** page of the ObserveIT Support Portal.

> You need a username and password.

1. Download the files you need from here.
2. Log in and from the **Downloads** page, click the **Link** you want.



3. Save the file to `C:\Temp` on the ObserveIT Application server.
4. Extract the content of the **ZIP** file.

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
- 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: Contains **ObserveIT.Installer.exe**, a self-contained one-click ObserveIT installer
- WinAgentUpdater32bit: Contains the Updater **It.Updater(x86).msi** installer for Windows 32 bit. You must install the Updated the first time you use it.
- WinAgentUpdater64bit: Contains the Updater **It.Updater(x64).msi** installer for Windows 64 bit. You must install the Updated the first time you use it.

Custom Installation Steps

Follow these steps to complete the installation process.

Before you begin, make sure you have completed Prerequisites for Custom Installation.

1. Preparing the Environment
    1. Formatting a Disk for Graphic Images Storage and the Database
    2. Creating and Sharing the Graphics Image Folders
    3. Installing Prerequisites for a Custom Installation
    4. Configuring Windows Firewall
2. Preparing Permissions
    1. Creating a Service Account User in Active Directory
    2. Assigning SQL Permissions to the Service Account User
    3. Adding the Service Account User to the Local Administrators Group
    4. Adding the Service Account User to the Local IIS_IUSRS Group
3. Installing and Configuring Databases
    1. Configuring Location for Recorded Screenshots
    2. Installing the ObserveIT Databases
    3. Verifying Database Installation
    4. Moving Database File to Drives
    5. Setting Initial Database File Sizes
    6. Installing Database Maintenance
4. Configuring Microsoft Internet Information Server (IIS)
    1. Obtaining a Digital Certificate
    2. Assigning a Digital Certificate
    3. Creating a New Application Pool in IIS 8.X
    4. Creating a New Website in IIS 8.X for the Application Server
    5. Creating a New Website in IIS 8.X for the Web Console
5. Installing ObserveIT Components
    1. Installing ObserveIT Application Server
    2. Installing ObserveIT Web Management Console
    3. Obtaining a Commercial License
    4. Installing the Screenshots Storage Optimizer
    5. Installing the Website Categorization Module
    6. Verifying the ObserveIT Services Identity
6. Configuring ObserveIT Installation
    1. Configuring the Admin Password
    2. Configuring LDAP Settings

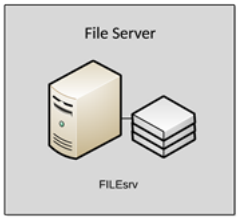
3. Configuring SMTP Settings
4. Configuring Screen Capture Data Storage

7. Configuring Traffic Security
    1. Configuring ObserveIT Application Server for Data Transit Encryption
    2. Configuring Windows Agents to Use SSL
    3. Configuring a Mac Agent to use SSL
    4. Configuring a Unix Linux Agent to Use SSL
    5. Configuring Screen Capture Data Storage
8. Installing ObserveIT Agents
    1. Windows Agent Deployment
    2. macOS Agent Deployment
    3. Unix/Linux Deployment

Preparing the Environment

Custom Installation is often used in environments with higher security procedures, requiring each component of the ObserveIT product to be installed separately and using dedicated service accounts; or in large-scale environments requiring custom modifications of some of the server-side components.

The diagram below shows an example of a file server. This is where the configuration starts.



The following tasks describes how to prepare your Windows Server machines for ObserveIT installation.

- Formatting a Disk for Graphic Images Storage and the Database
- Creating and Sharing the Graphics Image Folders
- Installing Prerequisites
- Configuring Windows Firewall

FORMATTING A DISK FOR GRAPHIC IMAGES STORAGE AND THE DATABASE

Screen capture data is configured separately.

As a matter of best practice, for medium to large scale deployments, ObserveIT recorded images are stored on a file share server in the network. Configuring all recorded graphic screenshots to be stored in the file system network share (a UNC path) instead of in the SQL database reduces the overall I/O overhead on the SQL Server.

This section describes how to configure the disks before creating the file share.

For information about creating the file share, see **Creating and Sharing the Graphics Image Folders**.

By default, all the recorded graphic screenshots are stored in the **ObserveIT_Data** database.

If using a file share, it is highly recommended to use a Windows Server 2016 machine with appropriate disk capacity, where the disk drive(s) are connected either locally, or on a storage device such as SAN/NAS using either iSCSI or Fiber Channel (FC). Where this is not possible, use virtual disks that are stored on the fastest and most optimized storage array for write IOPS.

Storage Types

There are a total of 3 types of storage you can use for recording screenshot data:

- **Hot storage**: Recording screenshot data is written immediately after being received from a remote ObserveIT Agent. Because all the graphic images stored on the hot storage are typically small, the disk needs to be formatted with NTFS file system for Windows Server 2016 using the allocation unit size of 4KB (4096K). This ensures best disk location usage and reduce disk space waste.
- **Warm storage**: Recording screenshot data is stored after an active ObserveIT session is closed. The recording screenshot data stored on the warm and archive storage is stored in a ZIP format, with each ZIP file containing all images for a single ObserveIT session. To optimize performance, format the warm and archive storage with 64KB block size. This configuration can be done using Disk Management or the DISKPART command line utility.
- **Archive storage**: Recording screenshot data is moved during an archive operation.

Do not enable disk compression.

Format the Disk Using Computer Management

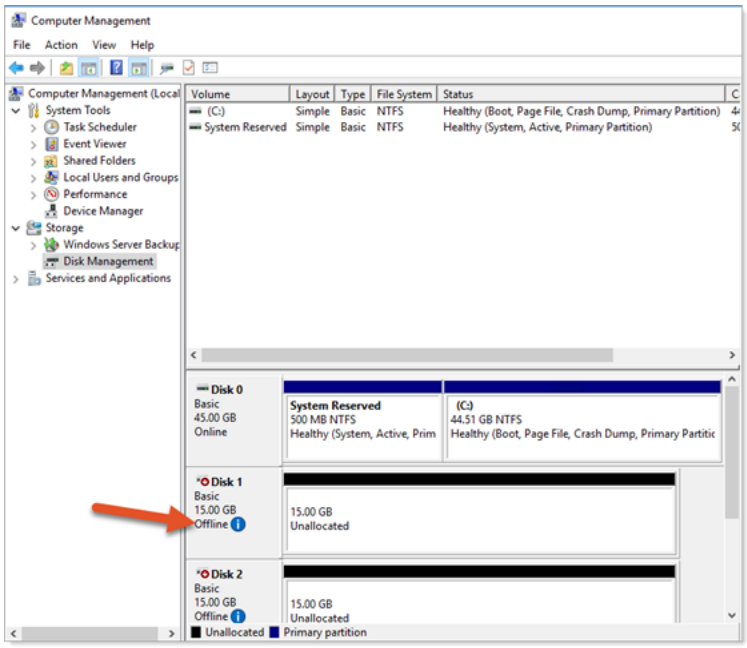
This example assumes the file share is to be located on a Windows Server 2016 Operating System and describes the procedure to configure the disks (and later – the file share) on this Operating System.

In this example, assume the new disk has just been connected to the machine, but no further action was taken.

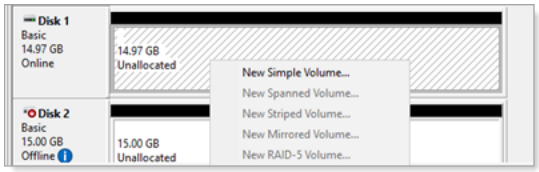
1. Connect to the computer acting as the ObserveIT file share.
2. From **Start**, type **Computer Management**.

   The **Computer Management** window opens.
3. Expand **Computer Management (Local)**, expand **Storage**, and click **Disk Management**.

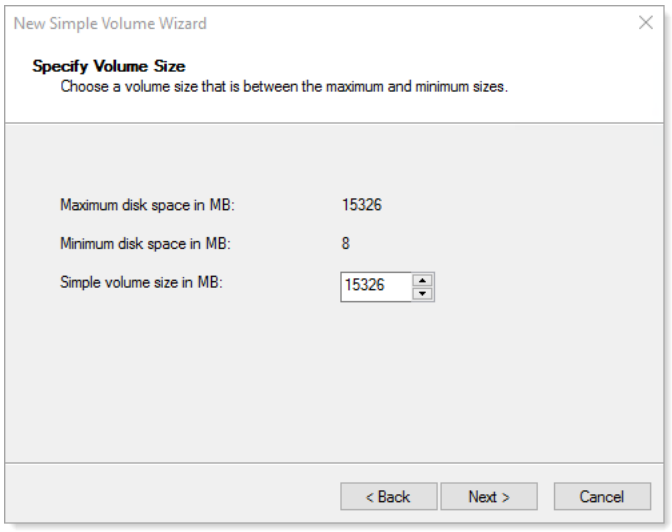
   The list of disks appears.
4. Find the new disk in the list. Usually, it is the only one with the status **Offline**.



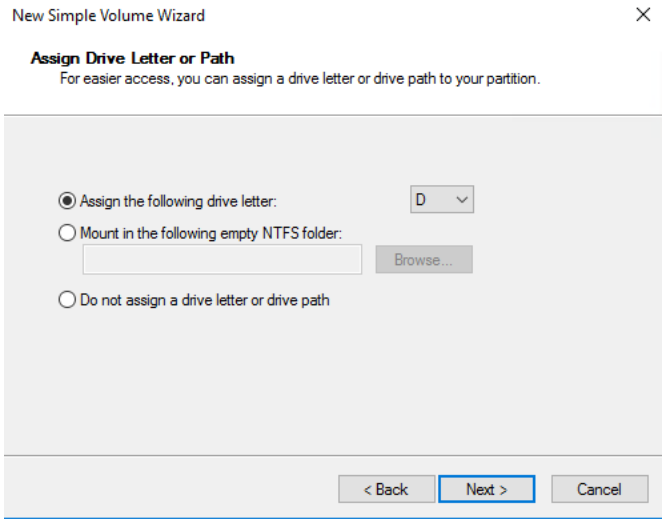
5. Right-click the disk and select **Online**.
6. Right-click the disk again and select **Initialize Disk**.
7. Click the **GPT (GUID Partition Table)** radio button and click **OK**.
8. Right-click the partition and select **New Simple Volume**.



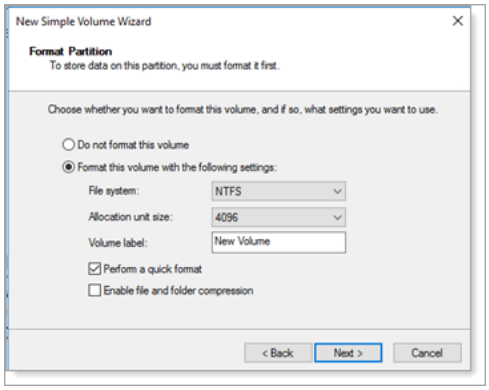
9. The Wizard opens, click **Next**.



10. Make sure maximum the values specified in the Maximum disk space in MB and Simple volume size in MB are equal. Click **Next**.



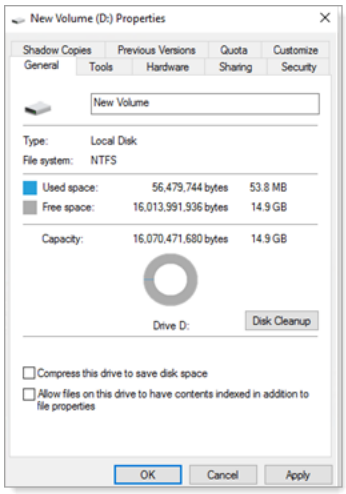
11. Assign an appropriate drive letter. Click **Next**.



12. Click the **Format this volume with the following settings** radio button and select **NTFS**.
13. Set the **Allocation unit size**:
    - 4096 for the hot storage.
    - 64KB for the warm and archive storage.
    - 64KB for SQL database.
14. Assign an appropriate volume label at the **Volume label** field.
15. Make sure **Perform a quick format** checkbox is checked.
16. Click **Next** and review the settings. Click **Finish**.
17. The disk is formatted and you are returned to the **Computer Management** window.

Validating Compression and Indexing Settings

1. From the **Computer Management** window, expand the **Computer Management (Local)** node, expand the **Storage** node, and click the **Disk Management** node.
2. In the main window, locate the volume designated for the ObserveIT screenshot data.
3. Right-click the volume and choose **Properties** from the menu.
4. Make sure the **Allow files on this drive to have contents indexed in addition to file properties** check box is unchecked.



5. Click **OK**.

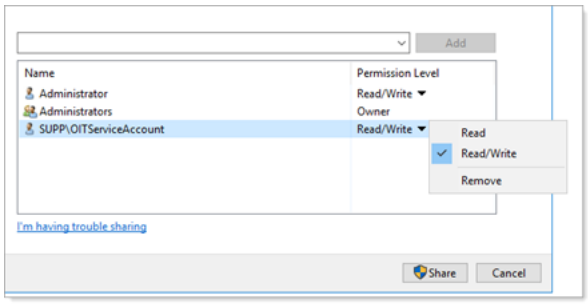
CREATING AND SHARING THE GRAPHICS IMAGE FOLDERS

This topic describes how to create a file share so you can share folders on a Windows Server file server.

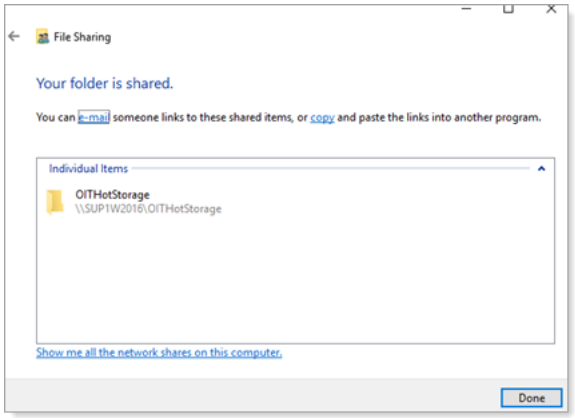
If you want to use Network Access Storage (NAS) or a different storage type, see your storage vendor documentation.

1. Connect to the computer acting as the ObserveIT file share.
2. Open Windows File Explorer. (You can open the **Start** menu and type in **explorer**, then Enter.)
3. In Windows **File Explorer**, navigate to a disk where the ObserveIT image store folder is to be located.
4. Create a new folder. (Click **New** and then **Folder**) and right-click some empty space inside the **File Explorer** window).
5. Give the folder an appropriate name, for example: **OITHotStorage**.
6. Right-click the folder, click **Share With**, and click **Specific people**.
7. Type in the account name, for example **OITServiceAccount** and click **Add**.

   The new account is added.
8. Select the account and set the Permission Level. Choose **Read/Write**. Click **Share**.



9. Your folder is shared.



10. Create folders for the ObserveIT Archive folder, for example: OITWarmStorage and OITArchive by repeating the previous steps.

    Make a note to remember the paths to the current shares. You'll need them later.

    For example:

    ```
    \\filesrv\OITData\OITHotStorage
    ```

    ```
    \\filesrv\OITData\OITWarmStorage
    ```

    ```
    \\filesrv\OITData\OITArchive
    ```

INSTALLING PREREQUISITES FOR A CUSTOM INSTALLATION

ObserveIT Application Server and ObserveIT Web Console require several prerequisites, such as Microsoft Internet Information Services and the .Net Framework. You can install these automatically using Power-Shell.

1. Mount a Windows Server 2016 installation DVD to the virtual machine or insert a Windows Server 2016 DVD into the DVD drive of the server.

   In this example, Windows Server 2016. You can install with Windows Server 2019.

   The following steps are similar for Windows Server 2012/2012R2 Operating Systems. If using one of these systems, mount or insert the appropriate DVD to the machine.

2. Open the **Start** menu and type in **PowerShell**.
3. Right-click the **PowerShell** shortcut and choose **Run as administrator**.
4. If prompted, **Do you want to allow this app to make changes to your device?** Click **Yes**.
5. Copy and paste the following 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-Ext45, Web-Asp, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Mgmt-Tools, Web-Mgmt-Console, NET-WCF-Services45, NET-WCF-HTTP-Activation45, NET-Framework-45-Core, NET-Framework-45-Features, NET-Framework-45-ASPNET
```

CONFIGURING WINDOWS FIREWALL

When Windows Firewall is enabled, you need to configure the Windows Firewall on the SQL server and the ObserveIT Application server.

Configuring Windows Firewall on SQL server

In this example, it is assumed that all default ports are used.

1. From the Windows **Run** window, open **PowerShell**.

   Make sure you are running **PowerShell** as an administrator.

2. If prompted **Do you want to allow this app to make changes to your device?**, click **Yes**.
3. Copy and paste the following code into the PowerShell window:

```
New-NetFirewallRule -DisplayName "SQL Server" -Direction Inbound
-Protocol TCP -LocalPort 1433 -Action allow

New-NetFirewallRule -DisplayName "SQL Admin Connection" -
Direction Inbound -Protocol TCP -LocalPort 1434 -Action allow

New-NetFirewallRule -DisplayName "SQL Database Management" -
Direction Inbound -Protocol UDP -LocalPort 1434 -Action allow

New-NetFirewallRule -DisplayName "SQL Debugger/RPC" -Direction
Inbound -Protocol TCP -LocalPort 135 -Action allow
```

4. Close the PowerShell window.

Configuring Windows Firewall on ObserveIT Application Server

In this example, it is assumed that all default ports are used.

1. From the Windows Run window open PowerShell.

   Make sure you are running PowerShell as an administrator.

2. If prompted Do you want to allow this app to make changes to your device?, click Yes.

3. Copy and paste the following code into the PowerShell window:

   ```
   New-NetFirewallRule -DisplayName "HTTPS" -Direction Inbound -
   Protocol TCP -LocalPort 443 -Action allow
   ```

4. Close the PowerShell window.

Preparing Permissions

In a custom installation, make sure the following permissions are configured:

- Permissions to create a service account user in Active Directory
- Permissions to grant the service account DBCREATOR permissions on the SQL Server
- Permissions to access the SQL Server database engine (SYSADMIN permissions)
- Logon permissions to computers, with administrative permissions (local administrator)

CREATING A SERVICE ACCOUNT USER IN ACTIVE DIRECTORY

This topic describes how to configure permissions to create a service account user in Active Directory. Active Directory is used connect to ObserveIT databases and to run ObserveIT services.

Permissions are required to set up a an Active Directory. For more information about this, contact the Active Directory team.

1. Connect to a Domain Controller or to a computer with Active Directory Remote Server Administration Tools installed.
2. Click **Start** and type `dsa.msc` and **Enter**.
3. Navigate to the **Organizational Unit** where the ObserveIT Service Account will be located.
4. Right-click the **Organizational Unit**, select**New** > **User**.

   Optional: Type **ObserveIT** into the **First Name** field and **Service Account** into the **Last Name** field.
5. Type **OITServiceAccount** into the **User logon name** field and choose the appropriate UPN suffix. Click **Next**.
6. Configure a password based on your organization's password policy requirements, uncheck the **User must change password at next logon** checkbox, and check the **Password never expires** checkbox. Click **Next**. Click **Finish**.
7. Close the **Active Directory Users and Computers** window.

ASSIGNING SQL PERMISSIONS TO THE SERVICE ACCOUNT USER

This procedure describes how to configure permissions to access the SQL Server database engine (SYSADMIN permissions) and grant the ObserveIT Server Account user the **dbcreater** role on the SQL server.

Use the following steps to grant the ObserveIT Service Account user the dbcreator role on the SQL server. This permission is required only during the installation phase and may be removed when the installation is complete. Removing this permission will prevent ObserveIT from creating additional archive databases with the service account and will require appropriate credentials when creating a new archive.

1. Connect to the SQL server or to a computer with SQL Server Management Studio installed.
2. Open SQL Server Management Studio, type the SQL server's FQDN or IP address in the **Server name** field and click **Connect**.

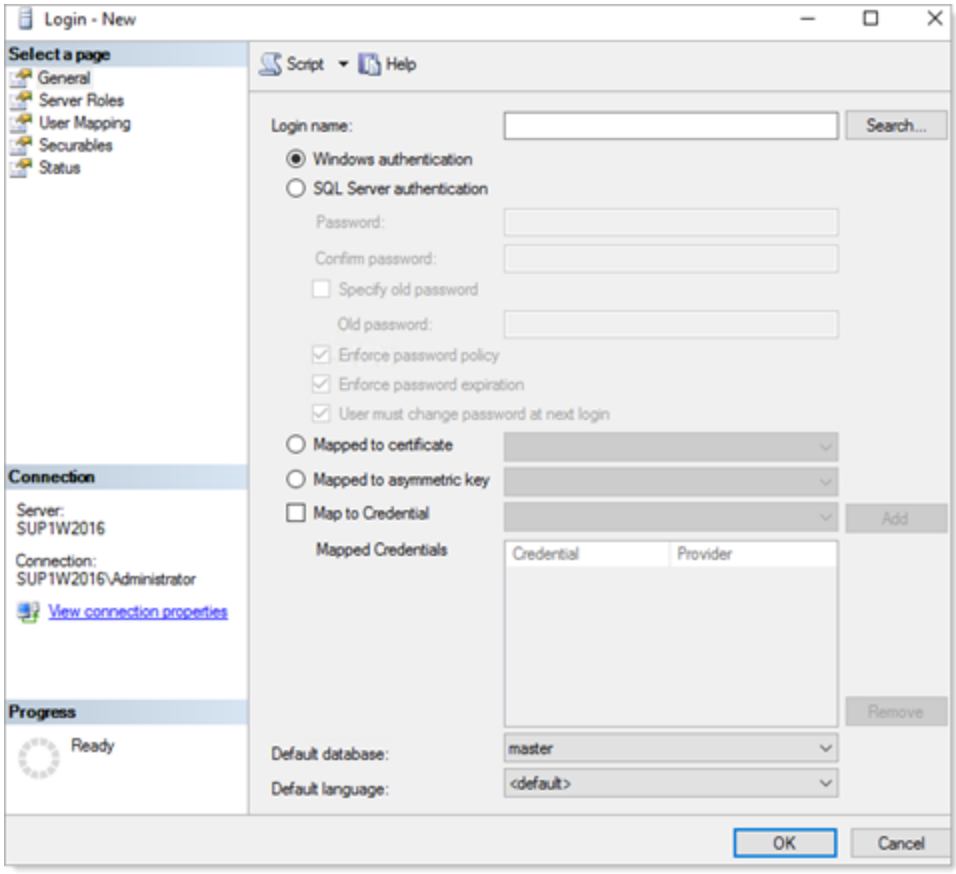
3. Select the authentication.

   Choose **Windows Authentication** if your account has sysadmin permissions on the SQL server.

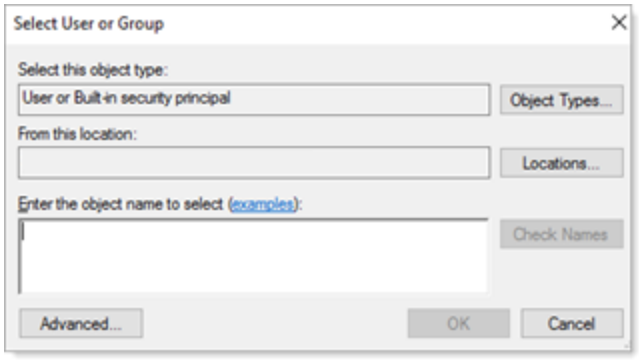
   Otherwise, choose **SQL Server Authentication** and log in with a sysadmin-level account. Click **OK** to connect.

4. From the menu on the left, expand **Security** right-click **Logins** and select **New Login**.

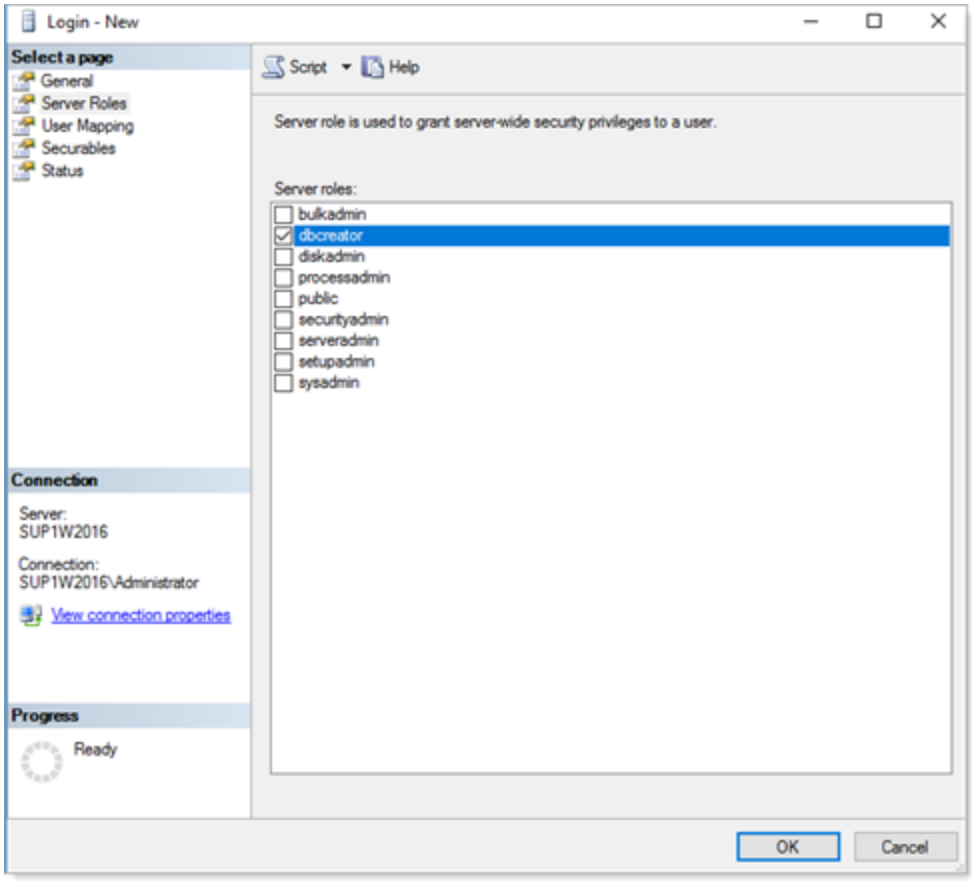
   The **Login** screen opens.



5. Click **Search**.



6. Click **Locations** and choose the location where the ObserveIT Service Account is located. Click **OK**.
7. In **Enter the object name to select** area, type the username for the ObserveIT Service Account user account, for example, **OITServiceAccount**. Click **OK**.
8. In the **Login** screen from the menu on the left, select **Select a Page** > **Server Roles**.



9. Select **dbcreator** and click **OK**.
10. Close the SQL Management Server Studio.

ADDING THE SERVICE ACCOUNT USER TO THE LOCAL ADMINISTRATORS GROUP

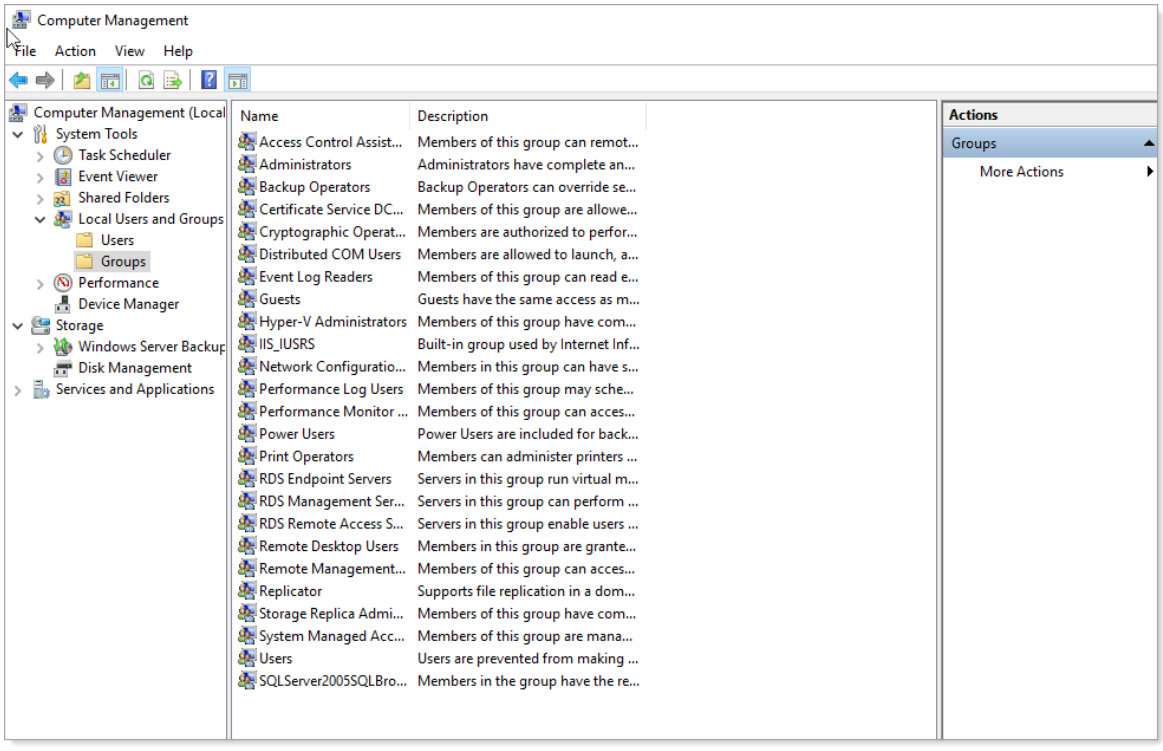
This topic describes how to addd the ObserveIT service account user to the local Administrators group on the ObserveIT Application Server(s) (and Web Console machine if installed on a separate computer).

> This is only required during the installation phase; the Service Account can be removed as soon as the installation has completed successfully.

1. On the ObserveIT Application Server, from **Start**, type **Computer Management**.

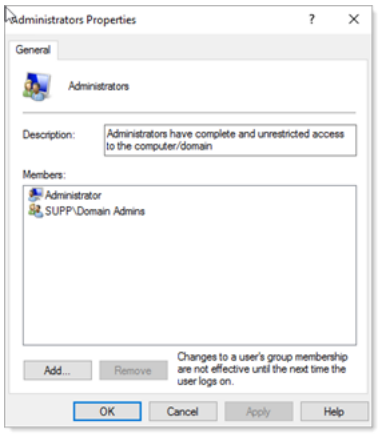
   The **Computer Management** window opens.

2. Expand **System Tools** and click **Local Users and Groups**. Expand **Groups** folder.



3. From the list of Groups, double-click **Administrators** group.

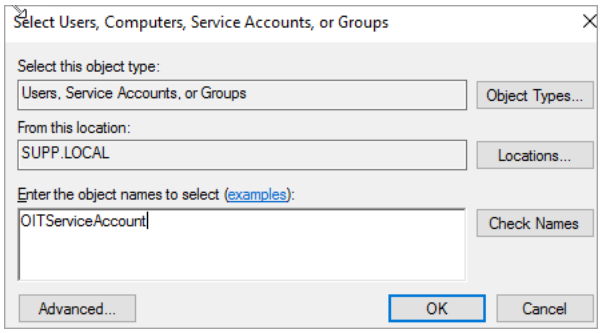
   The **Administrator Properties** dialog box opens.



4. Click **Add**.

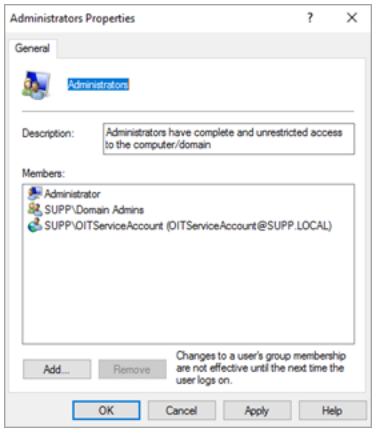
   The **Select Users, Computers, Service Accounts, or Groups** dialog box opens.

5. In the **Enter the object name to select** area, for example, **OITServiceAccount**.



6. Click **OK**.

   The **Administrator Properties** dialog box opens and **OITServiceAccount** appears in the **Members** list.



7. Click **OK**.

8. If you plan to deploy more than one ObserveIT Application Server, or if you plan to install the ObserveIT Web Console on a separate machine, repeat on all the computers that will host the ObserveIT Application and Web Console applications.

ADDING THE SERVICE ACCOUNT USER TO THE LOCAL IIS_IUSRS GROUP

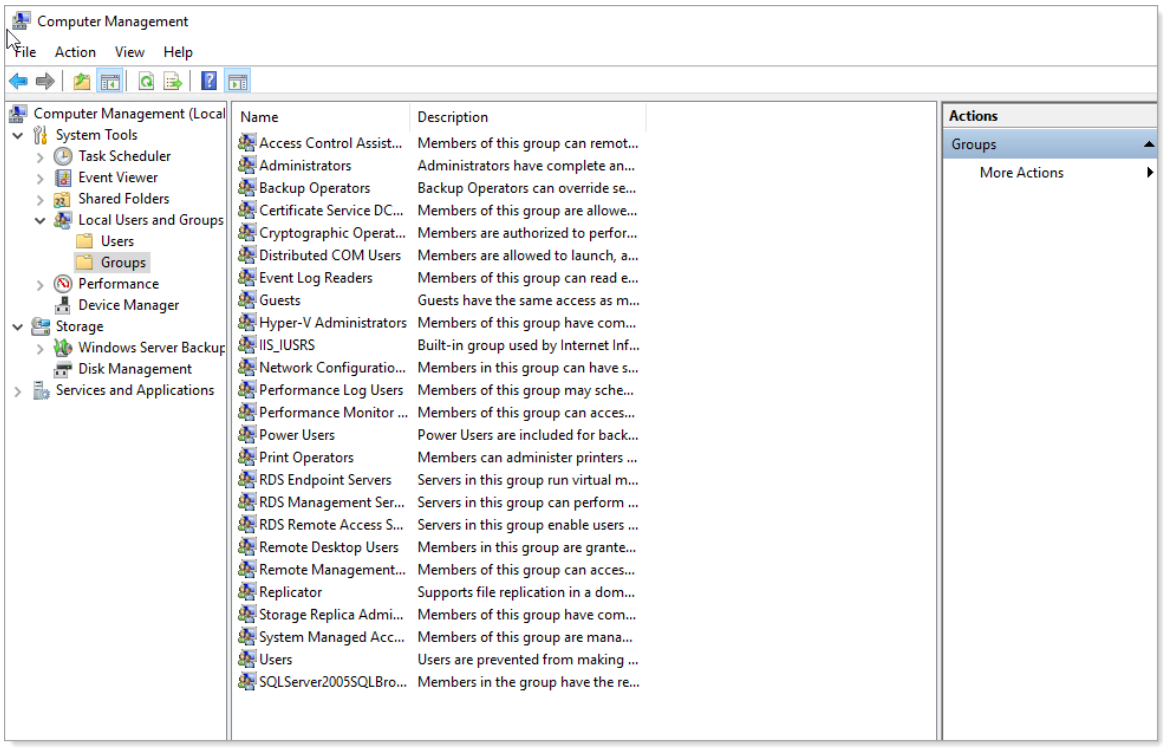
This topic describes how to add the ObserveIT service account user to the local IIS_IUSRS group on the ObserveIT Application Server(s) (and the Web Console machine if installed on a separate computer).

> This step is only required during the installation phase; the Service Account can be removed as soon as the installation has completed successfully.

1. On the ObserveIT Application Server, from **Start**, type **Computer Management**.

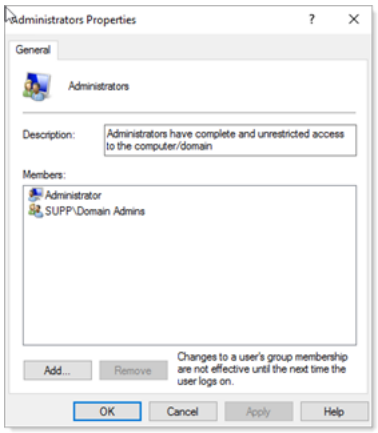
   The **Computer Management** window opens.

2. Expand **System Tools** and click **Local Users and Groups**. Expand **Groups** folder.



3. From the list of Groups, double-click **IIS_IUSRS** group.

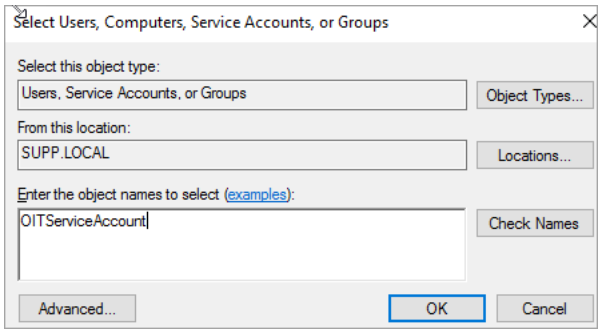
   The **Administrator Properties** dialog box opens.



4. Click **Add**.

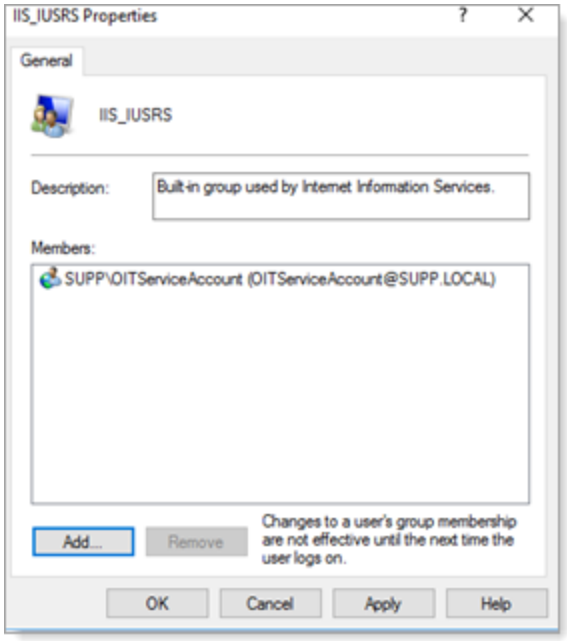
   The **Select Users, Computers, Service Accounts, or Groups** dialog box opens.

5. In the **Enter the object name to select** area, type **OITServiceAccount**.



6. Click **OK**.

   The **IRS_IUSRS Properties** dialog box opens and **OITServiceAccount** appears in the **Members** list.



7. Click **OK**.

8. If you plan to deploy more than one ObserveIT Application Server, or if you plan to install the ObserveIT Web Console on a separate machine, repeat on all the computers that will host the ObserveIT Application and Web Console applications.

Installing and Configuring Databases

When performing a custom installation, the database is the first component of ObserveIT that needs to be installed.

To successfully in install the database you need to:

- **Choose the location of the recorded graphic screenshots storage**: By default, all the recorded graphic screenshots are stored in the **ObserveIT_Data** database. In medium to large deployments of ObserveIT, it is strongly recommended to configure all recorded graphic screenshots to be stored in the file system network share (a UNC path) instead of in the SQL database. This will reduce the overall I/O overhead on the SQL Server. (For information about formatting the volumes.
- **Install the ObserveIT databases**: By default, ObserveIT uses Microsoft SQL Server databases for data storage. This storage includes user activity configuration data, user analytics data, textual audit metadata and possibly the screenshots captured by the ObserveIT Agents for video replay.
- Install the ObserveIT Analytics database.
- Add the ObserveIT Application Server(s) machine account to the ObserveIT databases.

  Choose the location of the recorded graphic screenshots storage.

  2. Edit the database installer configuration file to use file system storage for recorded graphic screenshots.

  3. Install the ObserveIT databases.

  4. Install the ObserveIT Analytics database.

  5. Add the ObserveIT Application Server(s) machine account to the ObserveIT databases.

You need to do complete the following tasks:

- Install the ObserveIT Databases
- Verify Database Installation
- Move Database File to Drives
- Set MDF and LDF File Size
- Install Database Maintenance

CONFIGURING LOCATION FOR RECORDED SCREENSHOTS

By default, all the recorded graphic screenshots are stored in the "ObserveIT_Data" database on the SQL Server.

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

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

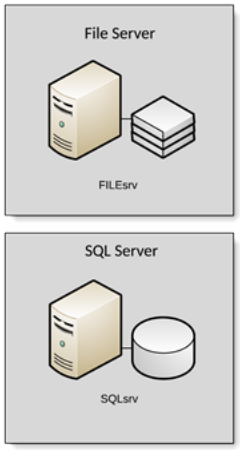
INSTALLING THE OBSERVEIT DATABASES

This topic describes how to attach the databases to the SQL server machine.

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

The time displayed in the Web Console is defined by the time zone of the database. Therefore, it is recommended that both the Web Console and Database are installed with the same time zone.

The diagram below shows the file server and the SQL database. The SQL database is installed after you configure the file server.



Prerequisites

- The database installer requires .NET Framework 4.5
- See Installing Prerequisites for more information.

Installing the Databases

1. Connect to the computer where you downloaded and extracted the ObserveIT Setup files.
2. Run the **SQLPackage.exe** file located in the **DB** folder which was created when you extracted the setup files from the archive.

   The **Database Installer** main window appears.

3. Select the SQL Server on which to install the database. The details of the **Server** field are in the following format:

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

   For example:

   `SQLsrv.test.lab\ObserveIT,1433`

4. If the account you are currently using is an SQL Server administrator, select **Windows Authentication** as the authentication method. Otherwise, select **SQL Server Authentication** and provide a user name and password with privileges to create databases and user accounts. If you select **Windows Authentication**, you will need to perform additional tasks.

5. Click **Run** to begin the installation.

   If the connection is successful, the installation will proceed. If not, check the connectivity to the SQL server and make sure the connection string is correct.

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

6. **Click OK** to ignore the following message:

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

   If you did not receive this error, it means that the ObserveIT service account has SYSADMIN permissions on the SQL Server. It is strongly suggested that you stop the installation at this phase, delete the resulting databases, change the ObserveIT service account permissions to DBCREATOR, and then re-execute the database installer program. While, by itself, this is

not a problem, the result is that the ObserveIT database and the subsequent connection strings used by all the ObserveIT components will use the "ObserveITUser" account in SQL Server instead of the ObserveIT service account. To fix this issue you will need to manually change the connection strings and change the SQL Server database settings. Contact support for information on how to perform these changes.

The message .**ObserveIT database successfully installed** appears.

7. Acknowledge the message the message **ObserveIT database successfully installed**. When the 4 databases are created, the window closes.

Installing the Analytics Database

1. Connect to the computer where you downloaded and extracted the ObserveIT Setup files.
2. Run the **SQLPackage.exe** file located in the **DB_Analytics** folder which was created when you extracted the setup files from the archive.
3. Select the SQL Server on which to install the database. The details of the **Server** field are in the following format:

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

   For example:

   `SQLsrv.test.lab\ObserveIT,1433`

4. If the account you are currently using is an SQL Server administrator, select **Windows Authentication** as the authentication method. Otherwise, select **SQL Server Authentication** and provide a user name and password with privileges to create databases and user accounts. If you select **Windows Authentication**, you will need to perform additional tasks.
5. From **File Explorer**, navigate and open the **DB_Analytics** folder and double-click the **SQLPackage** file.
6. Click **Run**.

   If the connection is successful, the installation will proceed. If not, check the connectivity to the SQL server and make sure the connection string is correct.

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

7. **Click OK** to ignore the following message.

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

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

The message .**ObserveIT database successfully installed** appears.

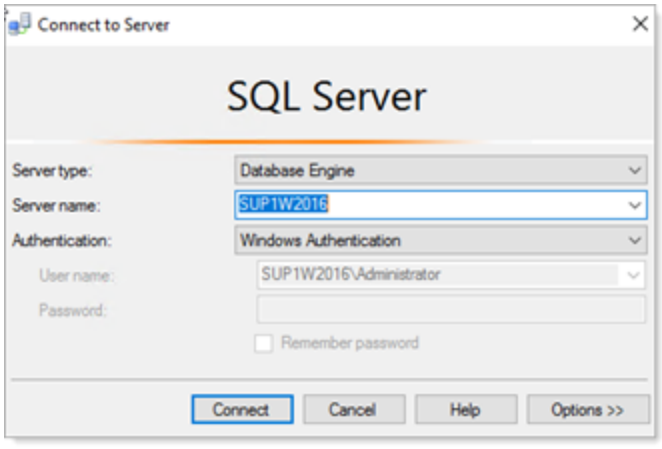
8. Acknowledge the success message **ObserveIT database successfully installed**.

VERIFYING DATABASE INSTALLATION

This topic describes how to verify that the databases were successfully installed on the SQL server.

1. Connect to the SQL server or to a computer with **SQL Management Studio** installed.
2. Open **Microsoft SQL Server Management Studio**.

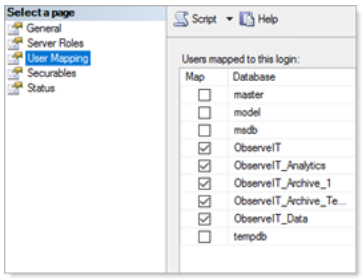
   The **Connect to server window** opens.



3. Type in the SQL server's FQDN or IP address into the **Server** name field.
4. Select **Windows Authentication** if your account has sysadmin permissions on the SQL server.

Otherwise, choose **SQL Server Authentication** and log in with a sysadmin-level account.

5. Click **Connect**.
6. In the Microsoft SQL Server Management Studio, Expand **Databases**. You should see five new ObserveIT databases.
7. Expand **Security** > **Logins**.
8. Right-click the **ObserveIT Service Account user** – in this example, OITServiceAccount – and select **Properties**.
9. Select **User Mapping** from **Select a Page** menu.



10. Under **User mapped to this login** click the ObserveIT database.
11. Make sure the checkbox in the **Map column** is checked.
12. Make sure that the checkbox for **db_owner** is checked.
13. Repeat for all databases.
14. Click **OK** and close **SQL Management Studio**.

MOVING DATABASE FILE TO DRIVES

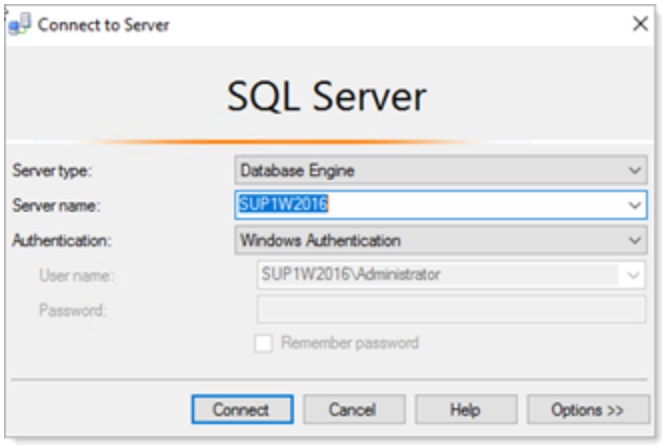
The best practice for SQL databases is to place the database data files (.mdf) and the database log files (.ldf) on separate drives.

This topic describes how to move the ObserveIT database files to designated drives.

The following steps assume two designated drives are present at the SQL machine. In the example, the database drive is assigned the drive letter E:, while the log drive is assigned the drive letter F:.

1. Connect to the SQL server or to a computer with **SQL Server Management Studio** installed.
2. Open **Microsoft SQL Server Management Studio**.

   The **Connect to server window** opens.



3. Type in the SQL server's FQDN or IP address into the **Server** name field.
4. Select **Windows Authentication** if your account has sysadmin permissions on the SQL server. Otherwise, choose **SQL Server Authentication** and log in with a sysadmin-level account.
5. Click **Connect**.
6. Paste the following code into the **New Query** window:

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

```
USE MASTER;

GO

ALTER DATABASE ObserveIT_Data

SET SINGLE_USER

WITH ROLLBACK IMMEDIATE;
```

```
GO

EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Data'

GO

USE MASTER;

GO

ALTER DATABASE ObserveIT

SET SINGLE_USER

WITH ROLLBACK IMMEDIATE;

GO

EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT'

GO

USE MASTER;

GO

ALTER DATABASE ObserveIT_Archive_1

SET SINGLE_USER

WITH ROLLBACK IMMEDIATE;
```

```
GO

EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Archive_1'

GO

USE MASTER;

GO

ALTER DATABASE ObserveIT_Archive_Template

SET SINGLE_USER

WITH ROLLBACK IMMEDIATE;

GO

EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Archive_
Template'

GO

USE MASTER;

GO

ALTER DATABASE ObserveIT_Analytics

SET SINGLE_USER

WITH ROLLBACK IMMEDIATE;
```

```
GO

EXEC MASTER.dbo.sp_detach_db @dbname = N'ObserveIT_Analytics'

GO
```

7. Click **Execute**. Wait for the query to finish.
8. Format 2 new disks in the machine. See "Formatting a Disk for Graphic Images Storage and the Database" on page 13

   In the example below: disk E: for the database data files and disk F: for the database log files.

   From **File Explorer**, navigate to disk E:.
9. Create a new folder, **MSSQLDATA**.
10. Navigate to disk F:.
11. Create a new folder, **MSSQLLog**.
12. Open PowerShell and run as an administrator.
13. If prompted **Do you want to allow this app to make changes to your device?** click **Yes**.
14. Paste the following code into the PowerShell window:

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


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

15. **Enter** key at the final prompt.
16. Return to the **SQL Server Management Studio**.

17. Click New Query.
18. Paste the following code into the New Query window:

```
CREATE DATABASE [[observeIT_Archive1] ON

( FILENAME = N'E:\MSSQLDATA\ObserveIT_Data_Data.mdf' ),

( FILENAME = N'F:\MSSQLLog\ObserveIT_Data_Log.ldf' )

FOR ATTACH

GO

CREATE DATABASE [ObserveIT] ON

( FILENAME = N'E:\MSSQLDATA\ObserveIT_Data.mdf' ),

( FILENAME = N'F:\MSSQLLog\ObserveIT_Log.ldf' )

FOR ATTACH

GO

CREATE DATABASE [ObserveIT_Analytics] ON

( FILENAME = N'E:\MSSQLDATA\ObserveIT_Analytics_Data.mdf' ),

( FILENAME = N'F:\MSSQLLog\ObserveIT_Analytics_Log.ldf' )

FOR ATTACH

GO
```

```
CREATE DATABASE [ObserveIT_Analytics] ON

( FILENAME = N'E:\MSSQLDATA\ObserveIT_Archive_1_Data.mdf' ),

( FILENAME = N'F:\MSSQLLog\ObserveIT_Archive_1_Log.ldf' )

FOR ATTACH

GO

CREATE DATABASE [ObserveIT_Archive_Template] ON

( FILENAME = N'E:\MSSQLDATA\ObserveIT_Archive_Template_Data.mdf'
),

( FILENAME = N'F:\MSSQLLog\ObserveIT_Archive_Template_Log.ldf' )

FOR ATTACH

GO
```

19. Click **Execute**. Wait for the query to finish.
20. Close the **SQL Server Management Studio**.

INSTALLING DATABASE MAINTENANCE

The ObserveIT databases have to be maintained on a regular basis in order for the system to work properly and efficient.

To ensure optimal database health and performance, add the automated maintenance procedure for your ObserveIT databases.

1. Connect to the machine containing the ObserveIT database or the machine where **SQL Server Management Studio** is installed.
2. Download the file: http://files.observeit.com/support/OIT-DB-Maintenance.zip

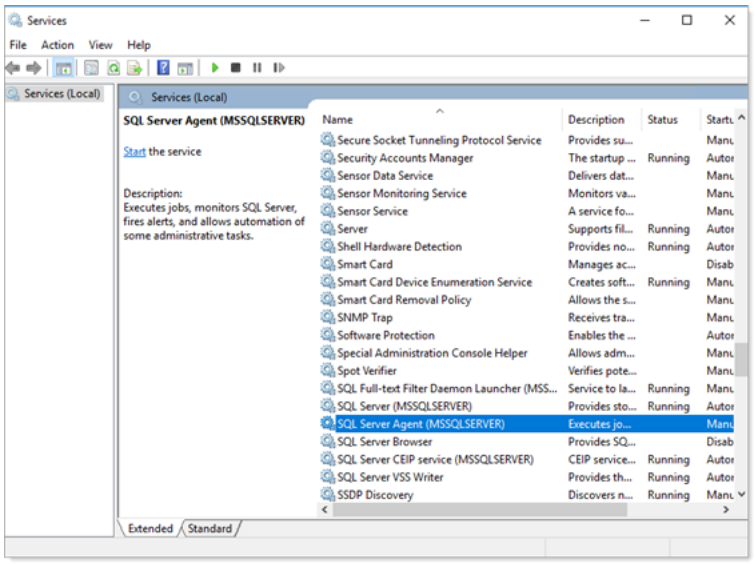
3. In **File Explorer**, navigate to the folder you downloaded.
4. Extract the files from **OIT-DB-Maintenance.zip**..

   From the extracted files, select and double-click **dbmaintprepare.sql** file.

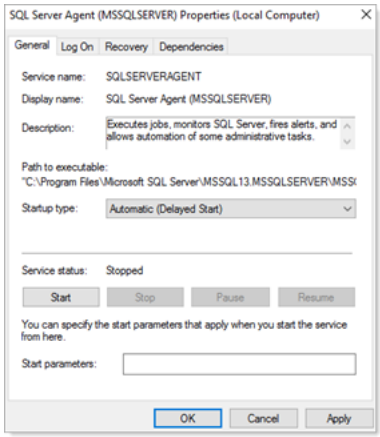
   If prompted **How do you want to open this file?** choose **SQL Management Studio** or **SSMS**. Click **OK**.
5. Open **SQL ServerManagement Studio**, specify the server name, authentication type and Login and Password to the ObserveIT SQL instance (if connecting via SQL Server Authentication). Click **Connect**.

   If successfully completed, a confirmation message appears in the **Messages** pane.
6. Return to the **File Explorer** window. From **File Explorer**, select and double-click **OIT-DB-Maint-Create-Jobs.sql** file.
7. From **SQL ServerManagement Studio**, select **Query** > **Execute**.

   If successfully completed, a confirmation message appears under the **Messages** pane. Ignore any warnings received.
8. Close the **SQL Server Management Studio**.
9. Open the **Start** menu and type in **Run**.
10. Type in **services.msc** to open the **Services** window. Press **Enter**.
11. Locate **SQL Server Agent** service.



12. Right-click the service and click **Properties**.



13. Change the value for **Startup Type** field to **Automatic (Delayed Start).**
14. Click **Start**.
15. Click **OK**.
16. Close the window.

Configuring Microsoft Internet Information Server (IIS)

The ObserveIT Application Server and the Web Management Console are implemented as ASP.NET Web applications that run on Microsoft Internet Information Server (IIS) 8.0 or higher, depending on the

Windows Server version.

You need to prepare Internet Information Services (IIS) for installing ObserveIT Web applications.

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

Related Topics:

OBTAINING A DIGITAL CERTIFICATE

A digital certificate is the digital equivalent of an ID card used with a public key encryption system. Also known as digital IDs, digital certificates are issued by trusted third parties known as Certification Authorities (CAs). This document assumes that the reader has prior knowledge of Public Key Infrastructure (PKI) and its related terminology.

For further details, refer to the Microsoft Knowledge Base article, see How to implement SSL in IIS.

Digital Certificate Source

A digital certificate must be issued from a Certificate Authority (CA), either a 3rd-party commercial CA (such as, Verisign, Thawte, Godaddy, Rapid SSL, and others), or from an internal CA. Third-party CAs sell digital certificates at prices ranging from a few dollars to a few hundred dollars per year, depending on the type of certificate issued, and other considerations, such as the CA's reputation.

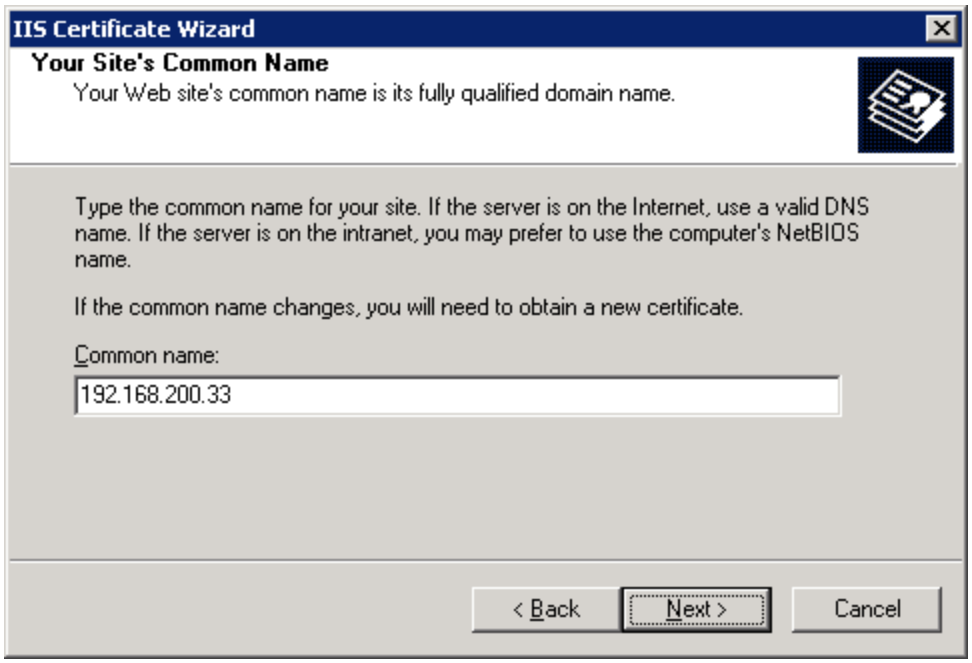
However, most operating systems are preconfigured to trust a list of known 3rd-party CAs. This facilitates deployment since you do not need to import anything to the computers running the ObserveIT Agents. To avoid paying for a digital certificate, you can use an internal CA. Note that Windows Server 2008/2012 has a built-in CA that you can install and use.

In cases where an internal CA is not required, or where such a deployment cannot be achieved, you can also use a Self-Signed Digital Certificate.

After a digital certificate is obtained, you must import the root CA digital certificate or the self-signed digital certificate to each client computer running the ObserveIT Agent, so that they trust your digital certificate source.

Digital Certificate Common Name

1. When issuing a digital certificate for the ObserveIT Application Server, you must make sure that the Common Name field or the Issued to field on that certificate contains the same name as the URL of the ObserveIT Application Server.



For example, if the ObserveIT Agents use the following Fully Qualified Domain Name (or FQDN) to connect to the ObserveIT Application Server:

server100.mydomain.local

Then the same exact name MUST be used when issuing the digital certificate for the ObserveIT Application Server.

2. When connecting to the ObserveIT Application Server, an IP address can be used instead of an FQDN. If the following IP address is used by the ObserveIT Agents to connect to the ObserveIT Application Server:

   192.168.200.33

   The same exact IP address MUST be used when issuing the digital certificate for the ObserveIT Application Server.

3. at ObserveIT.ClientSetupActions.ClientInstaller.Install(IDictionary stateSaver)

4. If you do not follow these guidelines, an error message similar to one of the following appears:

   System.Net.WebException: The underlying connection was closed: Unable to connect to the remote server.

   at ObserveIT.ClientSetupActions.RegisterServerManager.GetLicenseStatus()

at ObserveIT.ClientSetupActions.ClientInstaller.Install(IDictionary stateSaver)

-Or-

System.Net.WebException: The underlying connection was closed: Could not establish trust relationship with remote server.

at System.Net.HttpWebRequest.CheckFinalStatus()

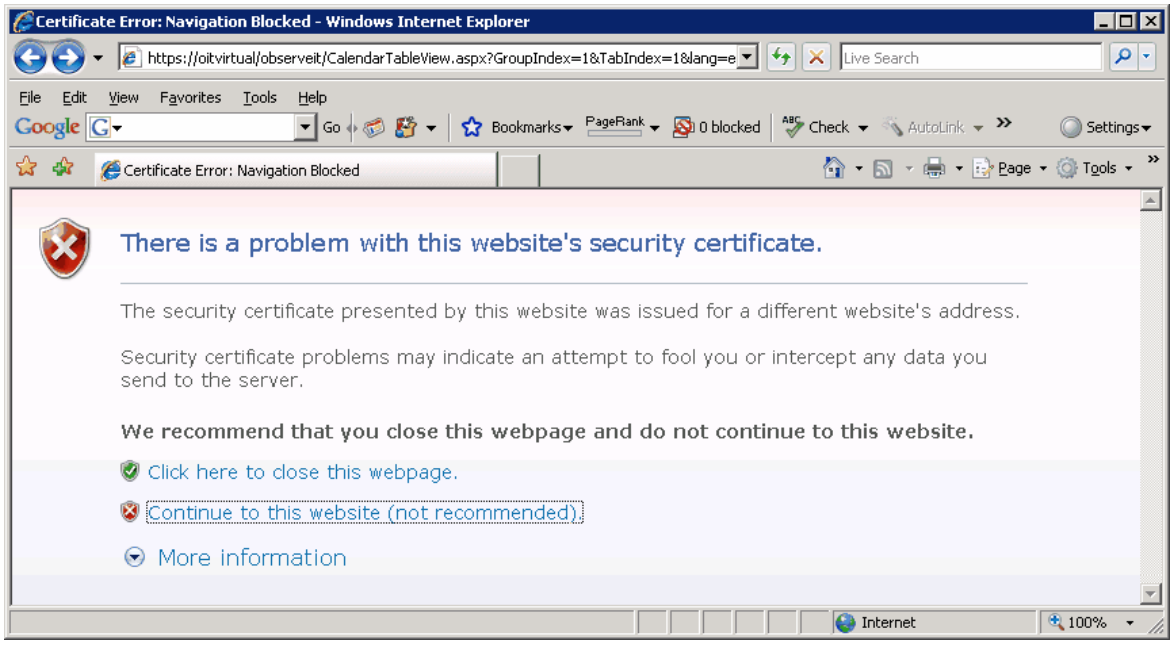
at System.Net.HttpWebRequest.EndGetRequestStream(IAsyncResult asyncResult)

at System.Net.HttpWebRequest.GetRequestStream()

at System.Web.Services.Protocols.SoapHttpClientProtocol.Invoke(String methodName, Object[] parameters)

at ObserveIT.ClientSetupActions.Proxy.HeartBeatPrxClone.IsAlive()

While not viewable by the ObserveIT Agent, if you manually try to connect to the ObserveIT Web Console while using an FQDN or IP address that does not match the one listed in the server's SSL digital certificate, a warning appears in the Web browser, similar to that shown in the following screenshot.



If you click Continue to this website (not recommended), you can view the digital certificate error message (by clicking the button).

ASSIGNING A DIGITAL CERTIFICATE

This topic describes how to assign a digital certificate for the Web Console. You can use the Microsoft Management Console or Internet Information Services (IIS) Manager.

ObserveIT Recommendations:

- Always assign a certificate
- Encrypt the Web Console traffic by using HTTPS.

Consult with your organization's security team to learn what type of digital certificate best fits your environment. When it is not possible to acquire a Certificate Authority certificate, a self-signed certificate may be used.

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

(The following assumes an Enterprise Certificate Authority certificate is used.)

Using Microsoft Management Console

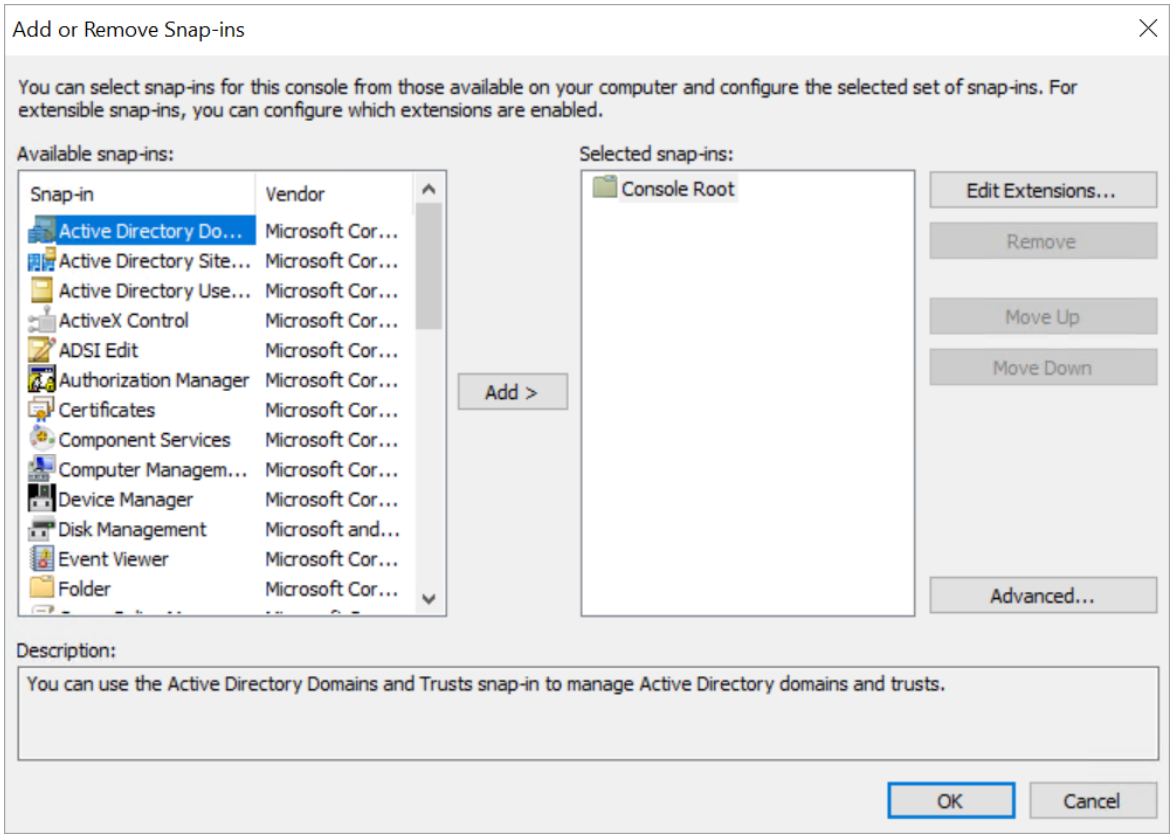
You can create an internal Enterprise Certificate Authority certificate for the Web Console using Microsoft Management Console.

1. From the **Start** menu and type **mmc** in the **Run** window. **Enter**.

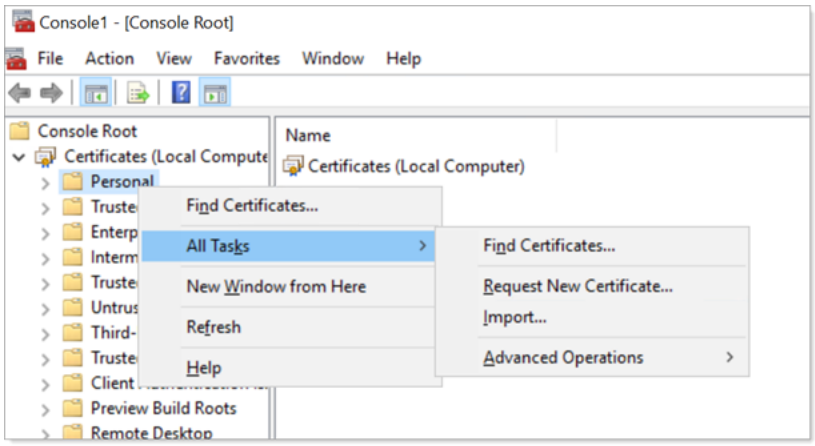
   If prompted **Do you want to allow this app to make changes to your device?** click **Yes**.

   The **Microsoft Management Console** window opens.

2. From the menu, select **File** > **Add/Remove Snap-in**.

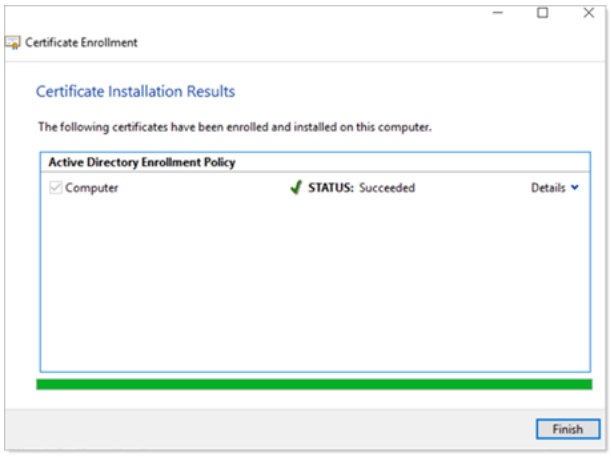


3. From **Available snap-ins** choose **Certificates** and click **Add**.
4. In the **Certificates snap-in** window choose **Computer account** and click **Next**.
5. In the **Select Computer** window, from **Select the computer you want this snap-in to manage** options, select **Local computer** and click **Finish**.
6. Click **OK** to return to the Console window.
7. Expand **Certificates (Local Computer)**.
8. Right-click **Personal**, select **All Tasks** and then **Request New Certificate**.

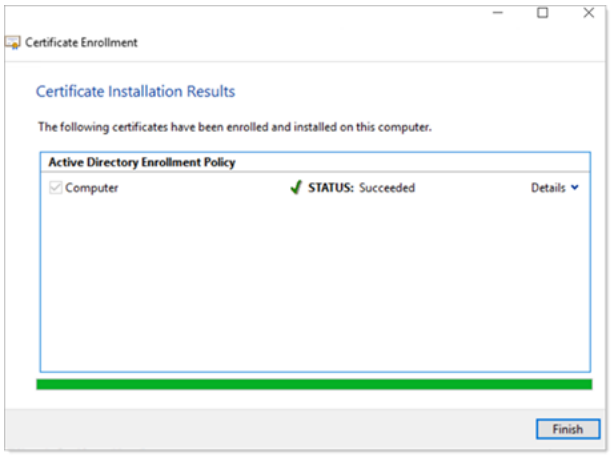


9. Click **Next** to close the **Certificate Enrollment** message. The **Certificate Enrollment Policy** page opens.

10. In the **Select Certificate Enrollment Policy** page select your enrollment policy (usually – Active Directory Enrollment Policy) and click **Next**.

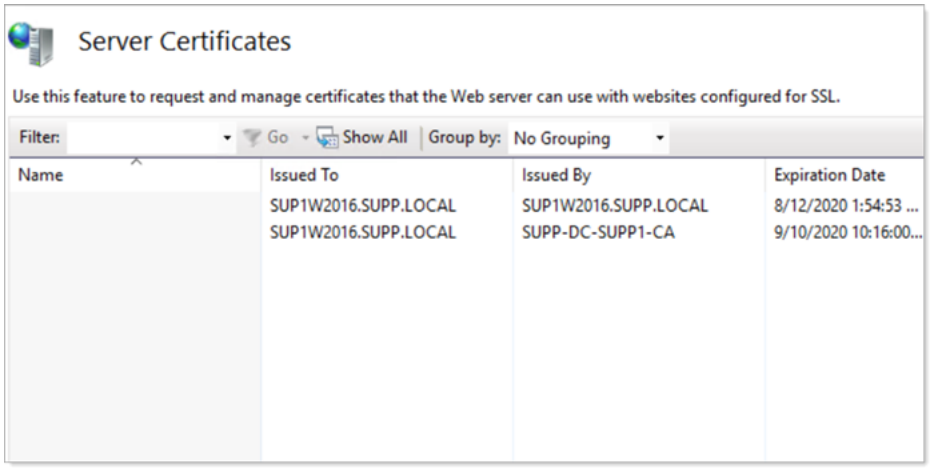


11. In the **Request Certificates** page select the certificate type (usually – Computer) and click **Enroll**.



12. Click **Finish** when the enrollment is successfully completed to close the window.
13. Confirm the newly-created certificate exists, ffrom the console, select **Personal**> **Certificates**.

    The FQDN of the current server displays in the **Issued To** column.



Using Internet Information Services (IIS) Manager

You can create a self-signed certificate for the Web Console using the IIS Manager.

1. Connect to the ObserveIT Web Console machine.
2. Open **Internet Information Services (IIS) Manager** .
3. In **Connections** area on the left, select the relevant server and double-click the **Server Certificates** icon at the main page.
4. In the **Actions** area on the right, click **Create Self-Signed Certificate**.

5. In the **Specify a friendly name for the certificate** field, enter a descriptive name for the certificate. Click **OK**.

CREATING A NEW APPLICATION POOL IN IIS 8.X

When installing ObserveIT, the installer automatically creates a new application pool in IIS and uses it for the ObserveIT server-side component installations. If a custom installation is required, you can manually create the application pool and configure the website to use it when installing the ObserveIT server-side components.

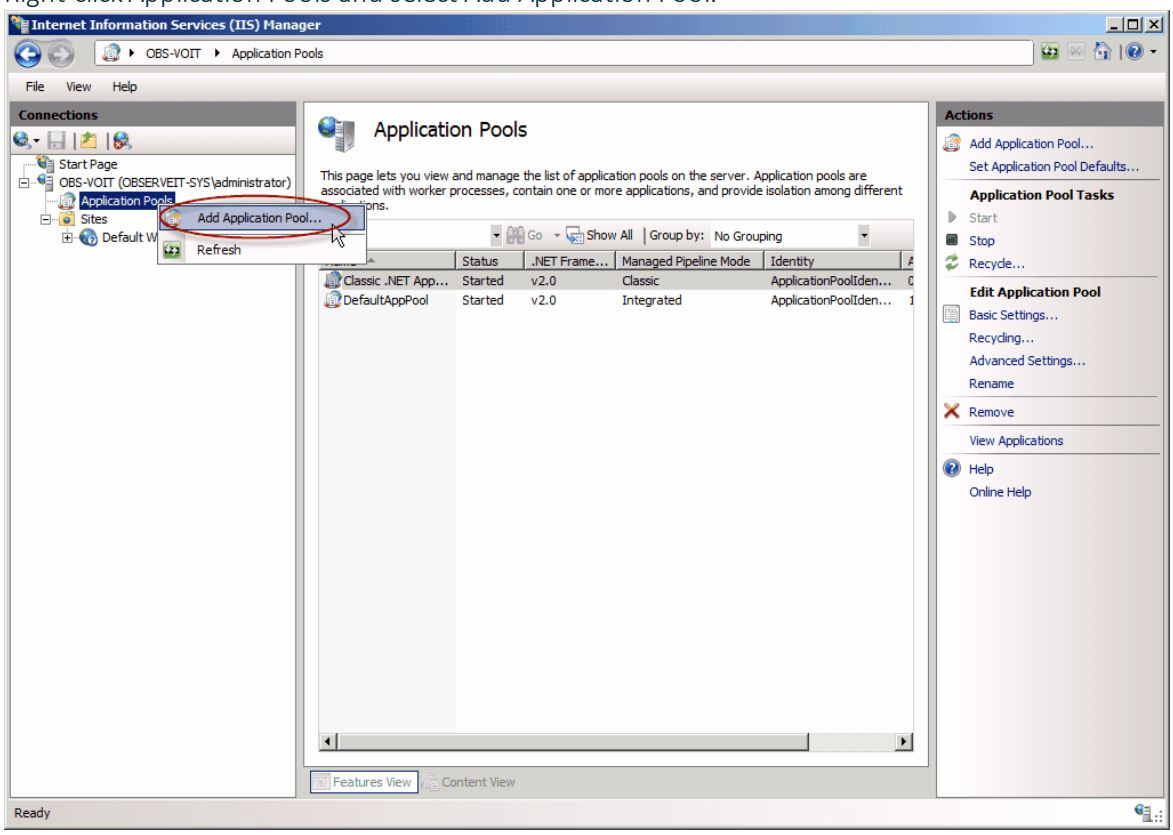
The application pool must be configured as Integrated in order to use it for the ObserveIT server-side component.

You can create an application pool manually or use Powershell commands.

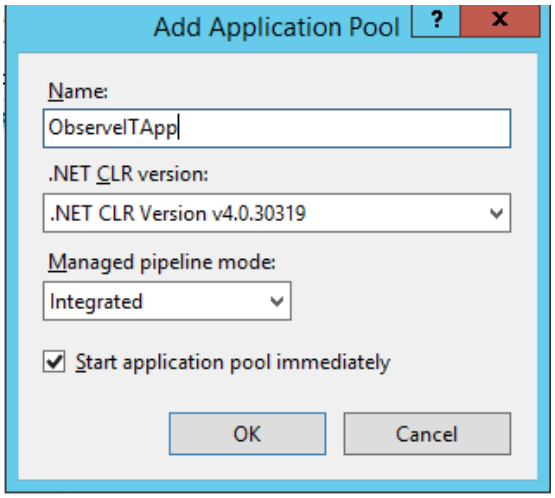
To create a new application pool in IIS 8.X for the Application server (Manual):

1. On the server running IIS, open IIS Manager from the Administrative Tools folder. Expand your server name.

2. Right-click Application Pools and select Add Application Pool.



3. In the Add Application Pool dialog box:
    1. In the Name field enter ObserveITApp. (The Application Pool name must not contain spaces.)
    2. In the Managed pipeline mode column, select Integrated from the list.
    3. Click OK.



The new application pool appears in the Application Pools list.

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

For example:

OITsrv1 – Application Server #1 – would hold a single ObserveITApplication Application Pool.

OITsrv2 – Application Server #2 – would hold a single ObserveITApplication Application Pool.

OITweb – Web Console – would hold a single ObserveITWebConsole Application Pool.

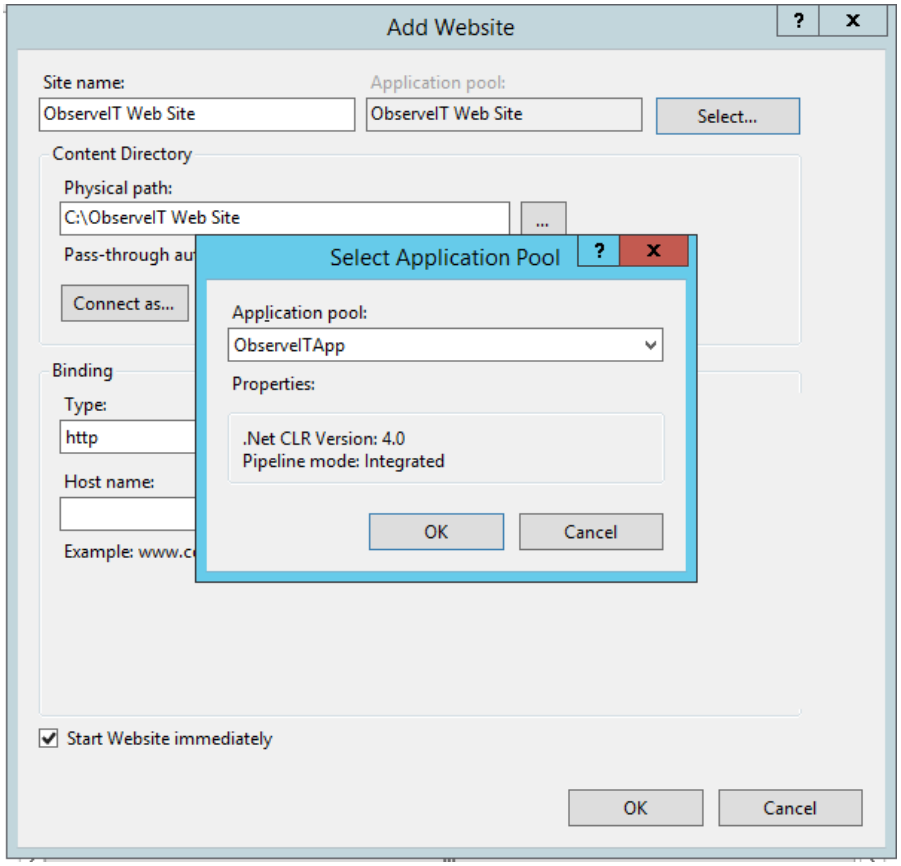
To create a new application pool in IIS 8.X for the Application server (PowerShell):
Open PowerShell as administrator and paste the following commands:

```
$WebSiteName = 'ObserveITApplication'

Import-Module WebAdministration

New-Item IIS:\Sites\$WebSiteName -PhysicalPath 'C:\Program Files\Ob-
serveIT\Web\' -Bindings @{pro-
tocol="https";bindingInformation=":443:"}

Set-ItemProperty IIS:\Sites\$WebSiteName\ -Name applicationpool -
Value $WebSiteName
```

To create a new application pool in IIS 8.X for the ObserveIT Console (manual):

1. Open Internet Information Services (IIS) Manager .
2. In Connections area on the left, select the relevant server and select Sites.

3. Right-click **Sites** and select **Add Website**.
4. In the **Site Name** field type in **ObserveITApplication**.
5. Click **Select** (next to the **Application Pool** field).
6. Select the **ObserveITApplication** Application Pool. Click **OK**.



7. Navigate to the following path: **C:\Program Files\ObserveIT\Web**. Click the Web folder. Click **OK**.
8. Click **Select** (next to the **Application Pool** field).

   If you cannot find the "ObserveITApplication" application pool make sure you properly created the application pool before creating the website.

9. In the **Binding** area, in the **Port** field, change the port value from 80 to 443.
10. Click **OK** to save the changes and create the new website.

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

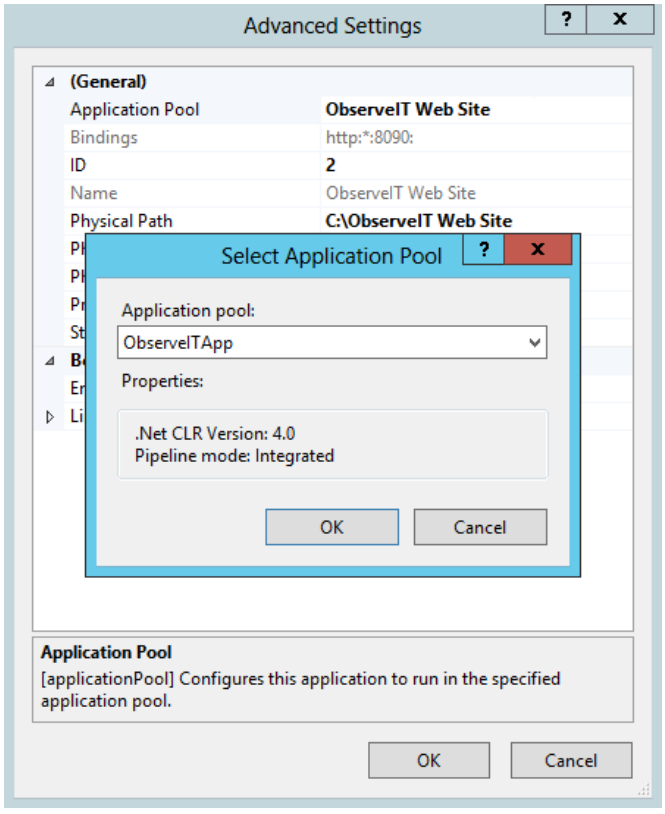
For example, if you plan to use the following setup:

- OITsrv1 – Application Server #1
- OITsrv2 – Application Server #2

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

When modifying an existing website, you need to configure that website to use this new application pool, as follows:

1. Select the existing website in the Sites list, and click the Advanced Settings link for that website.
2. In the Advanced Settings window, click the Application Pool section, and then click the [...] button next to the existing application pool.
3. In the Select Application Pool window, from the Application pool list, select ObserveITApp.
4. Click OK



Click OK to close the Advanced Settings window.

To create a new application pool in IIS 8.X for the ObserveIT Console (Automatic - PowerShell):

Open PowerShell as administrator and paste the following commands:

```
$WebSiteName = 'ObserveITApplication'

Import-Module WebAdministration

New-Item IIS:\Sites\$WebSiteName -PhysicalPath 'C:\Program Files\ObserveIT\Web\' -Bindings @{protocol="https";bindingInformation=":443:"}

Set-ItemProperty IIS:\Sites\$WebSiteName\ -Name applicationpool -Value $WebSiteName
```

Creating a New Application Pool in IIS 7.X

Creating a New Website in IIS 7.X

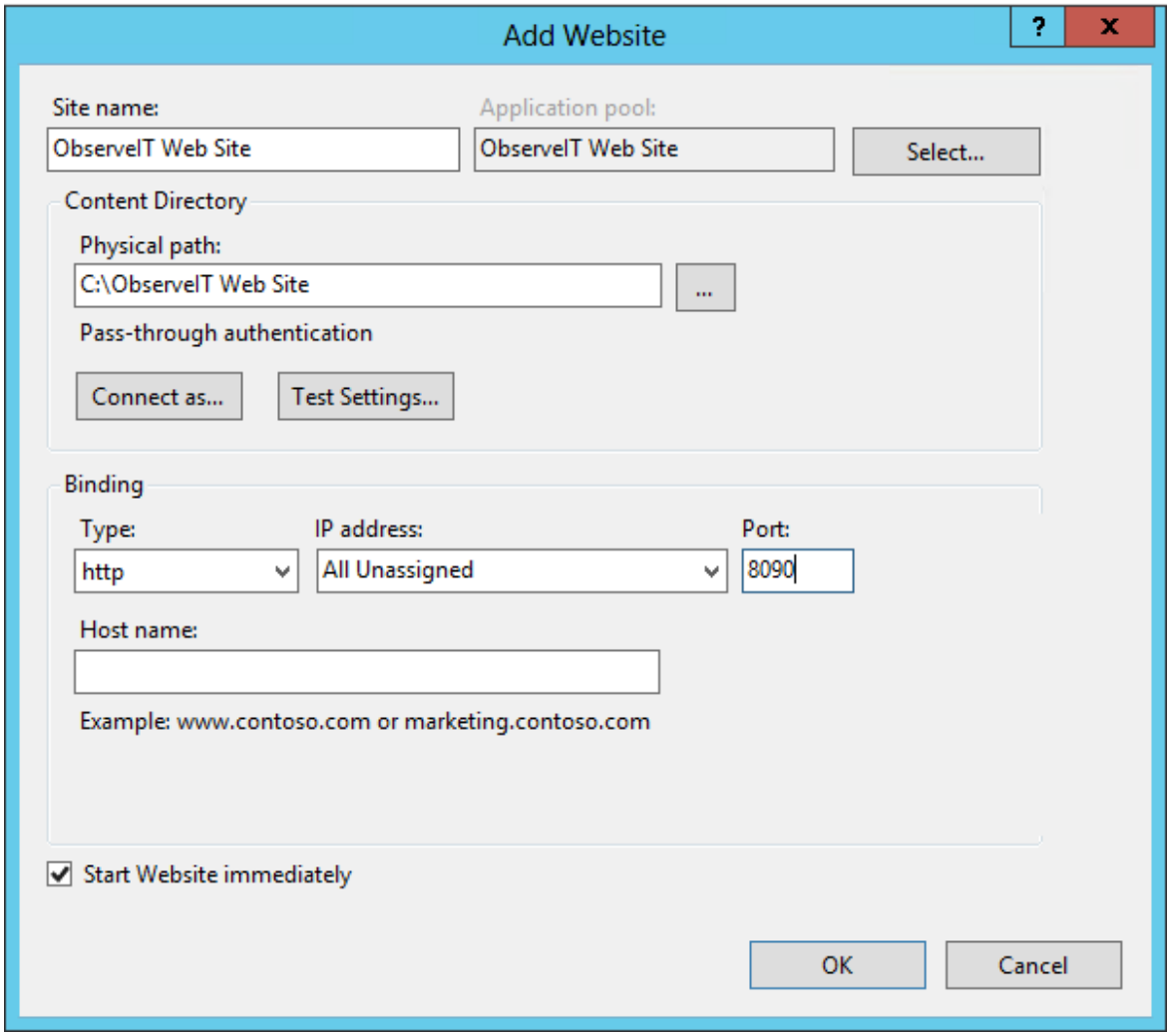
CREATING A NEW WEBSITE IN IIS 8.X FOR THE OBSERVEIT APPLICATION SERVER

When installing ObserveIT, the installer automatically creates a new website in IIS and uses it for the ObserveIT server-side component installations.

In a custom installation, you can create an additional website in IIS, and use this site to host the ObserveIT Application and Web Management virtual directories. However, in order to run multiple websites on the same IIS server, the listening IP address of each website, the listening TCP port of each website, and/or the Host Header of each website, must remain unique.

To create a new website for the ObserveIT Application Server (Using the Wizard - Manual):

1. On the server running IIS, open IIS Manager from the Administrative Tools folder. Expand your server name, then expand Sites.
2. Right-click Sites and select Add Website.
3. Follow the steps in the Web Site Creation Wizard. Make a note of the listening IP address of the new website, the listening TCP port of the new website, and/or the Host header of the new website.
4. In the Site Name field type ObserveITApp. Click Select.
5. From the Application pool dropdown, select ObserveITApp and click OK.

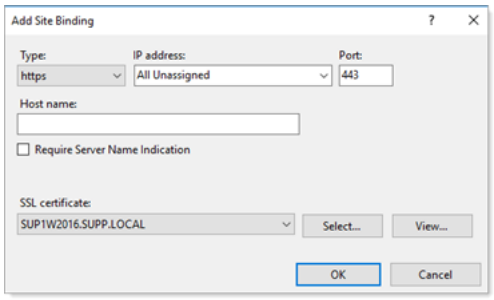


6. From the **Physical path** field, navigate to the following path: C:\Program Files\ObserveIT\Web. Select the **Web** folder and click OK.

7. Click the **Select** button next to the **Application pool** field

> If you cannot find the "ObserveITApplication" application pool make sure you properly created the application pool before creating the website.

8. In the **Binding** area, in the **Port** field, change the port value from 80 to 443.



9. Click **OK** to save the changes and create the new website.
10. If you have multiple Application Servers, you need to repeat this process for each machine.

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

    OITsrv1 – Application Server #1

    OITsrv2 – Application Server #2

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

To create a new website in IIS 8.x for the Application Server (Automatic - Powershell):
Open PowerShell as administrator and paste the following commands to execute above steps automatically.

```
$WebSiteName = 'ObserveITApplication'

Import-Module WebAdministration

New-Item IIS:\Sites\$WebSiteName -PhysicalPath 'C:\Program
Files\ObserveIT\Web\' -Bindings @
{protocol="https";bindingInformation=":443:"}

Set-ItemProperty IIS:\Sites\$WebSiteName\ -Name applicationpool -
Value $WebSiteName
```

CREATING A NEW WEBSITE IN IIS 8.X FOR THE OBSERVEIT WEB CONSOLE

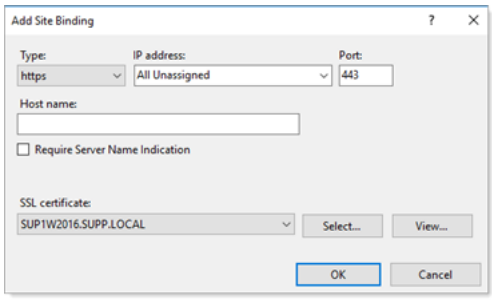
You can create an additional website in IIS.

To create a new website for the ObserveIT Web COnsole(Using the Wizard - Manual):

1. On the server running IIS, open IIS Manager from the Administrative Tools folder. Expand your server name, then expand Sites.
2. Right-click Sites and select Add Website.

3. Follow the steps in the Web Site Creation Wizard. Make a note of the listening IP address of the new website, the listening TCP port of the new website, and/or the Host header of the new website.
4. In the **Site Name** field type ObserveITApp. Click **Select**.
5. From the **Application pool** dropdown, select **ObserveITWebConsole** and click **OK**.
6. From the **Physical path** field, navigate to the following path: C:\Program Files\ObserveIT\Web. Select the **Web** folder and click OK.
7. Click the **Select** button next to the **Application pool** field

   If you cannot find the "ObserveITWebConsole"application pool make sure you properly created the application pool before creating the website.
8. In the **Binding** area, change the value from http to https. The value of the **Port** field will be automatically changed from 80 to 443.



9. In the **SSL certificate** field select a certificate you have previously created.
10. Click **OK** to save the changes.

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

To create a new website in IIS 8.x for the Application Server (Automatic - Powershell):
Open PowerShell as administrator and paste the following commands to execute above steps automatically.

```
$WebSiteName = 'ObserveITWebConsole'

Import-Module WebAdministration

New-Item IIS:\Sites\$WebSiteName -PhysicalPath 'C:\Program
Files\ObserveIT\Web\' -Bindings @
{protocol="https";bindingInformation=":443:"}
```

```
Set-ItemProperty IIS:\Sites\$WebSiteName\ -Name applicationpool -
Value $WebSiteName
```

Installing ObserveIT Components

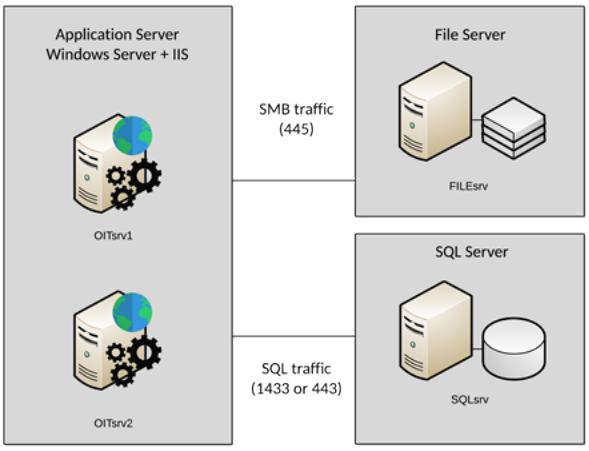
Installing ObserveIT components includes the following servers and modules:

- ObserveIT Application Server
- ObserveIT Web Management Console
- SQL Native Client
- Screenshot Storage Optimizer
- Web Categorization Module

INSTALLING OBSERVEIT APPLICATION SERVER

Depending on the sizing and architecture of the product deployment, you must install one or more ObserveIT Application Server(s).

This Application server is installed after you install the database and file server.



This topic describes how to install and verify the ObserveIT Application Server component on the first server. If you have multiple Application Servers, you need to repeat this procedure for each machine.

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

Prerequisite for installing the ObserveIT Application Server: Download the most recent version of Microsoft ASP .Net Core Runtime Windows Hosting Bundle.

Installing ObserveIT Application Server (Manual)

1. From the **Command Prompt**, select **Run as administrator**.

   If prompted, **Do you want to allow this app to make changes to your device?**, select **Yes**.

2. Navigate to the folder with the extracted ObserveIT Installer. Navigate to the Web folder.

   For example:

   `c:\Users\OITServiceAccount\Desktop\ObserveIT_Setup_vx.x.x.xx\Web`

3. Run **PreRequisite_nodeServices.exe**.

   Check the check box with the message **I agree to install the following products and click Install**.

   Wait for the installation to finish and then click **Close**.

4. From the command line, as an administrator, navigate to the folder with the extracted ObserveIT Installer. Navigate to the Web folder.

   For example: `cd c:\Users\OITServiceAccount\ObserveIT_Setup_vx.x.x.xx\Web\AppServer`

5. Open the **Start** menu and type **Command Prompt**.

6. Right-click the **Command Prompt** shortcut icon and select **Run as administrator**.

   If prompted **Do you want to allow this app to make changes to your device?**, click **Yes**.

7. From the command line, as an administrator, navigate to the folder with the extracted ObserveIT installer. Navigate to the Web folder.

   For example: `cd c:\Users\OITServiceAccount\ObserveIT_Setup_vx.x.x.xx\Web\AppServer`

8. Type ObserveIT.AppServerSetup.msi and **Enter**.

9. In the **ObserveIT Application Server** window click **Next**.

10. In the **Site** field, select **ObserveITApplication**.

11. In the **Application Pool** field, select **ObserveITApplication**. Click **Next**.

12. In the **Server** field, enter the details of the SQL server, in the following format:

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

For example: `SQLsrv.test.lab\ObserveIT,1433`

13. Select the **Windows Authentication** radio button and enter the password for the current account – the ObserveIT Service Account - in the **Password** field. Click **Test Connection**.

    If the test is successful, a success message displays, and the **Next** button becomes available.

14. Click **Next**. The installation begins.

15. After successful installation, click **Close**.

Installing ObserveIT Application Server (Powershell - Automatic)
Open PowerShell as administrator and paste the following commands to execute above steps automatically.

The following command assumes the ObserveIT installer is located under the C:\Temp\ObserveIT-_Setup_v7.8.2.270 path. After the execution of the command, the installation will starts – just follow the prompts.

```
iisreset /stop

Get-Service WAS | Start-Service

Start-Process msiexec -ArgumentList '/i', "C:\Temp\ObserveIT-_Setup_
v7.8.2.270\Web\AppServer\ObserveIT.AppServerSetup.msi", '/norestart',
'/l*v ObserveITWebConsole_setup.txt' -Wait

iisreset /start
```

Verifying Application Server Installation

1. Connect to the ObserveIT Web Console machine.
2. Open the **Start** menu and type **Run**. **Enter**.
3. Type `%userprofile%\AppData\Local\Temp`. **Enter**.
4. Locate `AppServer_CA_Log.txt` file. Double-click the file to open it.
5. Open the Find dialog. (Press CTRL+F on the keyboard.) Find **RegisterApplicationServer**
6. Locate the following line: **RegisterApplicationServer: Done**.

If the line does not exist or the word **Done** does not exist – the installation failed. Re-check the installation requirements, particularly the permissions for the SQL logins.

Installing Additional ObserveIT Application Servers

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

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

When deploying more than one Application Server, you need to load balance the Agent connections with the multiple Application Servers.

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

LOAD BALANCING

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

When deploying more than one Application Server, you need to load balance the Agent connections with the multiple Application Servers. You may use software-based load balancing solutions, such as Microsoft Network Load Balancing (NLB), or hardware-based solutions, such as F5, Citrix NetScaler, or others.

Expected reply: 200

For example:


```
{"_status":{"status":200,"code":"it:error:none","context":{"trans-
actionId":"","correlationId":""}},"_meta":{"origin":{},"stats":
{}},"status":"Healthy","database":
{"status":"Healthy","roundTripTime":"00:00:00.0017518"},"fileSystem":
{"status":"Healthy","roundTripTime":"00:00:00.0033923"}}
```


You can change the health check interval to 10 seconds by editing the HealthCheck-SecondsInterval value in the web.config file on the Application Server(s).

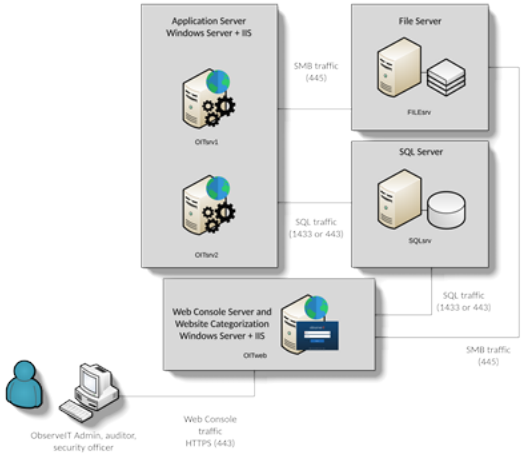
INSTALLING OBSERVEIT WEB MANAGEMENT CONSOLE

The ObserveIT Web Console is the component that is used to configure, administer and use the product. Multiple Web Consoles can be installed in an environment for redundancy purposes.

In most cases, the Web Console is installed on the same machine as the Application Server (the first one, in case of multiple Application Servers). However, it's also possible to configure a dedicated machine for this.

The time displayed in the Web Console is defined by the time zone of the database. Therefore, it is recommended that the Web Console and Database are installed with the same time zone.

Before you can verify the Web Console installation you must install the SQL Native client. This lets you work with ObserveIT REST APIs.



Prerequisite for installing the Web Management Console: Download the most recent version of Microsoft ASP .Net Core Runtime Windows Hosting Bundle.

Installing the Web Management Console (Manual)

1. Connect to the computer where you downloaded and extracted the ObserveIT setup files.

   If unable to log in as the ObserveIT Service Account interactively, see **Running elevated Windows PowerShell prompt as a different user**.

2. Open the **Start** menu and type in **Command Prompt**.
3. Right-click the **Command Prompt** shortcut found and choose **Run as administrator**.
4. If prompted **Do you want to allow this app to make changes to your device?** click **Yes**.
5. Navigate to the folder with the extracted ObserveIT installer. Navigate to the **Web** folder.

   For example:

   ```
   c:\Users\OITServiceAccount\Desktop\ObserveIT_Setup_vx.x.x.xx\Web"
   ```

6. Run **PreRequisite_nodeServices.exe**.
7. Check the check box with the message **I agree to install the following products** and click **Install**.

8. Wait for the installation to finish. Click **Close** when it does.
9. Navigate to the folder with the extracted ObserveIT installer. Navigate to the **Web\WebConsole** folder.

   For example: `c:\Users\OITServiceAccount\Desktop\ObserveIT_Setup_vx.x.x.xx\Web\WebConsole`
10. Type in **ObserveIT.WebConsoleSetup.msi** and **Enter**.
11. In the ObserveIT Console window click **Next**.
12. In the **Site** field select **ObserveITWebConsole**.
13. In the **Application Pool** select **ObserveITWebConsole**. Click **Next**.
14. Opt-out of the anonymous data usage submission if required.

    Choose whether you opt-out of ObserveIT collecting anonymous usage data of the Web Console use.
15. In the **Server** field enter the details of the SQL server, in the following format:

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

    For example: `SQLsrv.test.lab\ObserveIT,1433`
16. Click the **Windows Authentication** radio button and enter the password for the current account – the ObserveIT Service Account - in the **Password** field. Click **Test Connection**.

    If the test is successful, a success message displays, and the **Next** button becomes available.
17. Click **Next**. The installation begins.
18. After successful installation, click **Close**.

Installing the Web Management Console (Automatic)
To work with ObserveIT RESTful APIs, SQL Native Client is required.

1. To install the SQL Native Client, download

   https://download.microsoft.com/download/F/E/D/FEDB200F-DE2A-46D8-B661-D019DFE9D470/ENU/x64/sqlncli.msi.
2. After downloading, execute **sqlncli.msi** , and follow the Wizard to complete the installation.

Installing the Web Console

Open PowerShell as administrator and paste the following commands, substituting the relevant location.

The example below assumes the ObserveIT installer is located under the C:\Temp\ObserveIT-_Setup_v7.8.2.270 path.

After executing the commands bwlow, the installation wizard will start – just follow the prompts.

```
Start-Process "C:\Temp\ObserveIT_Setup_v7.8.2.270\Web\PreRequisite_nodeServices.exe" -Wait

Start-Process "C:\Temp\ObserveIT_Setup_v7.8.2.270\Web\sqlncli-2012-64-QFE.msi" -Wait

iisreset /stop

Get-Service WAS | Start-Service

Start-Process msiexec -ArgumentList '/i', "C:\Temp\ObserveIT_Setup_v7.8.2.270\Web\WebConsole\ObserveIT.WebConsoleSetup.msi", '/norestart', 'EXTRACTMICROSERVICES=True', '/l*v ObserveITWebConsole_setup.txt' -Wait

iisreset /start
```

Installing the SQL Native Client

(Manual)

1. Download the file: https://download.microsoft.com/download/F/E/D/FEDB200F-DE2A-46D8-B661-D019DFE9D470/ENU/x64/sqlncli.msi.
2. After downloading, execute the sqlncli.msi file, and follow the wizard to complete the installation.

(Powershell - Automatic)

Open PowerShell as administrator and paste the following commands to execute above steps automatically.

The below command assumes the ObserveIT installer is located under the `C:\Temp\ObserveIT-_Setup_v7.8.2.270` path. After the execution of below command, the installation wizard starts – just follow the prompts.

```
Start-Process "C:\Temp\ObserveIT_Setup_v7.8.2.270\Web\PreRequisite_nodeServices.exe" -Wait

Start-Process "C:\Temp\ObserveIT_Setup_v7.8.2.270\Web\sqlncli-2012-64-QFE.msi" -Wait

iisreset /stop

Get-Service WAS | Start-Service
```

```
Start-Process msiexec -ArgumentList '/i', "C:\Temp\ObserveIT_Setup_
v7.8.2.270\Web\WebConsole\ObserveIT.WebConsoleSetup.msi",
'/norestart', 'EXTRACTMICROSERVICES=True', '/l*v ObserveITWebConsole_
setup.txt' -Wait

iisreset /start
```

Verifying the Web Management Console installation

1. Connect to the ObserveIT Web Console machine.
2. Open the **Start** menu and type **Run**. **Enter**.
3. Type **`%userprofile%\AppData\Local\Temp`**. **Enter**.
4. Locate `WebConsole_CA_Log.txt` file. Double-click the file to open it.
5. Open the Find dialog. (Press CTRL+F on the keyboard.) Find **RegisterWebConsole**.
6. Locate the following line: **RegisterWebConsole: Done**.

If the line does not exist or the word Done does not exist – the installation failed. Re-check the installation requirements, particularly the permissions for the SQL logins created previously in this guide.

OBTAINING A COMMERCIAL LICENSE

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

Using a Full Paid License (Enterprise version)

This license is generated at the customer's request by ObserveIT's support staff, and represents the number of Agents (monitored servers) that were purchased by the client.

If you are installing ObserveIT for a client that has not yet received the full paid license, you can temporarily use the free time-limited license, and later upgrade the license to the paid one.

Some full paid licenses have a time limit. If a license has a time limit, a notification is displayed at the top of the screen in the Web Console showing the number of days left till the expiration date, and a hyperlink to contact the ObserveIT website at: http://www.observeit.com/request-pricing in order to request a license extension. If a time-limited license is due to expire in less than 30 days, the message will appear highlighted in the Web Console.

To obtain and activate a Commercial License

1. Go to the ObserveIT website: http://www.observeit.com/request-pricing.
2. Fill in the customer details and click Submit.

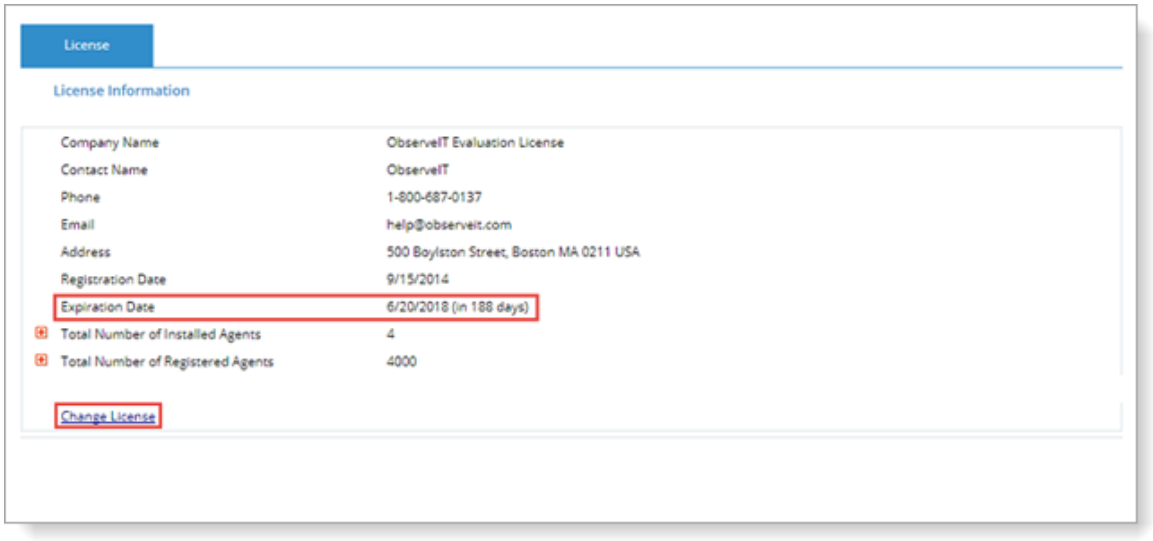
   Make sure that you use a corporate valid email address. Free email hosting addresses, such as Hotmail or Gmail, will not be accepted.

3. Obtain a valid serial number which is generated at the customer's request by ObserveIT's sales staff, and represents the number of Agents (or monitored servers) that were purchased by the client.
4. Insert the serial number using the ObserveIT Web Console.

   When using the default TCP port 4884, use the following URL to connect to the ObserveIT Web Console: http://servername:4884/ObserveIT, where servername is the name or IP of the server on which the ObserveIT Web Console is installed.

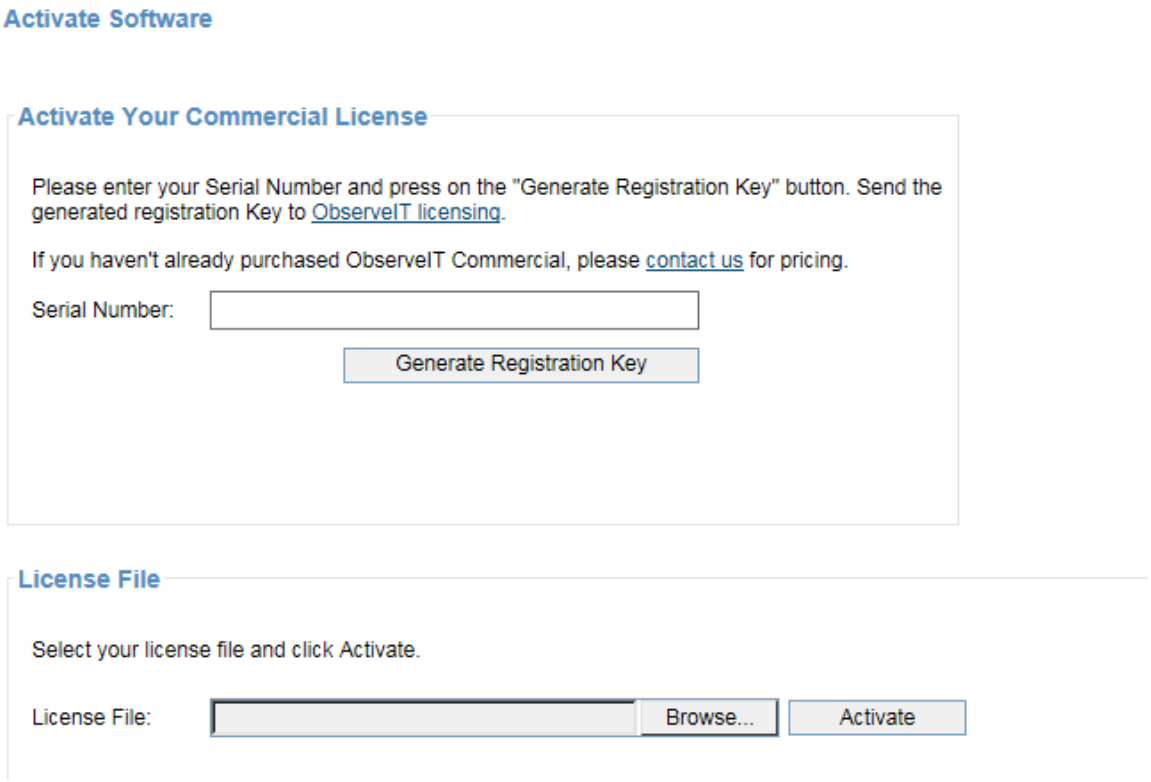
5. In the Web Console, open the License page by selecting Configuration > License.

   Note If the current license has a time limitation, the expiration date and number of days left until the expiration date are included in the License information, as shown below. In addition, a notification appears at the top of the screen with a hyperlink to contact the ObserveIT website at: http://www.observeit.com/request-pricing for details about extending the license.



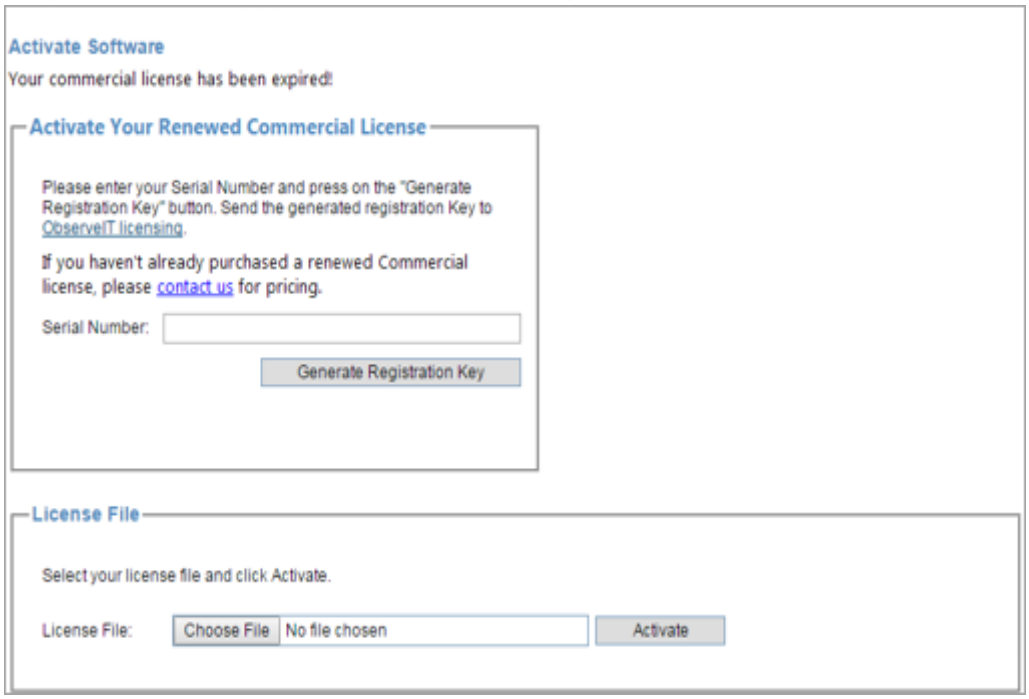
6. Click the Change License link.

   The Activate Software page opens.



Note: If a time-limited license has expired, the Activate Software page will open after you log in to the Web Console warning you that your commercial license has expired and enabling you to activ-

ate your renewed commercial license. For example:



7. Paste the Serial Number and click the Generate Registration Key button.
8. Copy the registration key, paste it into a new email message, and send it back to oit-sales@-proofpoint.com.

   You will receive an automated email containing a license file in the format of a .lic file.
9. In the License File section of the Activate Software page, click Browse to find the license file that was provided to you by the ObserveIT sales team.
10. Click the Activate button to use the specified license file.

    After your product has been activated, the Web Console Login screen will immediately open.

ObserveIT License Types

The License page displays the number of licensed computers.


License Information

Company Name	unix - dev Evaluation License
Contact Name	ObserveIT
Phone	1-800-687-0137
Email	help@observeit.com
Address	500 Boylston Street, Boston MA 0211 USA
Registration Date	9/15/2014
Expiration Date	5/30/2017 (in 78 days)
⊟ Total Number of Installed Agents	10
Workstations	3 / 99
Endpoints	1 / 99
Terminal Services	0 / 99
Unix	6 / 99
Sites	0 / 99
ActiveX	0
⊟ Total Number of Registered Agents	495
Workstations	99
Endpoints	99
Terminal Services	99
Unix	99
Sites	99

- Total Number of Installed Agents shows the number of Agents that were actually installed and used.
- Total Number of RegisteredAgents shows the number of licenses that were purchased by the client.

There are several license types:

- Workstations: Licensed computers running the Workstation type license. This license is for computers running Windows Vista/7/8/10 and Mac operating systems.
- Endpoints: Licensed computers running the Server type license. This license is for computers running Windows Server 2008/2008 R2/2012/2012 R2.
- Terminal Services: Licensed computers running the Terminal Server type license. This license is for computers running Windows Server 2008/2012 with the Terminal Services role installed, or for Windows Server 2008 R2 with the Remote Desktop Services role installed (note that on Windows Server 2008 R2, the Terminal Server role name was changed to Remote Desktop Services).

- Sites: Licensed computers running the Site type license. This license is for computers running any version of Windows operating system.

In this context, "Servers" relates to the operating system type that is installed on the monitored endpoint.

The client can install additional Agents for the type of license that they have, providing that they have available licenses.

For example: If the client bought 50 Workstation licenses and 25 Server licenses, they can install up to 50 Agents running on Windows Vista/7/8/10, and up to 25 Agents running on Windows Server 2008/2008 R2/2012. If the client wants to install an additional Workstation Agent or an additional Server Agent, they cannot do so, because no free Agents remain. However, if the client bought 75 Site licenses, they can install these 75 Agents on any type of operating system (Windows or Unix), as long as the total number of Agents does not exceed the 75 licenses. If the client has already used up all the available licenses for that type of Agent, to install an additional Agent the client must uninstall and unregister one existing Agent (which will free up one license, making it available for a new machine), or purchase at least one additional license based upon the required installation type.

INSTALLING THE SCREENSHOTS STORAGE OPTIMIZER

ObserveIT can store sessions with full video recording in the file system or in the SQL database. Archiving full sessions with many screenshots takes up processor time and bandwidth.

If configured, ObserveIT will store sessions on "Hot" Solid State Drive (SSD) based devices to provide faster session archiving. After sessions stored in the SSD-based Hot storage are closed and signed, the Screenshots Storage Optimizer packs and zips session video on an SSD-based "Warm" storage device. This speeds the archiving process and uses less processor time.After sessions stored in the SSD-based Hot storage are closed and signed, the Screenshots Storage Optimizer packs and zips session video on a "Warm" storage device. This speeds the archiving process and uses less processor time."

The Screenshots Storage Optimizer can be installed anywhere on the same domain as the ObserveIT Application server and Web Console. It must have access to the “Hot” and “Warm” storage folders. More specifically, we recommended installing it directly to the SSD-based "Hot" storage drive where the "Hot" storage folder is configured.

Access to **Advanced Web Console Setup** is required to complete the Screenshot Optimizer installation.

During installation of Screenshot Storage Optimizer version 7.9, you’ll be asked to provide an installation configuration file that contains a token for authentication. This file can be downloaded from **Service Settings** in the **Configuration** tab from the ObserveIT Web Console.

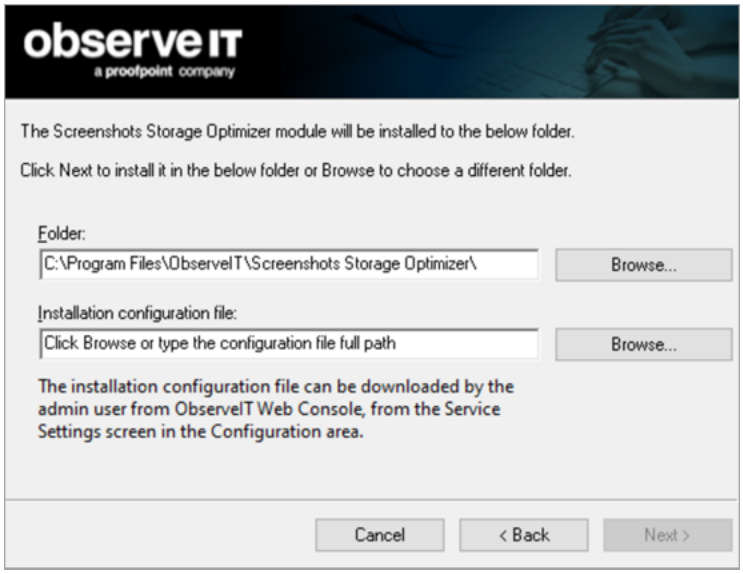
Installing the Screenshot Storage Optimizer (Manual)

1. Navigate to the ObserveIT Web Console (from your Internet broowser), for example `https://OITsrv1/ObserveIT`.
2. When prompted by the ObserveIT Web Console, set up the password for the build-in admin user.
3. From **License File**, click **Choose File** and select your ObserveIT license. Click Activate.
4. In the ObserveIT Web Console, select **Management Console** > **Configuration** and select **Service Settings** on the left.
5. Click the **Download** button for the **Screenshot Storage Optimizer** service.
6. Save the file to the ObserveIT Console server.
7. Connect to the Web Console machine, where you downloaded and extracted the ObserveIT Installer.
8. Make sure to **Run as administrator**.
9. Navigate to ObserveIT_Setupv.xx > Screenshots Storage Optimizer folder and click ScreenshotsStorageOptimizer installer. Follow the Wizard. When prompted to provide the configuration, make sure to use the file saved in Step 6

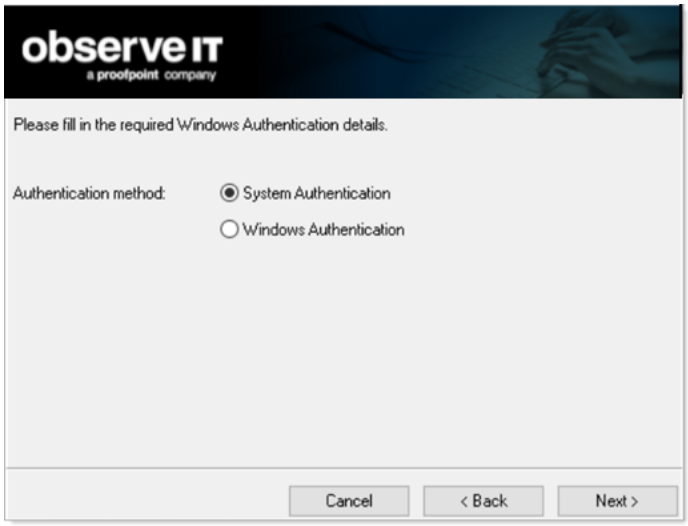
Screenshot Storage Optimizer Wizard

1. Open the wizard using manual or automatic installation.

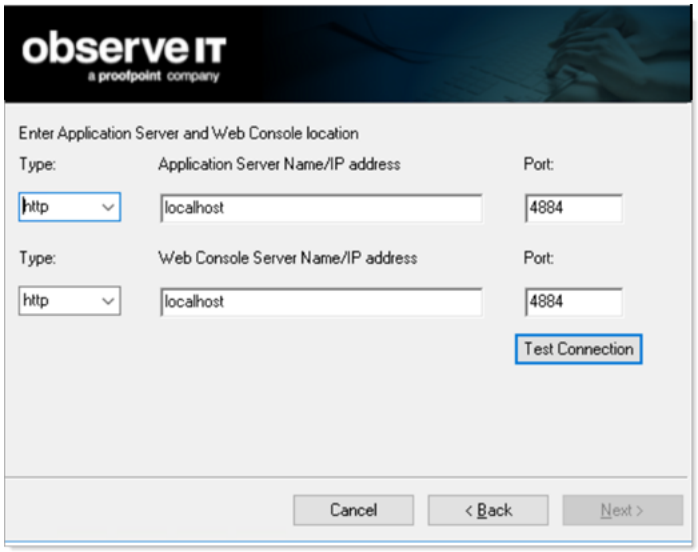
2. Click **Next**.



3. Install in the default folder or browse to the folder you want. Click **Next**.



4. Select the authentication method. Click **Next**.



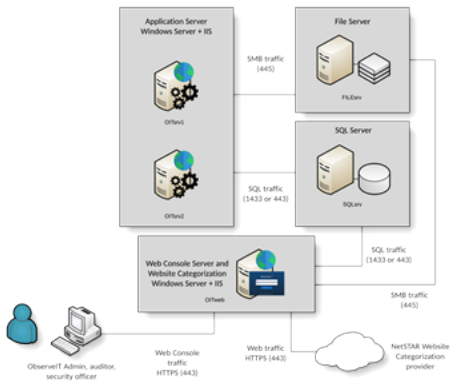
5. Enter the locations. Click **Test Connection**.
6. If the test is successful, click **Next**. The installation starts.
7. When complete, click **Close**.

   When the Wizard is done, continue with Advanced Web Console Setup.

INSTALLING THE WEBSITE CATEGORIZATION MODULE

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

The diagram below shows the configuration including the Web Categorization module.



WEBSITE CATEGORIZATION PREREQUISITES

In order to trigger alerts on Internet browsing, the Website Categorization module must be installed. The Website Categorization module can be installed on the same machine as the Web Console or on a separate dedicated machine (recommended).

Prerequisites for installing the Website Categorization module

- To download the initial data and receive updates directly from NetSTAR cloud service, your machine (that is, the server on which the Website Categorization module is installed), you must have Internet access.

  If you don't have Internet access you can use an HTTP proxy that will provide Internet access and allow the data download.

- Make sure that port number 443 is open, and that the URL https://nsv10.netstar-inc.-com/gcfus/get.cgi (that the module needs to access NETSTAR for initial data download and daily database updates) is not blocked by the Firewall.

- Make sure that the URL https://nsv10.netstar-inc.com/gcfus/get.cgi and http://dss.netstar-inc.-com/ (that the module needs to access NETSTAR for initial data download and daily database updates) are not blocked by the Firewall.

- 12 GB minimum memory requirement. If you install the Website Categorization module on a machine with less than 12 GB RAM, the first time that the module detects the categorized browsed URLs, alerts will not be generated. Upon subsequent browsing, alerts will be generated on these URLs.

- Open port 8000 between the Application server and the Website Categorization.

Installing the Website Categorization Module

The following procedures describe the steps required to install the Website Categorization module for a Custom installation and One-Click Installation. The module can be installed on a separate dedicated machine or executed from the One-Click installation.

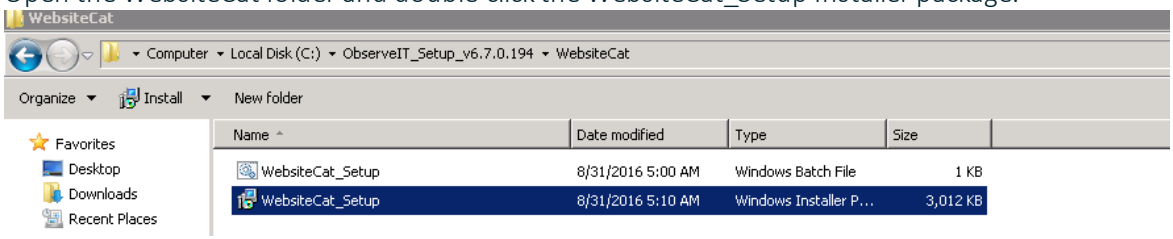
Custom installation installs the Website Categorization module via a separate installation file.

System events related to installation of the Website Categorization module and download of the web categories database are generated by the system. For details, see Event Types.

Installing the module using a Custom installation

1. On the ObserveIT Application Server, open Windows Explorer and browse to the ObserveIT Installation folder.

2. Open the WebsiteCat folder and double-click the WebsiteCat_Setup Installer package.



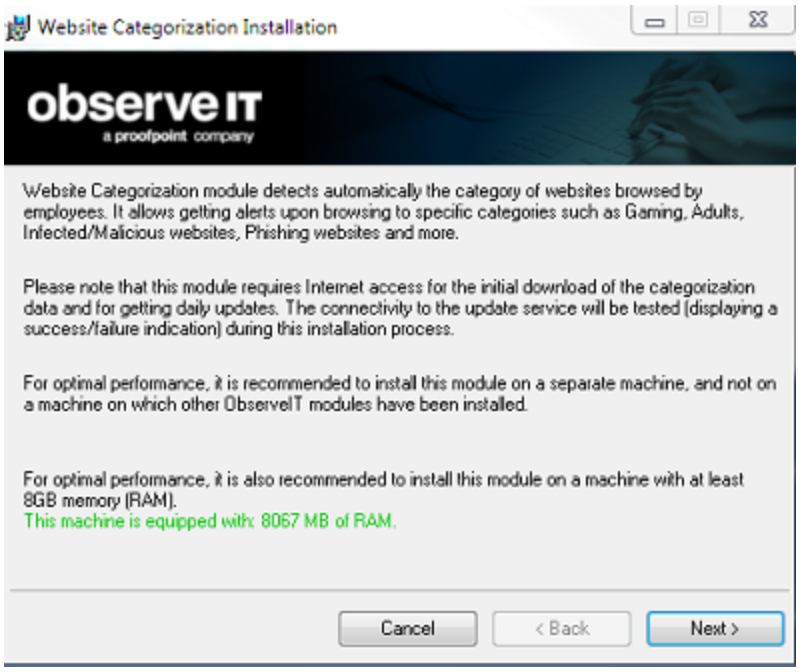
The installation process searches for the installed ObserveIT SQL Server database. The following message is displayed:

Gathering information for installing the Website Categorization module.
Please wait...

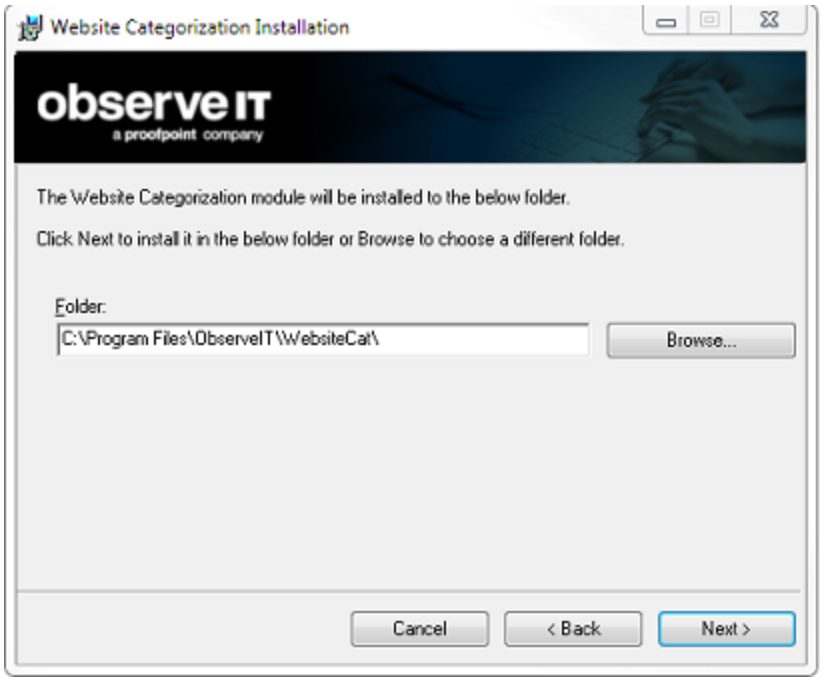
If after gathering information, the ObserveIT database was not found, the following message is displayed:
SQL Server with ObserveIT databases was not found.
Please install ObserveIT databases before running the installation of the Website Categorization module.

The installation checks whether the module is already installed on this machine; if it is, you can repair or remove it.

If the module is not already installed, the Website Categorization Installation wizard opens, displaying the following information.

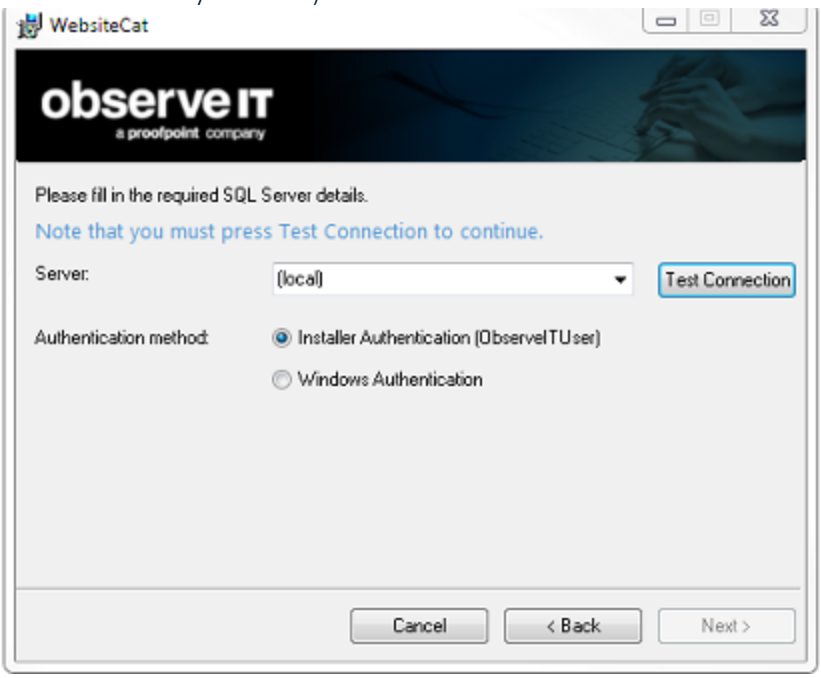


3. To continue, click Next.
   The default installation folder is displayed. If you want to change the default installation folder, click the Browse button and select the required folder.

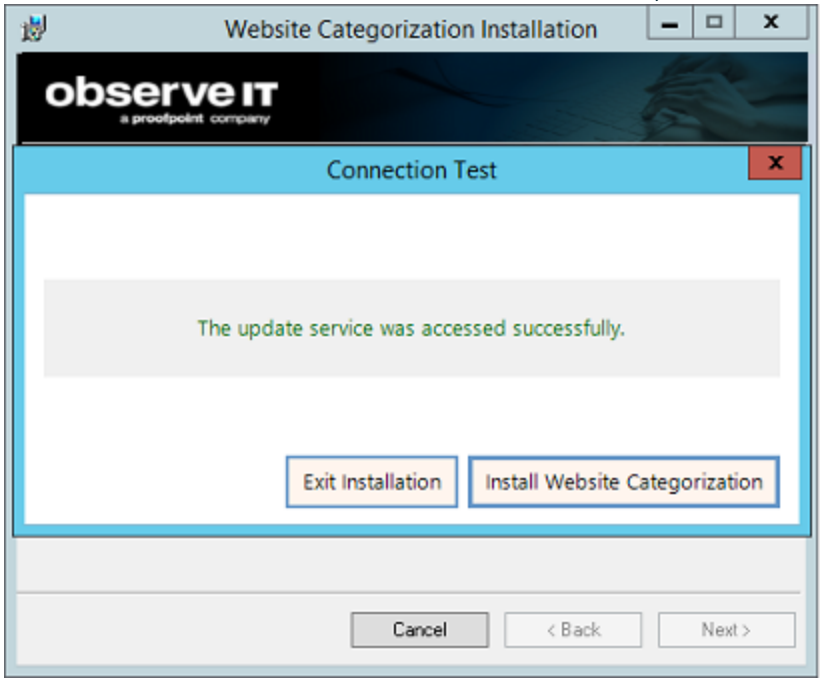


4. Click Next.

5. Select the SQL Server with which the module will interact (the drop-down list includes SQL Servers which are already installed).



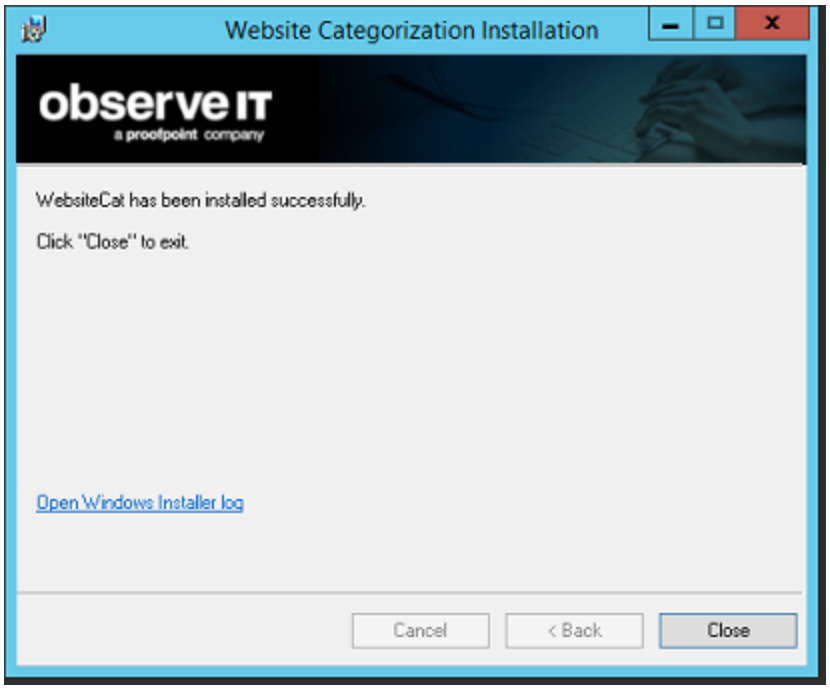
6. Click Test Connection to check the status of connectivity to the server.



7. Click Install Website Categorization to install the module (regardless of success or failure of the connectivity test).
   -Or-

   Click Exit Installation to abort the installation.

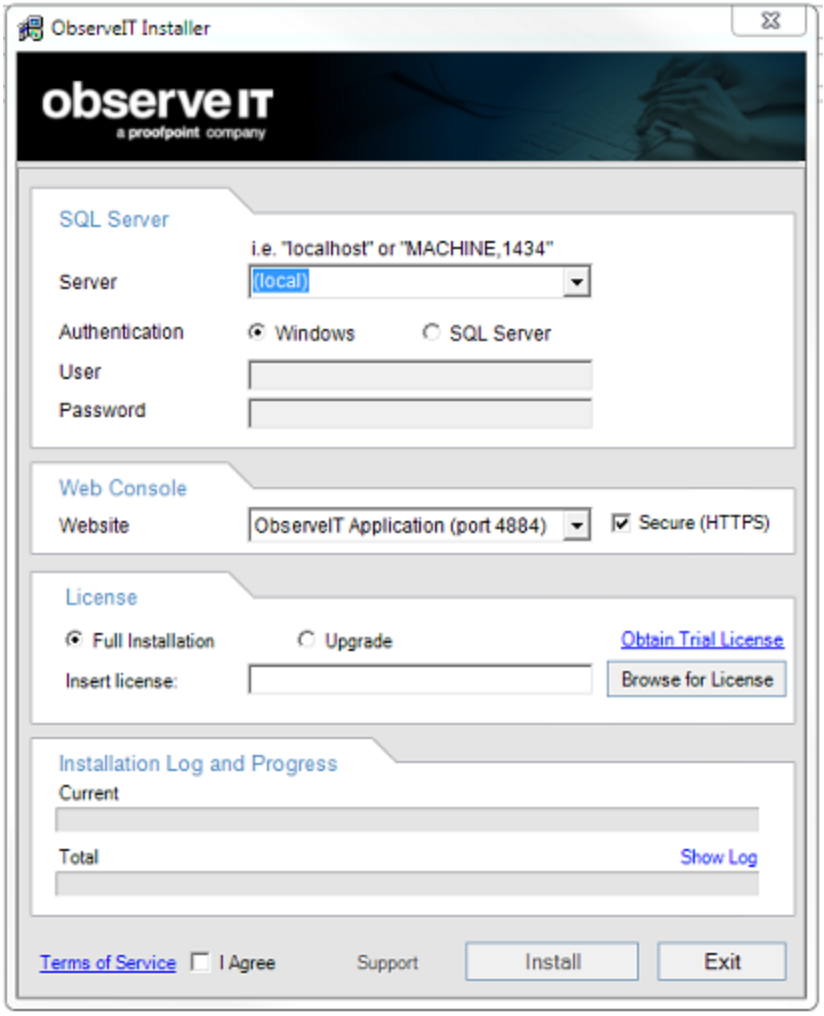
   Upon successful installation of the module, the last screen of the wizard displays:



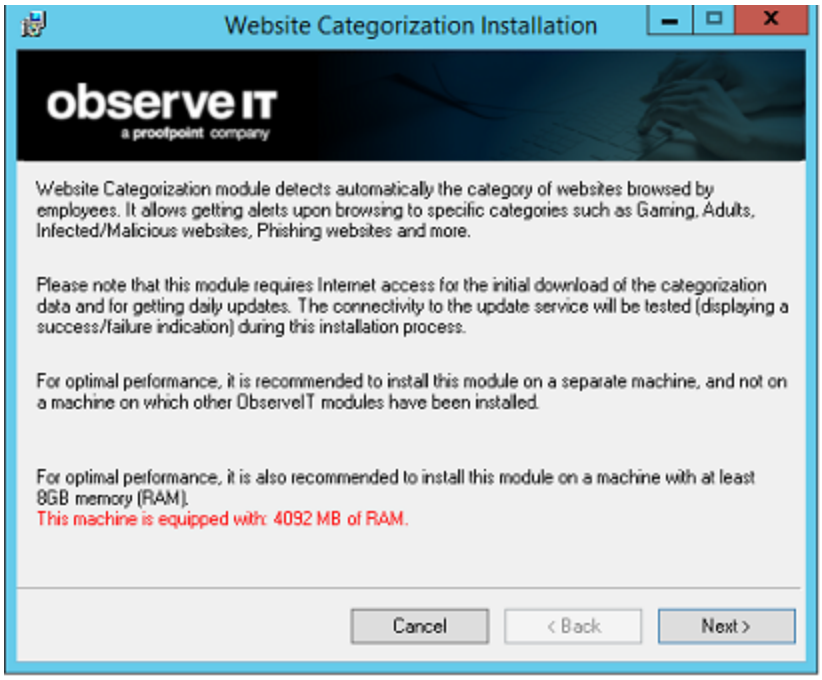
8. Click Close to exit the installation wizard.

Installing the module using a One-Click installation

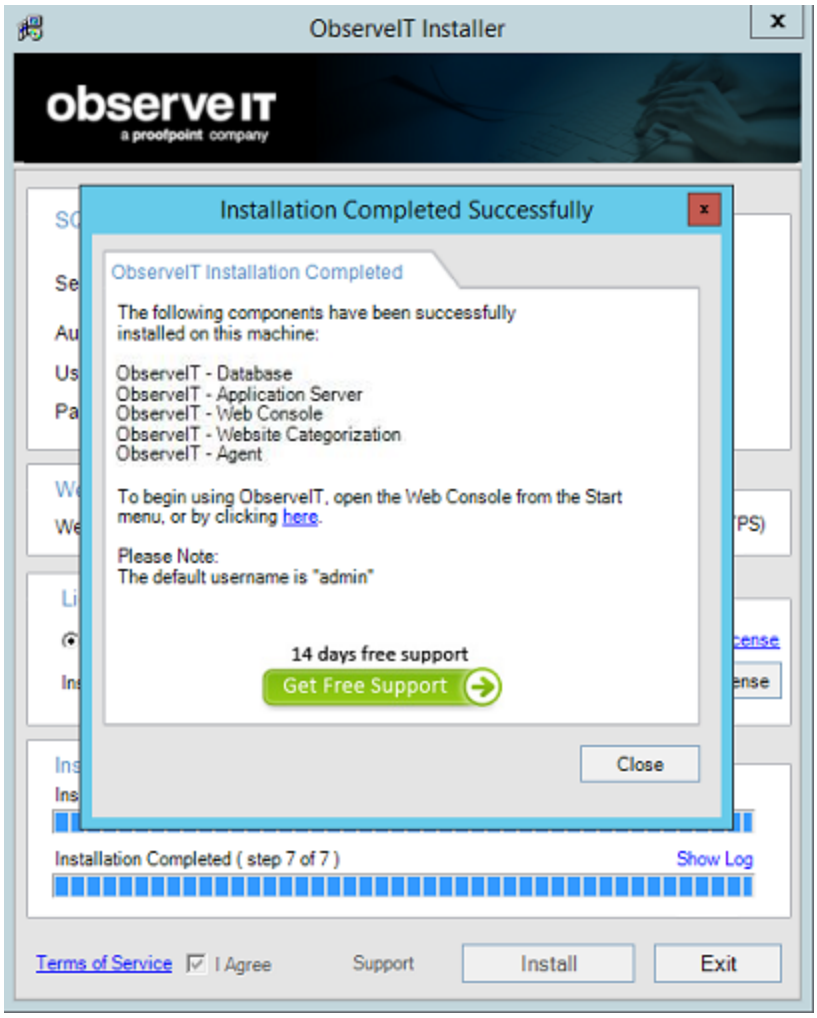
1. Run the the Setup.exe Installer file from the ObserveIT installation folder.
   The ObserveIT main installation screen opens, in which you can configure the settings for SQL Server, Web Console (which includes also the Application Server), License, and Installation Log and Progress. For details, see ObserveIT One-Click Installation.



2. Click Install to begin the installation.
   A window opens, displaying information about the Website Categorization Installation, including the volume of installed memory available on the machine on which the module will be installed. Note that 12 GB is the minimum recommended memory requirement.



3. Click Next to continue.
   Upon successful installation of the module, the last page of the One-Click installation wizard shows a summary of the installed components, including ObserveIT - Website Categorization:



4. Click Close to exit the installation.

Installing the module using PowerShell
Open PowerShell as administrator and paste the following commands to execute automatically.

The below command assumes the ObserveIT installer is located under the `C:\Temp\ObserveIT-_Setup_v7.8.2.270` path. Replace the location with the location of ObserveIT installer you are using.

After the execution of below command, the installation Wizard opens.

```
Start-Process msiexec -ArgumentList '/i', "C:\Temp\ObserveIT-NL_
Setup_v7.8.2.270\WebsiteCat\Websitecat_Setup.msi", '/norestart',
'/l*v ObserveITWebConsole_setup.txt'
```

Related Topics:

CONFIGURING INTERNET PROXY SETTINGS FOR WEBSITE CATEGORIZATION MODULE

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

Website Categorization module does not support proxy authentication.

1. Connect to the ObserveIT Website Categorization module machine.
2. Open the **Start** menu and type **Run**. **Enter**.
3. Right-click the **Notepad** shortcut icon and click **Run as administrator**.

   If prompted **Do you want to allow this app to make changes to your device?**, click **Yes**. Select **File** > **Open**.
4. Navigate to the following folder: `C:\Program Files\ObserveIT\WebsiteCat\Adapters\NetStar\db\etc\`.
5. In Notepad, change the file type from **Text Documents (*.txt)** to **All Files (*.*)**.
6. Locate the **gcf1.conf** file, click it, and click **Open**.
7. In the **# Proxy Settings** section, locate the **PROXY_HOST=** string. Enter the IP address or the FQDN of the proxy server after the = sign.
8. Locate the **PROXY_PORT=** string. Enter the port of the HTTP or HTTPS proxy after the = sign.
9. From the **File** menu, select **Save**.
10. Close Notepad.
11. Open the **Start** menu and type**PowerShell.**.
12. If prompted **Do you want to allow this app to make changes to your device?**, click **Yes**. Select **File** > **Open**.
13. Paste the following command into the PowerShell window and press the Enter key:

```
Get-Service WebsiteCat.Manager,GCF1Service | Restart-Service -Force

&"C:\Program Files\ObserveIT\WebsiteCat\WebsiteCat.Manager.exe" -dw
```

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

VERIFYING THE OBSERVEIT SERVICES IDENTITY

The ObserveIT installation creates four services. When running the ObserveIT installer as the ObserveIT Service Account, the services will be automatically configured to use the ObserveIT Service Account identity.

On the ObserveIT Application Server machine(s) the following service is present:

- ObserveIT Activity Alerts Service

On the Web Console machine, the following services are present:

- ObserveITNotificationService
- ObserveIT Health Monitoring Service
- ObserveIT Analytics Service
- Screenshots Storage Optimizer
- GCF1Service
- WebsiteCat.Manager

Verifying the ObserveIT Alerts Services Identity (Manual)

1. Connect to the ObserveIT Application Server machine.
2. Open the **Start** menu and type **Run**. **Enter**.
3. Type **services.msc**. **Enter**.
4. Find the **ObserveIT Activity Alerts Service** in the list.
5. Verify the **Log On As** column reflects the ObserveIT Service Account identity. If it does not, follow the rest of this procedure. Otherwise, verify the ObserveIT Service Account identity for other ObserveIT services.
6. Right-click the service and click **Properties**.
7. Click the **Log On** tab.
8. Select **This account**. Click **Browse**.
9. Click **Locations** and ensure your Active Directory domain is selected.
10. In the **Enter the object name to select** field, type **OITServiceAccount**. Click **OK**.

11. In the Password and Confirm password fields enter the password for the ObserveIT Service Account user.
12. Click OK. If a message pops up that the user OITServiceAccount has been granted the Log on as a service rights, click OK.
13. Right-click the ObserveIT Activity Alerts Service and click Restart.
14. Perform steps 5-12 on the remaining 3 ObserveIT services – 4 total – named ObserveIT Health Monitoring Service, ObserveIT Notification Service and ObserveIT User Analytics Service.

Verifying the ObserveIT Alerts Services Identity (Powershell - Automatic)
Open PowerShell as administrator and paste the following commands to execute above steps automatically. After the execution of below command, you will be prompted to supply the ObserveIT Service Account credentials. Enter the credentials and press the OK key to continue. All the ObserveIT components will be configured to use the new credentials.

```
function Set-OITAccount ($Credentials){

if (!$Credentials) {

$Credentials = Get-Credential

}

$UserName = $Credentials.GetNetworkCredential().Domain + '\' +
$Credentials.GetNetworkCredential().UserName

$Password = $Credentials.GetNetworkCredential().Password


$OITServices = Get-Service observeit*, screenshot*, websitecat*,
gcf1*

foreach ($Service in $OITServices) {

$Service = $Service.Name

Write-Output "Working service $Service"

$svc_Obj = Get-WmiObject Win32_Service -filter "name='$service'"

$ChangeStatus = $svc_Obj.change($null, $null, $null, $null, $null,

$null, $UserName, $Password, $null, $null, $null)

If ($ChangeStatus.ReturnValue -eq "0")

{Write-host "User Name sucessfully for the service '$Service'"}
```

```
If ($ChangeStatus.ReturnValue -eq "0")

{Write-host "The service '$Service' Started successfully"}

}


foreach ($service in $OITServices) {

Get-Service $Service.Name | Restart-Service

}

Write-Output "Setting credentials for the ObserveIT Application Pool"

Import-Module WebAdministration

Get-Item IIS:\AppPools\ObserveIT* | Set-ItemProperty -name
processModel -value @{userName = "$UserName"; password = "$Password";
identitytype = 3}

Start-Process iisreset -NoNewWindow

}


Set-OITAccount
```

Configuring ObserveIT Installation

To configure ObserveIT installation, complete the following tasks.

- Configuring Your Admin Password
- Obtaining a Commercial License
- Configuring LDAP Settings
- Configuring SMTPSettings
- Configuring Screenshot Data Storage

CONFIGURING THE ADMIN PASSWORD

The first time you access the ObserveIT Web Console, you are prompted to configure the password for the default ObserveIT Admin user account.

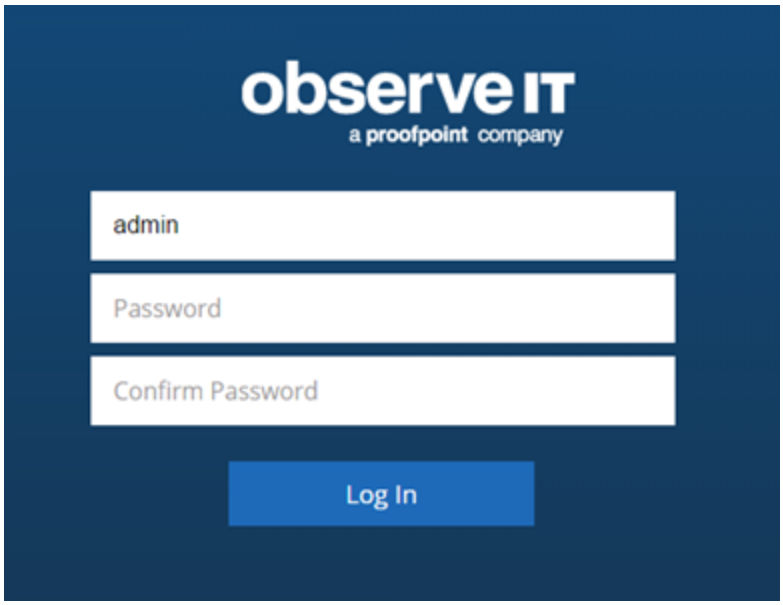
1. Open your preferred Web browser. In the address bar type the URL address of your ObserveIT Web Console in the format:

   https://<WebConsoleServerAddressFQDN>/ObserveIT

   For example:

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

2. The browser window opens and you are prompted to set the password for the admin user.



3. In the **Password** and **Confirm Password** fields enter the password for the ObserveIT Admin user account.

4. Click **Log In**. Your password is now set.

CONFIGURING LDAP SETTINGS

In a Custom Installation, you must manually configure the LDAP connector settings.

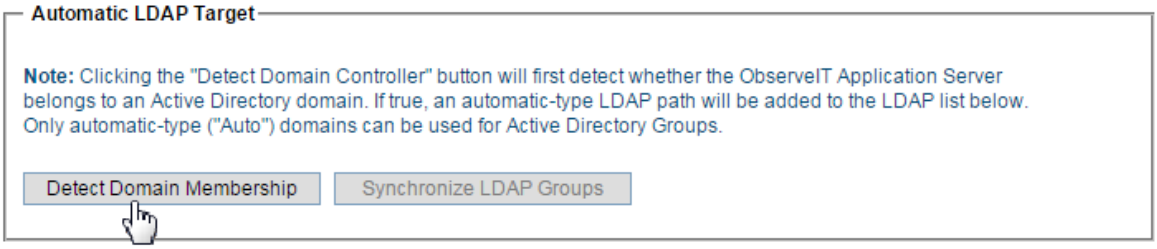
The LDAP connector enables usage of Active Directory-based users and groups for various system settings, such as:

- Using Active Directory with Console groups
- Integrating Active Directory users with Secondary Authentication
- Filtering Active Directory groups by Secondary Authentication
- Displaying logon messages to specific Active Directory users

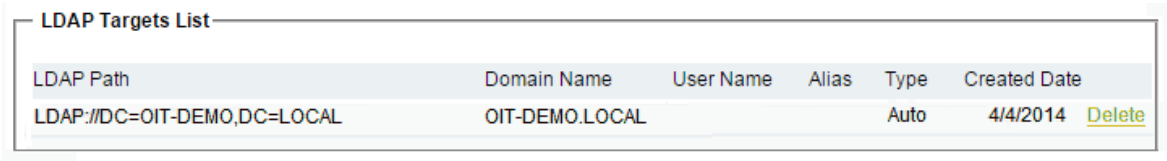
- Recording/no recording Active Directory users and groups
- Integrating DNS for Agent auto-configuration
- Using Active Directory users when detecting Identity Theft

1. From the the ObserveIT Web Console, select **Management Console**. Then select **Configuration**> **LDAP Settings**.

2. From the **LDAP Settings** tab, in the **Automatic LDAP Target** area, select **Detect Domain Membership**.



If the Domain path and credentials are valid, the connection will be added to the LDAP Target List. The LDAP Target type will be set to **Auto**.



The Detect Domain Membership button is grayed out and cannot be used again, because the endpoint can be a member of only one domain.

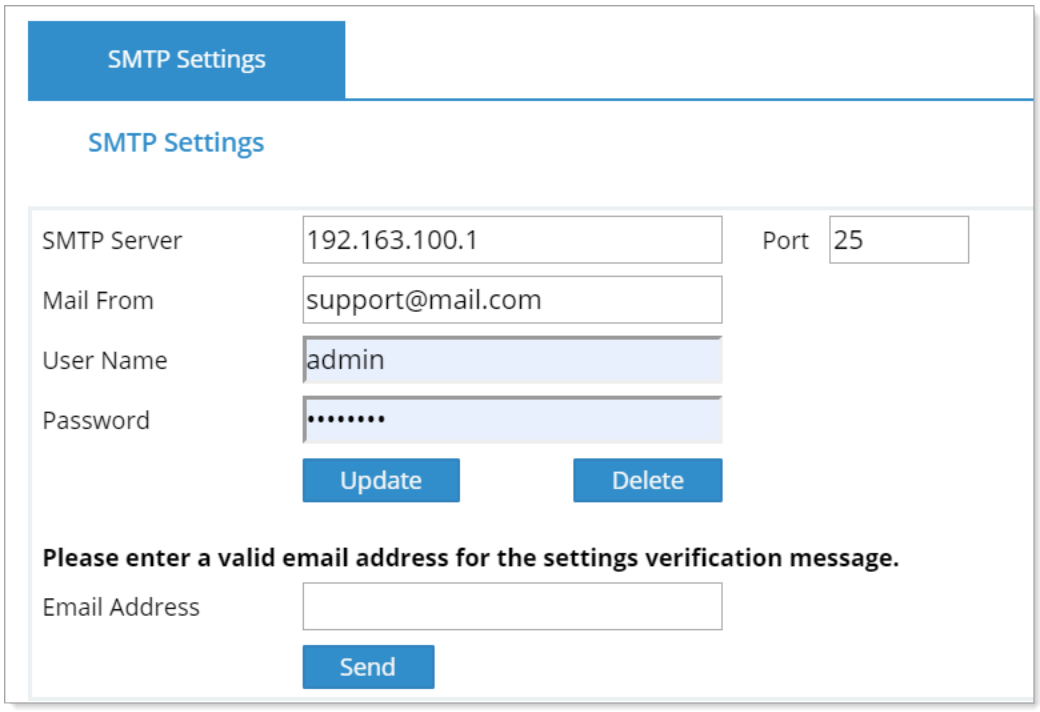
CONFIGURING SMTP SETTINGS

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

The Web Console is responsible for sending emails from ObserveIT. Allow the Web Console to send email via your email server.

1. Log into the ObserveIT Web Console.

2. Select **Management Console** at the top of the screen, select **Configuration** > **SMTP Settings**.



3. In the **SMTP Server** field, enter the FQDN of your email server. Adjust the **Port** field value if necessary.
4. In the **Mail From** field, enter the email address which will identify the sender of ObserveIT notifications.
5. Optional: In the **User Name** and **Password** fields enter credentials for the account authorized to send emails using the specified email server.
6. Click **Update** to save the details.
7. To verify ObserveIT can successfully send emails, enter a working email address in the **Email Address** field and click **Send**.

   If the verification is successful, a **Successfully Verified** message appears and you should receive an email from an email address specified in the **Mail From** field.

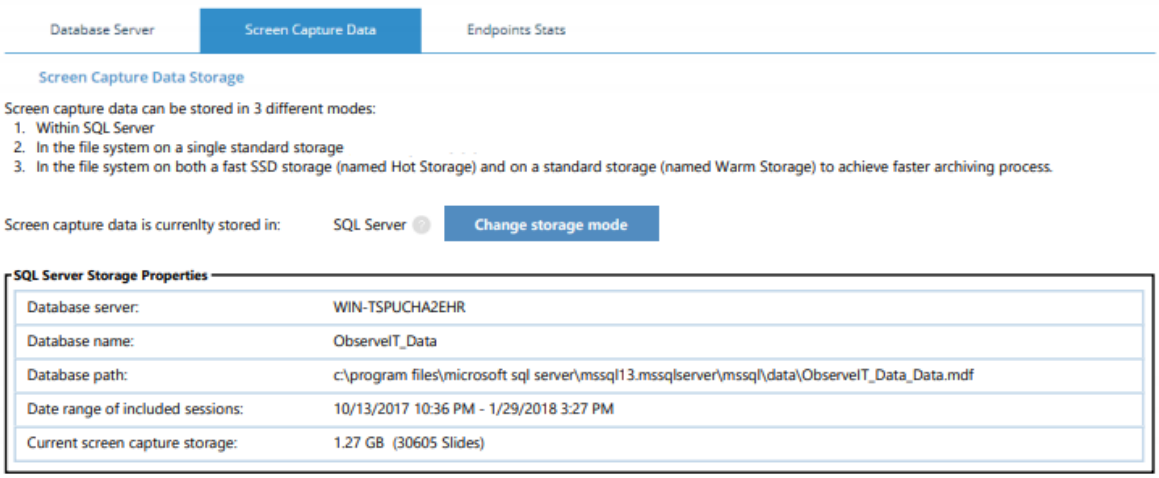
CONFIGURING SCREEN CAPTURE DATA STORAGE

Screen capture data takes up more storage space than metadata and is configured separately.

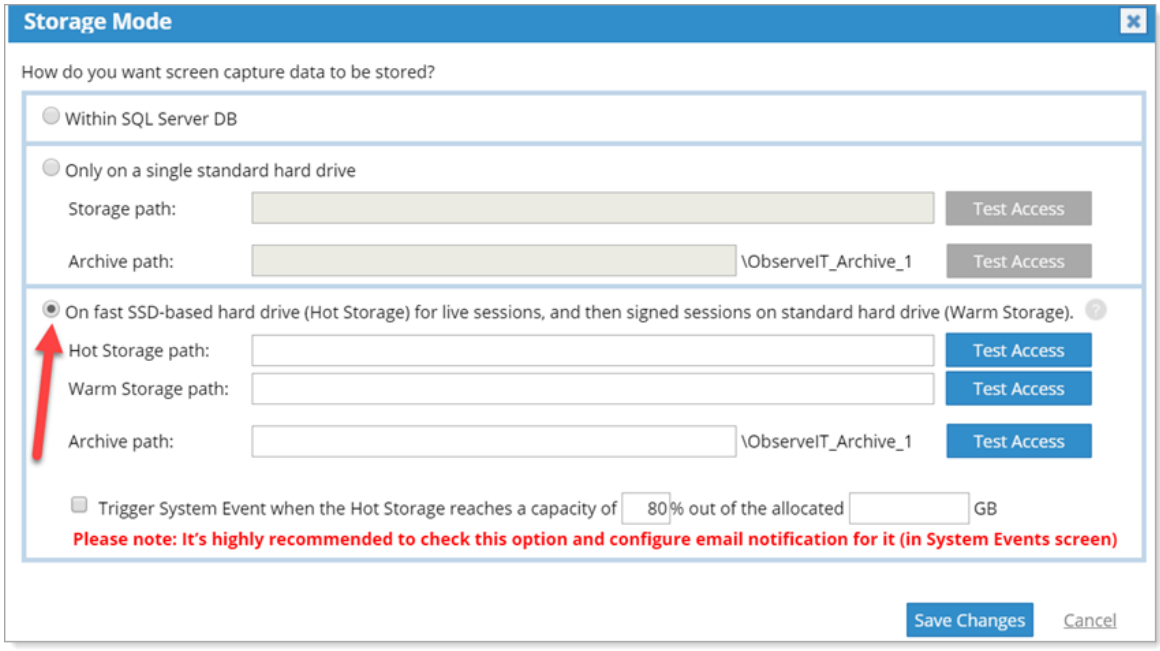
For most deployments, it is essential to store the screenshot data directly on a file system (such as NTFS).

This procedure describes how to move the default storage location to the file system.

1. From the ObserveIT Web Console, navigate to Configuration > Storage.
2. Select the Screen Capture Data tab.



3. Select Change storage mode. When prompted about changes, click **Yes**.



4. Select **On fast SSD-based hard drive (Hot Storage) for live sessions, and then signed sessions on standard hard drive (Warm Storage)**.
5. Specify the Hot Storage path, the Warm Storage path, and the Archive path.

6. Click **Test Access** for each path to verify ObserveIT can successfully access each path.
7. Click **Save Changes**.

Configuring Traffic Security

This topic describes how to encrypt data in transit.

By default, ObserveIT Agents communicate with the ObserveIT Application Server by using the HTTP protocol.

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

Encryption can be enabled to further secure the communications:

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

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

REQUIREMENTS

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

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

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

- Obtain a digital certificate.
- Encrypt the traffic from ObserveIT Agents to ObserveIT Application Server.
- Configure ObserveIT Agent for Windows to use SSL.
- Configure the ObserveIT Agent for Mac to use SSL.
- Configure the ObserveIT Agent for Unix/Linux to use SSL.

CONFIGURING OBSERVEIT APPLICATION SERVER FOR DATA TRANSIT ENCRYPTION

To configure ObserveIT Application server for data in transit encryption, you need to set the protocol to HTTPS, not HTTP. In addition, you need SSL certification.

1. Connect to the ObserveIT Web Console machine and if you need, request or create a digital certificate.
2. From the **Start** menu and type **Run**. **Enter**.
3. Type IIS, select the **Internet Information Services (IIS) Manager**. **Enter**.
4. From the menus, expand **Sites**.
5. Right-click the ObserveITApplication website, and select **Edit Bindings.**
6. Click **Add**.
7. Change the value in the **Type** field from **http** to **https**.
8. Make sure the value for **Port** field is set at **443**.
9. Under SSL certificate select the certificate you have created or acquired.
10. Click **OK** to create the bindings. Click **Close** to close the window.

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

CONFIGURING WINDOWS AGENTS TO USE SSL

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

New ObserveIT Agent Deployment

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

- During the ObserveIT Agent deployment, in the **Enter Application Server Location** screen, set the value for **Type** field to **https**. Specify the server's FQDN in the **Server Name** field.

  If a non-default HTTPS port is used, specify it in the Port field.

- If using self-signed certificates, ensure the certificates are trusted by both parties. You can skip this step if certificates from Enterprise Certificate Authority are used.

- If a firewall is enabled on the ObserveIT Application Server, ensure the correct incoming port is allowed in the firewall settings.

Existing ObserveIT Agent Deployment

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

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

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

   ```
   Use ObserveIT

   select * from  dbo.ServerConfiguration

   WHERE PropertyId = 4
   ```

8. Click **Execute** to run the query.
9. Paste the following code into the query window, where **NEW_APP_SERVER_URL** is the new

address, with the HTTPS connectivity specified, and **OLD_APP_SERVER_URL** is the address currently in use.

```
Use ObserveIT

UPDATE dbo.ServerConfiguration

SET PropertyValue = '<NEW_APP_SERVER_URL>'

WHERE PropertyId = 4

AND PropertyValue = '<OLD_APP_SERVER_URL>'
```

For example:

```
Use ObserveIT

UPDATE dbo.ServerConfiguration

SET PropertyValue = 'https://oitsrv1.oit-
demo.local:10443/ObserveITApplication'

WHERE PropertyId = 4

AND PropertyValue = 'http://oit-srv1.oit-
demo.local:4884/ObserveITApplication'
```

10. Click **Execute** to run the query

CONFIGURING A MAC AGENT TO USE SSL

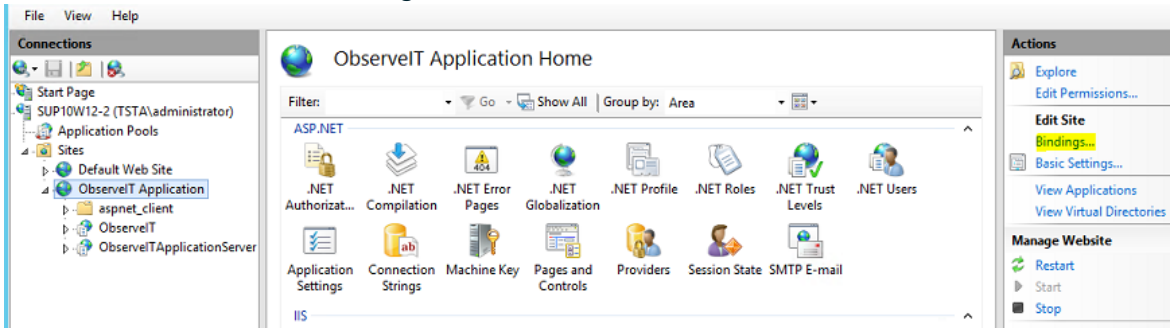
This procedure describes how to install a trusted internal CA certificate on a Mac.

OBTAINING AND IMPORTING A CERTIFICATE

If you do not already have a trusted internal CA certificate, perform the following procedure to obtain and import the certificate.

To obtain and import certificates

1. Go to Start > run and enter inetmgr.

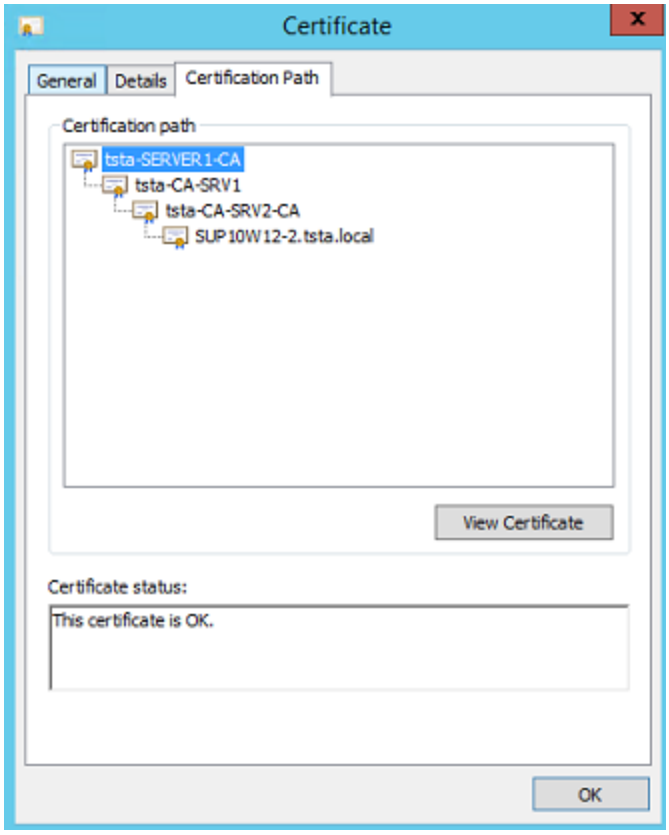


2. Go to ObserveIT Application, and select Bindings.

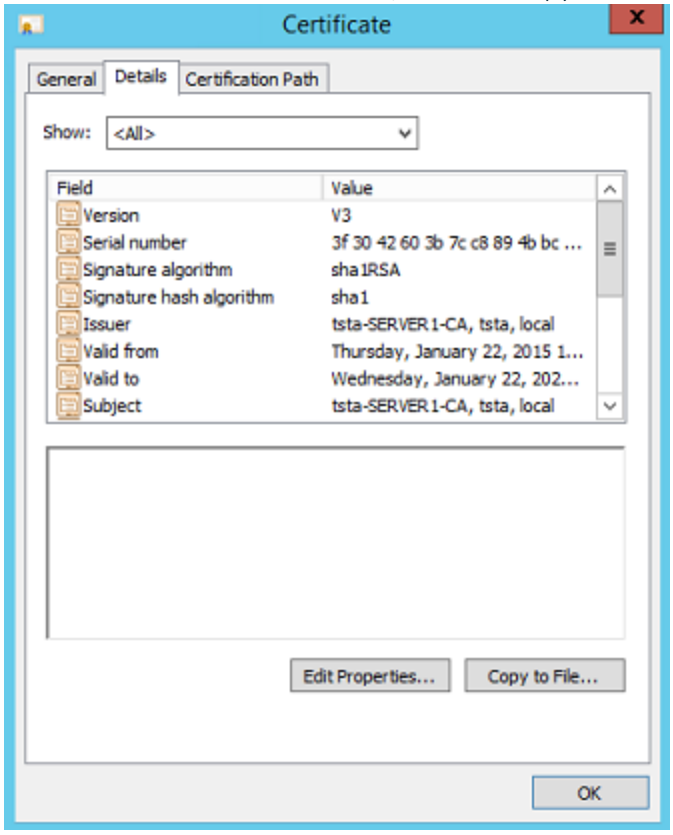
3. In the Site Bindings dialog box, select the https protocol and click Edit.

4. In the Edit Site Bindings dialog box, click View.

5. In the Certificate dialog box, select the Certification Path tab, select the root CA certificate, and click View Certificate.



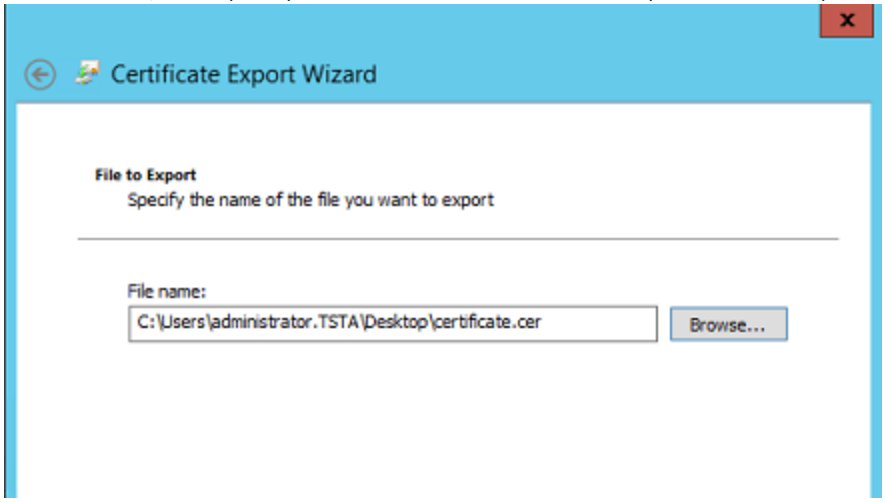
6. Select the certificate's Details tab, and click Copy to File.



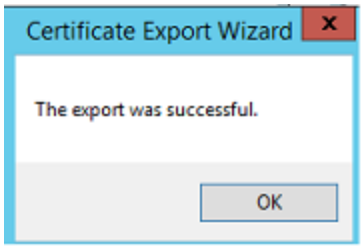
7. In the Certificate Export Wizard that opens, click Next.

8. Select the Base-64 encoded X.509 (.CER) format option, and click Next.

9. Click Browse, and specify the name of the file to which you want to export the certificate.



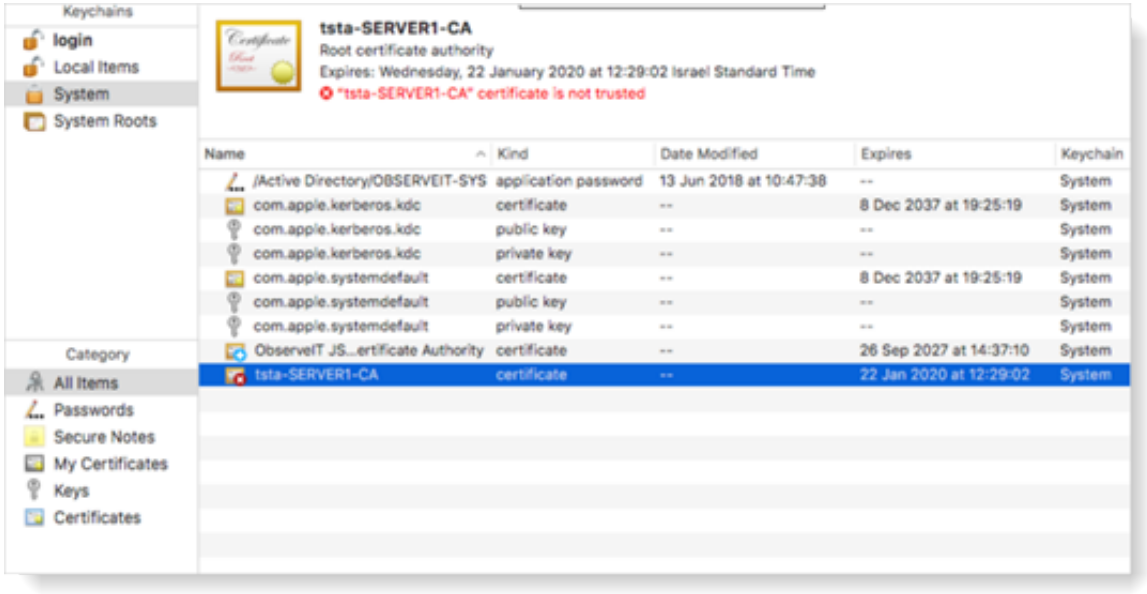
10. Click Next, and then click Finish to close the Certificate Export Wizard.
11. In the message box stating that the export was successful, click OK.



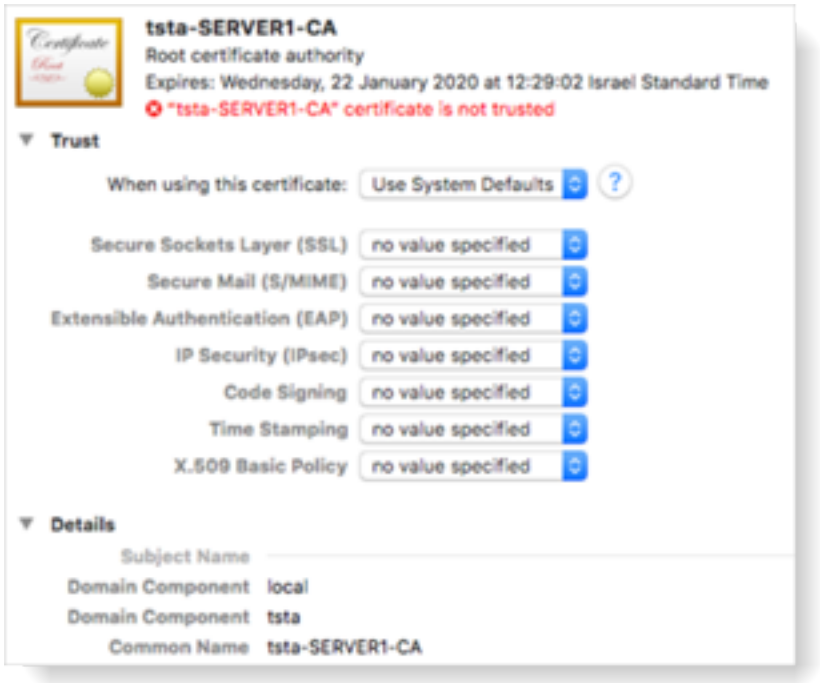
COPY THE CERTIFICATE TO YOUR MAC

1. Copy the Certificate to your Mac target server.
2. Select Keychain Access  .

   The list of certificates displays. A red X indicates that the certificate is not trusted, for example, *tsta-SERVER1-CA* in the list below.



3. Select the certificate you want to make Trusted.



4. Set the Trust level according to your company's requirements. At a minimum, you must select **Always Trust** for the **When using this certificate** option.

CONFIGURING A UNIX LINUX AGENT TO USE SSL

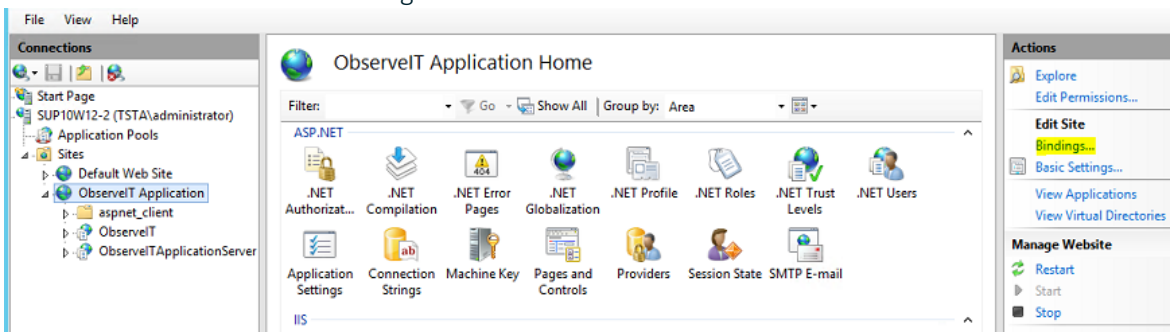
This procedure describes how to install a trusted internal CA certificate on a Unix/Linux server.

OBTAIN AND IMPORT A TRUSTED INTERNAL CA CERTIFICATE

If you do not already have a trusted internal CA certificate, perform the following procedure to obtain and import the certificate.

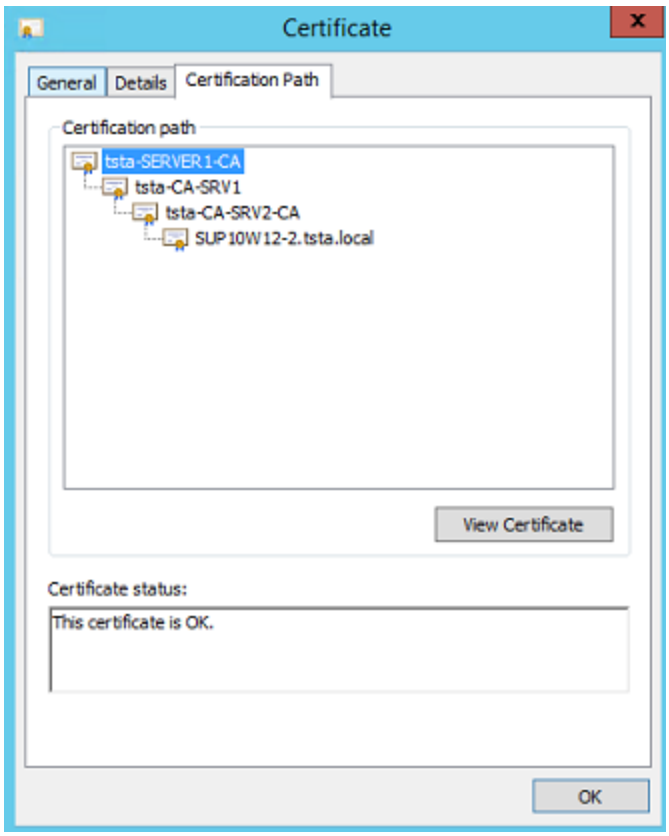
To obtain and import certificates

1. Go to Start > run and enter inetmgr.

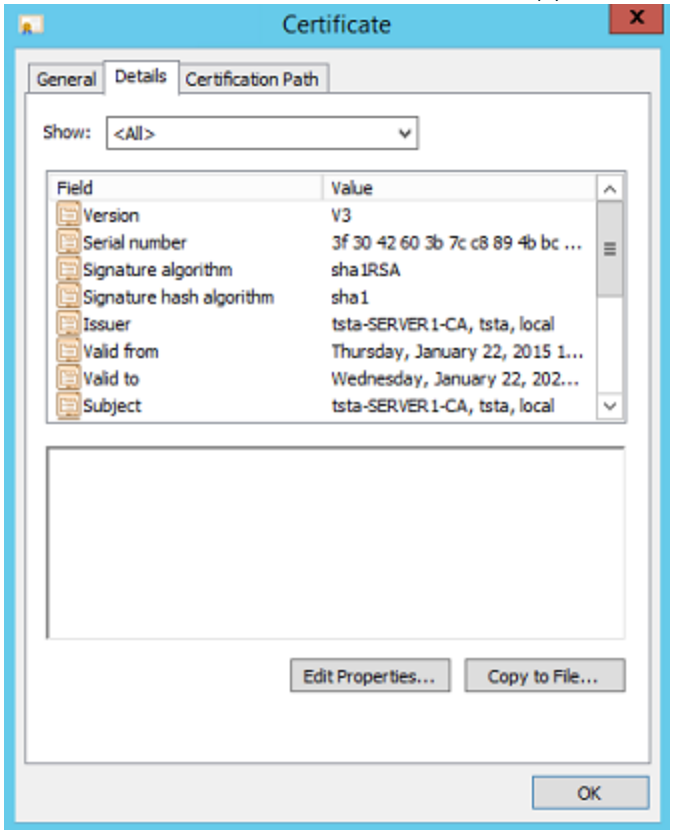


2. Go to ObserveIT Application, and select Bindings.
3. In the Site Bindings dialog box, select the https protocol and click Edit.
4. In the Edit Site Bindings dialog box, click View.
5. In the Certificate dialog box, select the Certification Path tab, select the root CA certificate, and

click View Certificate.



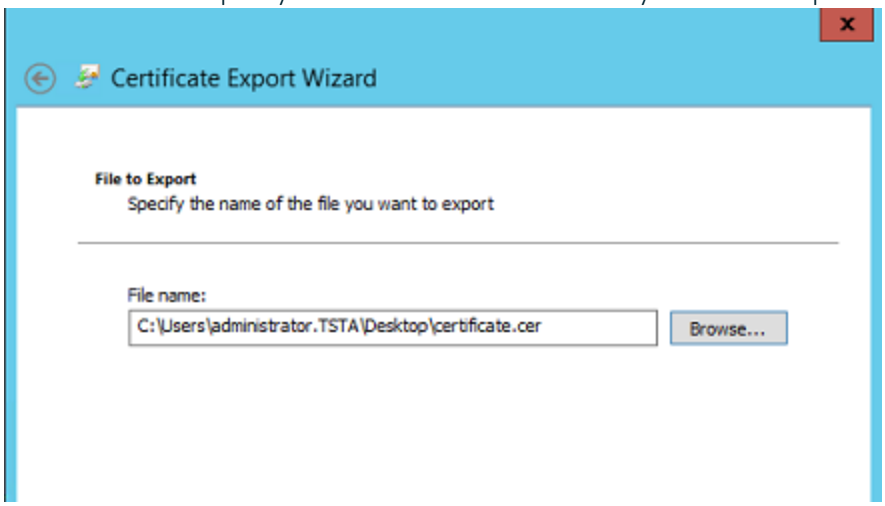
6. Select the certificate's Details tab and click Copy to File.



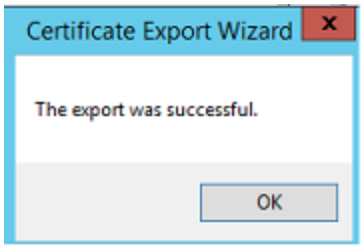
7. In the Certificate Export Wizard that opens, click Next.

8. Select the Base-64 encoded X.509 (.CER) format option, and click Next.

9. Click Browse and specify the name of the file to which you want to export the certificate.



10. Click Next and then click Finish to close the Certificate Export Wizard.
11. In the message box stating that the export was successful, click OK.



COPY THE CERTIFICATES TO A LINUX SERVER

Prerequisite: See Locating the Certificates for information about verifying and locating a certificate and how to locate the /certs directory.

1. You must transfer the exported certificates to the /certs directory of the appliance, using SCP/FTP or any other protocol.
2. If you are transferring the files using WinSCP, the file permissions might have changed. To verify the file permissions, run the command: ls -la
   The output should look like: -rw-r--r--.

If the output looks different, change the file permissions so that "user", "group", and "other" will have read permissions. Run the following command to make the changes: chmod w+r or chmod o+r.

To enable OpenSSL to identify the certificates, link them as follows

1. Extract the certificate's hash, and use it as a symbolic link to the certificate:
   ln -s certificate.pem 'openssl x509 -in certificate.pem -noout -hash'.0

   Or

   ln -s certificate.cer `openssl x509 -in certificate.cer -noout -hash`.0

2. Verify the certificate installation by running the command:
   openssl verify certificate.pem

   openssl verify 3ee7e181.0

Configuring Simple Recovery Mode

Simple recovery mode is the recommended ObserveIT database mode for a stand-alone, non-clustered SQL server. Simple recovery mode may be configured manuallyor may be configured automatically via a query

CONFIGURING SIMPLE RECOVERY MODEL FOR THE OBSERVEIT DATABASES ON THE SQL SERVER

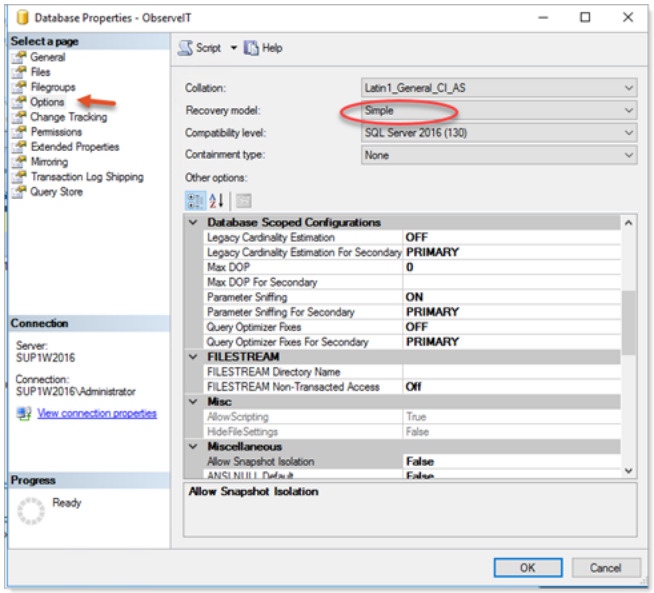
A recovery model is a database property that controls how transactions are logged, whether the transaction log requires (and allows) backing up, and what kinds of restore operations are available. It automatically reclaims log space to keep space requirements small, essentially eliminating the need to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

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

1. Connect to the SQL server or to a computer with **SQL Server Management Studio** installed.
2. Open **SQL Server Management Studio**.
3. Type in the SQL server's FQDN or IP address into the **Server name** field.
4. Choose **Windows Authentication** if your account has sysadmin permissions on the SQL server.

Otherwise, choose **SQL Server Authentication** and log in with a sysadmin-level account.

5. Click **Connect**.
6. From the menus on the left, expand **Database**s.
7. Right-click the ObserveIT database and select **Properties**.
8. From **Select a page**, select **Options**.
9. From **Recovery model** options. select **Simple**.



10. Click **OK**.

Repeat these steps for each ObserveIT database.

CONFIGURING SIMPLE RECOVERY MODEL FOR THE OBSERVEIT DATABASES VIA SQL QUERY

1. Connect to the SQL server or to a computer with **SQL Server Management Studio** installed.
2. Open **SQL Server Management Studio**.
3. Type in the SQL server's FQDN or IP address into the **Server name** field.
4. Choose **Windows Authentication** if your account has sysadmin permissions on the SQL server.

Otherwise, choose **SQL Server Authentication** and log in with a sysadmin-level account.

5. Click **Connect**.
6. Select **File** > **New** > **Query with Current Connection**.
7. Paste the following code into the New query window:

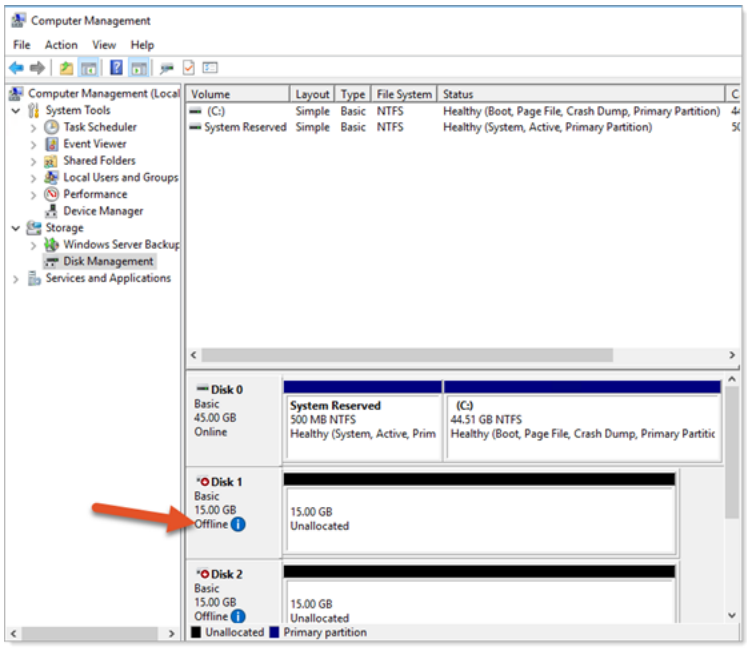
```
USE master ;

ALTER DATABASE ObserveIT SET RECOVERY SIMPLE ;

ALTER DATABASE ObserveIT_Analytics SET RECOVERY SIMPLE ;

ALTER DATABASE ObserveIT_Archive_1 SET RECOVERY SIMPLE ;

ALTER DATABASE ObserveIT_Archive_Template SET RECOVERY SIMPLE ;

ALTER DATABASE ObserveIT_Data SET RECOVERY SIMPLE ;
```

8. Click **Execute** to run the query.

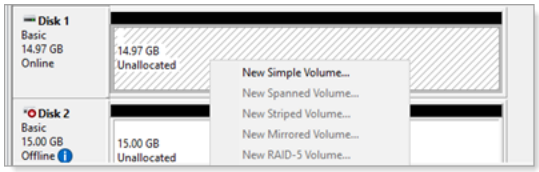
Formatting NTFS

When using an NTFS volume for ObserveIT image store, the drive containing the images may become fragmented and reach a limit where no further file operation will be available. To avoid this condition, format the drive with support for large file size records.

1. Connect to the computer acting as the ObserveIT file share.
2. Open the **Start** menu and type in **COMPMGMT.MSC**. Press the **Enter**.
3. In the **Computer Management** window, expand **Storage** , and click **Disk Management**.
4. Find the new disk in the list. Usually, it is the only one with the status **Offline**.



5. Right-click the disk and select **Online**.
6. Right-click the disk again and select **Initialize Disk**.
7. Click the **GPT (GUID Partition Table)** radio button and click **OK**.
8. Right-click the partition and select.



9. Click **Next**.Make sure maximum the values specified in the Maximum disk space in MB and Simple volume size in MB are equal. Click **Next**.
10. Assign an appropriate drive letter. Click **Next**.
11. Click the **Format this volume with the following settings** radio button and select **NTFS**.
12. Set the Allocation unit size:
    - 4096 for image storage.
    - 64KB for SQL database.

13. Assign an appropriate volume label at the Volume label field.
14. Make sure **Perform a quick format** checkbox is checked.
15. Click **Next** and review the settings. Click Finish.
16. Click the **Start** menu and type in **RUN**.
17. Type in CMD. Right-click the Command Prompt shortcut and click Run as administrator.
18. If prompted ***Do you want to allow this app to make changes to your device?*** click **Yes**.
19. Type in the following command:

    format <driveletter>: /FS:NTFS /Q /X /L /A:4096

    where <driveletter> is the letter of the volume you specified
20. If asked to specify current volume name, enter it and press **Enter**.
21. At the **Proceed with format** prompt type in **Y** and press **Enter**.
22. At the **Volume** label prompt enter a volume label, if required, and press **Enter**.
23. At this point the volume is formatted correctly.
24. Type **EXIT** and press **Enter** to exit the command prompt.

Using PowerShell

Windows PowerShell is a command-line shell for system administrators. You can use it for many of the installation procedures. It allows you to automate processes that might take more time manually.

To start PowerShell, from the **Start** menu, type **powershell** and **Enter**.

RUNNING ELEVATED WINDOWS POWERSHELL PROMPT AS A DIFFERENT USER

In situations when logging in interactively as the ObserveIT Service Account is impossible, use the following procedure to start an elevated Windows PowerShell prompt as the ObserveIT Service Account.

This will allow you to run ObserveIT installers as the ObserveIT Service Account.

1. In the PowerShell window, type in the following command, replacing Domain\Account with the NETBIOS name of your Active Directory domain and the account name for the ObserveIT Service

Account:

```
Start-Process powershell.exe -Credential "DOMAIN\account" -
NoNewWindow -ArgumentList "Start-Process powershell.exe -Verb
runAs"
```

Enter.

2. In the Windows Security window enter the credentials of the ObserveIT Service Account.
3. Click OK.

   If prompted Do you want to allow this app to make changes to your device? click Yes.

   A new elevated PowerShell window will start running as the ObserveIT Service Account.