

CONTRIBUTED DOCUMENTATION

This document is NOT supported by Computing Services.
DO NOT contact the Help Center with questions on this document.

WebISO IIS Installation Guide 3.0

Audience

This guide is intended for professional system administrators intimately familiar with the NT file system, system registry, and IIS.

Objectives

This guide walks you through the process of installing the Pubcookie 3.0 ISAPI filter on your Microsoft Internet Information 6.0 server. Other objects include:

1. How to export your SSL certificate and private key using the Certificate Export Wizard
2. How to setup and use the Pubcookie keyclient utility to obtain an encryption key
3. How to add the Pubcookie ISAPI filter to IIS 6.0
4. How to test the Pubcookie ISAPI filter to confirm that authentication works

What is WebISO?

Before describing what WebISO is a little background information is needed. WebISO does not refer to a particular software package or technology. But is an acronym for "web initial sign-on" from the Internet2 working group of the same name. At Carnegie Mellon, we use a software package known as Pubcookie to authenticate users using Kerberos. Pubcookie is a web authentication system originally developed by the University of Washington. It provides a way to authenticate web users.

How does Pubcookie work?

When a user attempts to access a web resource protected by Pubcookie for the first time, the web server will redirect the user to a login server, operated by Computing Services. This login server will prompt the user for their user ID and password. If the username and password are valid, the login server will issue a cookie to the user's web browser. The user is then redirected back to the protected resource.

The user's browser presents the cookie to the web server containing the protected resource, which validates the cookie. The web server or the web application can then determine if the user should be allowed to view the resource based on the user ID.

Further visits to protected pages don't require the user to log in again, until the user

- the user quits the web browser entirely
- the login cookie expires (12 hours after the initial login)
- or logs out by visiting <https://webiso.andrew.cmu.edu/logout.cgi>

How is this different from KWeb?

Pubcookie only requires the client web browser to support cookies and SSL encryption. Nearly all browsers support these features. KWeb requires the use of a browser plug-in to handle authentication. Computing Services isn't able to develop and test plug-ins for every possible browser and operating system combination, so there are very limited combinations that work.

Pubcookie requires the user to enter their username and password into the web browser once per session. KWeb doesn't require the user to ever enter their username and password, since it can read the user's Kerberos ticket from the operating system.

Prerequisites

Before you begin:

- Obtain your granting certificate, **pubcookie_granting.cert**, at this AFS address: [/afs/andrew.cmu.edu/data/db/pubcookie/client/usr/www/pubcookie/keys/pubcookie_granting.cert](#)
- Obtain a copy of your Certificate Authority's certificate in PEM format, at this AFS address: [/afs/andrew.cmu.edu/data/db/pubcookie/client/usr/www/pubcookie/keys/CMU-CA-server-1-06-mime.pem](#)
- Download the [login server distribution](#).

System requirements for your IIS machine are:

- Microsoft Windows 2000 Server or later on Intel hardware
- Microsoft Internet Information Server (IIS) 4.0 or later
- SSL enabled Web site using a 1024-bit private key (requires a SSL certificate -- we have a [Certificate Authority](#) service if you need a certificate)
- Accurate system time - **IMPORTANT!**. It is recommended that you synch to **ntp.net.cmu.edu**.
- Server registered in [NetReg](#) and in the cmu.edu domain

Installation Instructions

First, unzip the pubcookie distribution for Microsoft IIS into a folder of your choice. We will use **c:\pubcookie** in this document.

Verify the SSL Certificate key size (1024 bits required):

1. If you have installed your SSL Certificate on your web server then the easiest way to determine the key size is to open a secure (https) connection to your server. Double-click the lock at the bottom of the browser window and verify the key size is 1024-bits.
2. If you have not installed your SSL Certificate on your web server then open the certificate by double-clicking on it and verify the key size is 1024-bits. Install the certificate and then continue.
3. If you have not yet obtained an SSL Certificate for your web server then generate a new certificate signing request (CSR) and be sure to specify a 1024-bit private key. Send the request off to your Certificate Authority and install the new certificate and then continue.

NOTE: Pubcookie requires a 1024-bit private key!

To export your SSL cert and private key:

1. Bring up the IIS Management console.
2. Select your web site, click Properties.
3. Select the Directory Security tab.
4. Click View Certificate...
5. Select the Details tab, click Copy to File...
6. Follow the Certificate Export Wizard:
 1. Click Next
 2. Select Yes, export the private key, then click Next.
 3. Select PKCS#12 (.PFX) making sure to check Enable strong protection then click Next.
 4. Type and confirm the password then click Next.
 5. Enter a filename (e.g. C:\pubcookie\appserver.pfx) and click Next.
 6. Click Finish.

7. Click OK.

The intended result of this is a PFX-formatted file named appserver.pfx that contains your SSL certificate and private key.

To convert from PFX format to PEM format:

1. Open a command prompt.
2. Run the following command:

```
cd c:\pubcookie\openssl pkcs12 -in appserver.pfx -out appserver.pem -nodes
```

3. This will produce appserver.pem in the c:\pubcookie directory.

To separate your SSL certificate and private key:

1. Open appserver.pem in WordPad.
2. Use WordPad to extract the RSA private key into a new file called pubcookie_session.key.
3. Use WordPad to extract the certificate into a second new file called pubcookie_session.cert.
4. Save both new files in C:\pubcookie where the rest of the files reside.

To assemble the remaining required files:

1. Place the Pubcookie_granting.cert (from above) in the folder where you extracted the distribution (e.g. c:\pubcookie\pubcookie_granting.cert).
2. Place the CMU-CA-server-1-06-mime.pem (from above) in the folder where you extracted the distribution (e.g. C:\pubcookie\CMU-CA-server-1-06-mime.pem). This file will be used to establish the keyclient-keyserver trust.

To install the IIS ISAPI filter within your Web site:

1. Edit PubcookieFilter_Install.bat and adjust names if necessary and save the file. Below is a sample .bat file:

```
mkdir %Systemroot%\System32\Inetsrv\Pubcookie
  mkdir %Systemroot%\System32\Inetsrv\Pubcookie\keys
  copy pubcookie_granting.cert %Systemroot%\System32\Inetsrv\Pubcookie\keys
  copy pubcookie_session.cert %Systemroot%\System32\Inetsrv\Pubcookie\keys
  copy pubcookie_session.key %Systemroot%\System32\Inetsrv\Pubcookie\keys
  copy CMU-CA-server-1-06-mime.pem %Systemroot%\System32\Inetsrv\Pubcookie\keys
  copy PubCookieFilter-3.0.0.dll %Systemroot%\System32\Inetsrv\Pubcookie
  rem Remember to remove "Everyone" access to your Pubcookie dir
  rem Remember to add "System" read and "Administrator" change control
  rem Remember to add "System" execute to the DLL
  pause
```

2. Double-click PubcookieFilter_Install.bat to run it. It will copy all the necessary files from c:\pubcookie to a new Pubcookie folder in your Systemroot folder called:

```
%systemroot%\System32\Inetsrv\Pubcookie
```

3. Remove the Everyone group from the access list to this folder.
4. Grant the following accounts Read and Execute access to this folder: System account and the WPG_IIS group.
5. Grant the Administrators group Modify access.
6. Make sure the PubCookieFilter-3.0.0.dll in the %Systemroot%\System32\Inetsrv\Pubcookie folder is executable by the System account.
7. Start the Internet Service Manager (usually found in the Administrative Tools Start Menu folder).

8. Right-click on the Web site into which you want to install the Pubcookie ISAPI filter and select Properties from the popup menu.
9. In the ISAPI Filters tab, click Add.
10. Enter Pubcookie for Filter Name.
11. Click Browse and locate the Pubcookie DLL for Executable (e.g. %Systemroot%\System32\Inetsrv\Pubcookie\PubCookieFilter-3.0.0.dll).
12. Click OK. And click OK.
13. Right-click your Web site. Stop and restart it.
14. Verify that IIS is installed by reviewing the Properties of your Web site. The status of the Pubcookie ISAPI filter should be loaded; the arrow should be up and green.
15. Leave the Internet Service Manager window open. You will need to use it during configuration.

Configuration Instructions

To add local configuration settings to the registry:

1. Right-click **example.reg** from the distribution. Select **Edit**. This file contains registry settings used to configure the Pubcookie ISAPI filter. Below is a sample registry file that is used to configure Pubcookie to work in the CMU environment:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PubcookieFilter]
"AuthTypeName1"="webiso"
"Keymgmt_URI"="https://webiso.andrew.cmu.edu:2222/"
>Login_URI"="https://webiso.andrew.cmu.edu/"
"Enterprise_Domain"=".cmu.edu"
"Web_Login"="http://webiso.andrew.cmu.edu/"
"Debug_Dir"="C:\Windows\System32\LogFiles\PubcookieFilter"
"Debug_Trace"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PubcookieFilter\Webapp]
"AuthType"="webiso"
"Web_Login"="https://webiso.andrew.cmu.edu/"
"AppID"="WebApp"
"Hard_Timeout"=dword:00000e74
"Inactive_Timeout"=dword:00000190
"Timeout_URL"="https://webiso.andrew.cmu.edu/logout.cgi"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PubcookieFilter\Webapp\app-and-clearlogin-logout]
"Logout_Action"=dword:00000003

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PubcookieFilter\Webapp\app-and-redirect-logout]
"Logout_Action"=dword:00000002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PubcookieFilter\Webapp\app-only-logout]
"Logout_Action"=dword:00000001
```

2. Change the value assigned to Web_Login. Use the location of the WebISO login server.
3. Change the value assigned to Enterprise_Domain. This defines the scope necessary to send granting request cookies between your IIS server and your login server.
4. Click File. Select Save. Close this window.
5. Double-click example.reg to enter these settings into the registry.

To force the IIS ISAPI filter to read new registry settings:

1. Start a Web browser and open **/pubcookiefilter_reset** on your IIS server. For example:

```
http://webserver.cmu.edu/pubcookiefilter_reset
```

Stopping and restarting your Web site has the same effect.

2. Installation and configuration is complete. Close the Internet Service Manager window.

Testing Instructions

To test the Pubcookie ISAPI filter:

1. Copy the **WebApp** folder and content from the distribution to your Web site's root folder (e.g. **C:\inetpub\wwwroot\WebApp**).

You can think of this as creating a IIS-protected application called WebApp. Notice that the configuration instructions pre-populated the registry with a AuthType setting for this application.

2. Start a Web browser and open **https://webserver.cmu.edu/WebApp** on your IIS server. For example:

```
https://webserver.cmu.edu/WebApp
```

You should be redirected to your login server. After being authenticated, you should be redirected back.

3. Verify that the response generated by **/WebApp/Default.asp** displays the correction information. It should look something like this:

```
Authentication Sample
You logged in as user: kspacey@ANDREW.CMU.EDU
LOGOUT links:
• invoke app-only-logout
• invoke app-and-redirect-logout
• invoke app-and-clearLogin-logout
Pubcookie Appid: webapp
Pubcookie User: kspacey@ANDREW.CMU.EDU
Pubcookie Creds: 1
Pubcookie Version: Pubcookie ISAPI Filter,
3.0.0
Time: 2:32:03 PM on 2/25/2004
You were authenticated using:
Virtual Server: webserver.cmu.edu
Actual Server: webserver
Web Instance: 1
URL: /webapp/Default.asp
See all the Server Variables with Dumpvars.asp
```

4. Enjoy!