

People. Your most valuable asset.
Your greatest risk.

Configuring ObserveIT to use SSL

ObserveIT for Servers is a client/server software application that monitors, audits and records all activities performed by people on an enterprises servers. The indexed, searchable, visual database allows those activities to be replayed to see exactly what is happening on the monitored servers. As with any product, ObserveIT has been designed to provide the highest possible level of security.

By default, the ObserveIT Agent and Application Server use a token exchange mechanism to prevent session hijacking and replay, and to encrypt the data communication. The security mechanism for the communication consists of:

- Encryption (Rijndael)
- Digital signing
- Token exchange

You can further secure the communication by configuring IIS on the Application server to require SSL, and the Agent to use HTTPS instead of HTTP.

In order to configure SSL traffic between the ObserveIT Agent and the ObserveIT Application Server, you will need to perform the following tasks:

On the ObserveIT Application Server

1. Creating a Digital Certificate request - This is done through the Internet Information Services (IIS) Manager MMC snap-in.
2. Submitting the Digital Certificate request to a Certificate Authority (CA) - This is done either by using an online process or web enrollment form, or by sending a text file containing the request to the CA.
3. Issuing and downloading the Digital Certificate - After the CA has approved your request.
4. Installing the Digital Certificate - This is done through the Internet Information Services (IIS) Manager MMC snap-in.

On the ObserveIT Agent

1. Configure the ObserveIT Agents to use SSL to communicate with the ObserveIT Application Server.

People. Your most valuable asset.
Your greatest risk.

Obtaining a Digital Certificate

A Digital Certificate is the digital equivalent of an ID card used with a public key encryption system. Also called digital IDs, digital certificates are issued by trusted third parties known as certification authorities (CAs). This guide assumes that the reader holds prior knowledge of PKI and its related terminology.

If necessary, please consult with these online knowledge bases and documentation:

<http://support.microsoft.com/kb/299875>

<http://support.microsoft.com/kb/887490>

In general, there should be 2 major considerations when deciding on where to obtain the Digital Certificate from, and what will the information that is provided by it.

Digital Certificate source - Internal CA, 3rd-party CA or Self-Signed?

A Digital Certificate needs to be obtained from a CA (Certification Authority), either a 3rd-party commercial CA such as Verisign, Thawte, Godaddy, Rapid SSL and others, or from an internal CA. 3rd-party CAs sell Digital Certificates for prices ranging from a few dollars per year, to a few hundred dollars, depending on the type of certificate issued, and other considerations such as the CA's reputation. Most operating systems are pre-configured to trust known 3rd-party CAs. Therefore you won't be required to import anything to the computers running the ObserveIT Agents, making this a much easier to use deployment.

In order to avoid having to pay for a Digital Certificate you can use an internal CA. Windows Server 2000/2003/2008 has a built-in CA that can be installed and used.

In cases where there is no need for an internal CA, or in cases where such a deployment cannot be achieved, you can also use a Self-Signed Digital Certificate.

While easy to obtain and 100% free of cost, issuing a Digital Certificate from your internal CA, or using a Self-Signed Digital Certificate does have some drawbacks. Especially worth noting is the fact that you must make sure that the computers running the ObserveIT Agent that are going to connect to the ObserveIT Application server are properly configured to trust this Digital Certificate. Unless these computers are made members of the Active Directory domain where you've installed your internal CA, they will not automatically trust your internal CA, and thus your connection will fail. In these scenarios, when a computer running ObserveIT Agent tries to connect to the ObserveIT Application Server, that computer does not trust the CA where the Digital Certificate was obtained from, and will refuse the connection.

People. Your most valuable asset.
Your greatest risk.

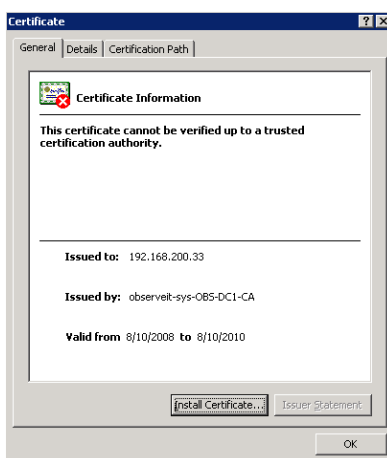


Figure 1: Un-trusted Digital Certificate

In such scenarios you must import the Root CA Digital Certificate (or the Self-Signed Digital Certificate) into each client computer in order to make them trust your Digital Certificate source. After importing the Root CA Digital Certificate the computer will trust that source and communication through SSL will be allowed.

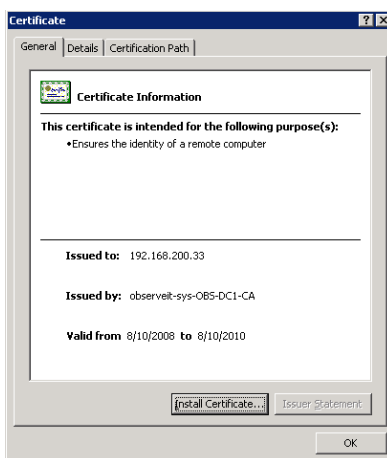


Figure 2: Trusted Digital Certificate

Common name

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.

People. Your most valuable asset. Your greatest risk.

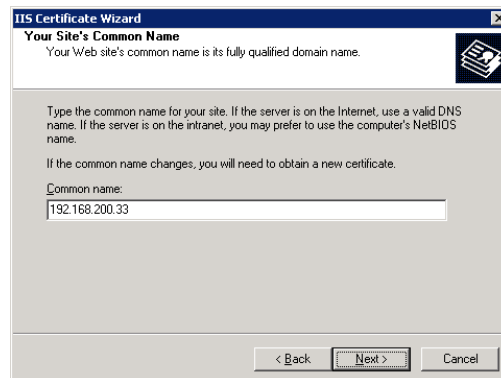


Figure 3: Digital Certificate Common Name

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.

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

Then the same exact IP address **MUST** be used when issuing the Digital Certificate for the ObserveIT Application Server.

If you do not follow these guidelines, you will receive an error message similar to this one:

```
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)
```

Note: While not viewable by the ObserveIT Agent, if you manually try to connect to the ObserveIT Web Management Console while using an FQDN or IP address that does not match the one listed in the server's SSL Digital Certificate, you will receive a warning in the web browser, similar to this:

People. Your most valuable asset. Your greatest risk.

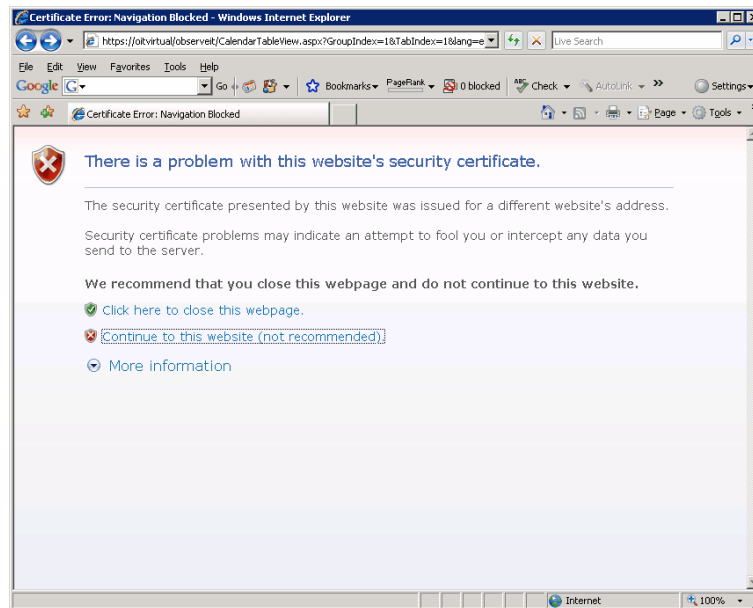


Figure 4: Digital Certificate Common Name and URL mismatch

And if you click "Continue to this website (not recommended)", you will be able to view the Digital Certificate error message by clicking on the button:

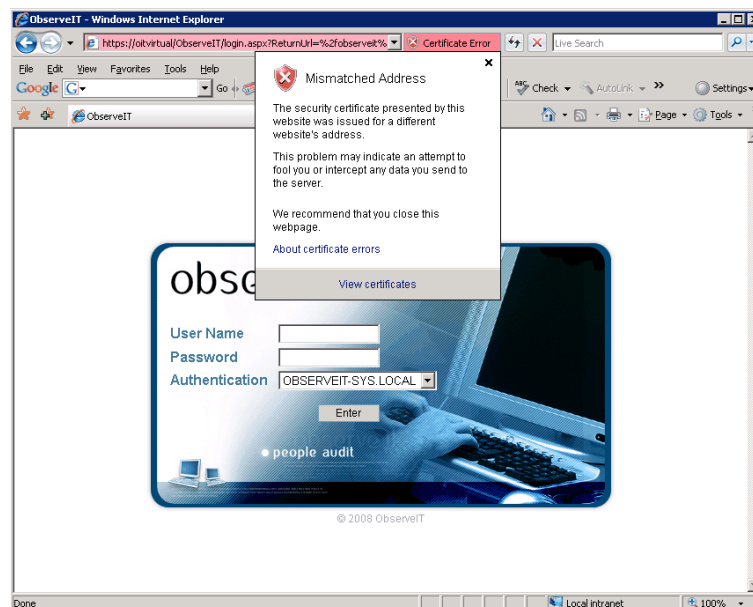


Figure 5: Digital Certificate Common Name and URL mismatch

People. Your most valuable asset.
Your greatest risk.

Configuring IIS to Require SSL

After obtaining the Digital Certificate you must configure the ObserveIT Application Server to require usage of SSL for Agent communication. This procedure is performed on the ObserveIT Application Server by using the Internet Information Services (IIS) Manager MMC snap-in. To do this, follow these steps:

1. Start the Internet Information Services (IIS) Manager. To do this, click Start, point to Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. Double-click the server name so that you see all of the Web sites. In IIS 6.0, expand Web Sites.
3. Right-click the ObserveIT Web site and then click Properties.
4. On the Directory Security tab, under "Secure Communication", click on the "Edit" button.
5. In the "Secure Communication" window, click to select the "Require Secure Channel (SSL)" checkbox. Also click to select the "Require 128-Bit Encryption" checkbox.

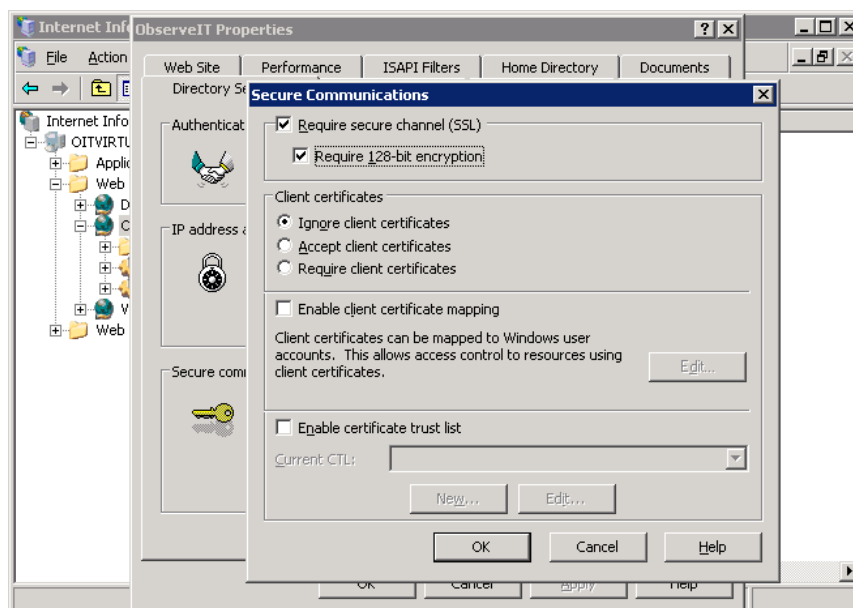


Figure 6: Require SSL

6. Click Ok.
7. Click on the "Web" tab. Make sure that port 443 is entered in the "SSL Port" text box.

Note: In case more than one website exists on the server hosting the ObserveIT Application Server, you will need to make sure that a unique combination of TCP ports and/or IP addresses is used. Otherwise, you might cause port conflict between the different sites, causing one of the conflicting sites to stop functioning.

People. Your most valuable asset.
Your greatest risk.

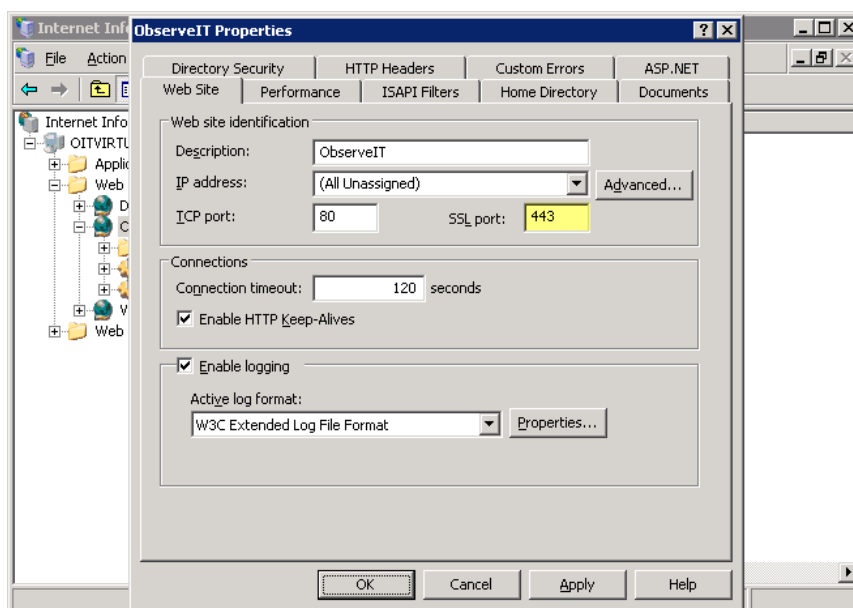


Figure 7: SSL Port

8. Click Ok to close the ObserveIT website Properties page.

Configuring the ObserveIT Agent to Use SSL

After obtaining the Digital Certificate and configuring the ObserveIT Application Server to require usage of SSL, you will now need to configure the ObserveIT Agent to use SSL when communicating with the ObserveIT Application Server. This procedure is performed on all the servers where the ObserveIT Agent is installed. To do this, follow these steps:

For new ObserveIT Agent installations

When deploying the ObserveIT Agent, you can use a manual installation method, or an automated one.

In the Server Configuration screen of the Agent installation process specify a URL to the ObserveIT Application Server, the one which the Agent will communicate with. The URL should be in the format of *HTTPS://FQDN/ObserveITApplicationServer*, or *HTTPS://IP_address/ObserveITApplicationServer*.

Note: Make sure that the server or computer running the ObserveIT Agent trusts the source of the Digital Certificate. Also make sure that the ObserveIT Application Server FQDN or IP address exactly matches those entered in the Digital Certificate.

People. Your most valuable asset.
Your greatest risk.

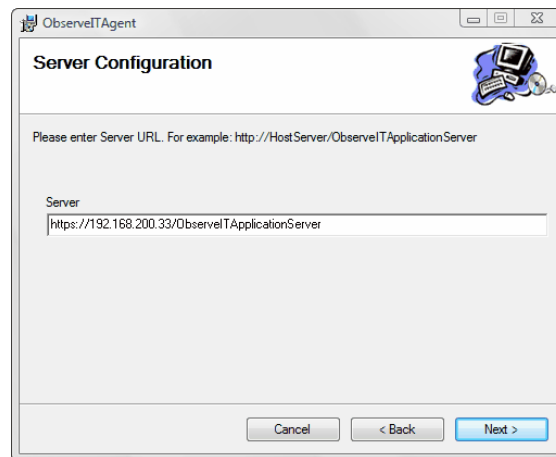


Figure 8: Server URL in the manual Agent installation

For existing ObserveIT Agent installations

When configuring SSL traffic between the ObserveIT Application Server and existing ObserveIT Agents you need to make changes in the ObserveIT Database. This change will propagate to the existing ObserveIT Agents and will thereafter configure them to use SSL when communicating with the ObserveIT Application Server.

In order to make the changes to the ObserveIT Database, run the following script in the SQL Server Query Analyzer or Management Studio (depending on the version of SQL Server you're using):

```
UPDATE dbo.ServerConfiguration
    SET PropertyValue = 'NEW_APP_SERVER_URL'
WHERE PropertyId = 4
    AND PropertyValue = 'OLD_APP_SERVER_URL'
```

Where `OLD_APP_SERVER_URL` is the old ObserveIT Application Server URL, in the format of `HTTP://FQDN/ObserveITApplicationServer`, or `HTTP://IP_address/ObserveITApplicationServer`.

And where `NEW_APP_SERVER_URL` is the new ObserveIT Application Server URL, in the format of `HTTPS://FQDN/ObserveITApplicationServer`, or `HTTPS://IP_address/ObserveITApplicationServer`.