# Beneficiary Travel (BT) Dashboard

# Version 1.0

**C3-C1 Conversion Project**

# Installation Guide

**Beneficiary Travel Patch DGBT*1*19**

**July 2012**

Department of Veterans Affairs
Office of Information and Technology (OIT)
Product Development (PD)

# Revision History

| Date | Revision | Description | Author |
|---|---|---|---|
| May 2011 | 1.0 | Initial template | Redacted |
| June 2011 | 1.1 | Copied BT Install Guide into the template | Redacted |
| June 2011 | 1.2 | Added content | Redacted |
| July 2011 | 1.2 | Accepted Lucy's Changes except for Trouble-Shooting Section, Made Name Field Unidentifiable in Post-Install Considerations. | Redacted |
| July 2011 | 1.3 | Prepped for ESE Checklist | Redacted |
| July 2011 | 1.4 | Removed yellow highlighting by "AJR" | Redacted |
| July 2011 | 1.5 | Continued to prep for ESE Checklist | Redacted |
| September 2011 | 1.6 | • Added Beneficiary Travel Patch DGBT*1*19<br>• Changed dates to October 2011 for release | Redacted |
| September 2011 | 1.7 | Updated content | Redacted |
| October 2011 | 1.8 | • Fixed formatting<br>• Updates from LA (v10/27/11) | Redacted |
| November 2011 | 1.9 | • Changed dates to November 2011<br>• Added more info about the configuration file | Redacted |
| January 2012 | 2.0 | • Updates from LA (v01/11/12)<br>• Updates from 01/20/2012 meeting | Redacted |
| February 2012 | 2.1 | • Added a Troubleshooting item<br>• Updated with Cindy/Lenny edits<br>• Updated with edits from 2/22/12 meeting<br>• Updated with edits from 2/24/12 meeting<br>• Updated with SH input for web server and TA input for FAQ | Redacted |
| March 2012 | 2.2 | • Updated the Troubleshooting section<br>• Changed dates to March 2012<br>• Incorporated updates from LA | Redacted |

| Date | Revision | Description | Author |
|---|---|---|---|
| April 2012 | | • Changed dates<br>• Updated with CH comments<br>• Added Step 6 and Appendix A: IIS Instructions for Using Cache for Remote Web Servers from the CSP Gateway Configuration Guide<br>• Added Appendix B: Instructions for Obtaining a Security Certificate<br>• Prepped for June release | Redacted |
| May 2012 | | • Updated with Product Support comments<br>• Added bt folder information | Redacted |
| June 2012 | | • Item 8 of step 5 should be Step 8 per LA<br>• Changed dates to July 2012<br>• Added changes from CH | Redacted |

# Table of Contents

**Introduction** ..... **1**
**Pre-installation Considerations** ..... **2**
Before Installing BT Dashboard ..... 3
Minimum Required VistA Packages ..... 3
Minimum Server Requirements ..... 4
**Installation** ..... **5**
Step 1: VistA patch DGBT*1*19 should be installed before the web server installation ..... 5
Step 2: Vista-side Operating System and Caché Installation: Create two directories ..... 5
Step 3: Vista-side Operating System and Caché Installation: Create a CSP Application ..... 6
Before Creating a CSP Application ..... 6
Configuring a CSP Application ..... 10
Configured CSP Application ..... 13
Step 4: Vista-side Operating System and Caché Installation: Import the Source Code XML ..... 14
Step 5: Web Server: Configure a Shared Web Server ..... 16
Step 6: Windows Server for IIS: Configure/Setup a Remote Web Server Using Caché Server Pages ..... 22
Step 7: Copy the bt Folder ..... 22
Step 8: Test the URL ..... 22
**Additional Information** ..... **23**
Software and Documentation ..... 23
Attention: Facility ISOs and Privacy Officers Update your existing site Privacy Impact Assessments (PIA) ..... 23
**Appendix A: IIS Instructions for Using Cache for Remote Web Servers from the *CSP Gateway Configuration Guide*** ..... **25**
**Section 4: Web Servers for Microsoft Windows** ..... **25**
Section 4.1: Microsoft Internet Information Services Version 7 (IIS v7) ..... 25
4.1.1 Installation ..... 26
4.1.2 Determining the Supported Interfaces ..... 27
4.1.3 Installing the ISAPI and CGI Services (If Required) ..... 27
4.1.4 Setting Permissions for the Gateway Components ..... 28
4.1.5 Configuring the CSP Application Path ..... 28
4.1.6 .Bitness — Running 32-bit Applications on 64-bit Servers ..... 29
4.1.7 Request Filtering Module ..... 30
4.1.8 Note on Mapping CSP File Extensions ..... 31
4.1.9 Manual Step for Enabling URLs with /bin ..... 31
4.1.10 Option 1: (Recommended) Using the Native Modules (CSPms*.dll) ..... 31
4.1.11 Option 2: Using the ISAPI Modules (CSPms*.dll) ..... 33
4.1.12 Option 3: Using a Native Module with the NSD (CSPcms.dll) ..... 34
4.1.13 Option 4: Using an ISAPI Module with the NSD (CSPcms.dll) ..... 37
4.1.14 Option 5: Using the CGI Modules with the NSD (nph-CSPcgi*.exe) ..... 39
4.1.15 Restarting IIS ..... 41
4.1.16 Troubleshooting ..... 41
Section 4.2: Microsoft Internet Information Services Version 6 (IIS v6) or Earlier ..... 42
4.2.1 Installing with Microsoft Web Servers (All Connectivity Options) ..... 42
4.2.2 Option 1 (Recommended): IIS and ISAPI Modules (CSPms.dll) ..... 43
4.2.3 Option 2: IIS and ISAPI Module with NSD (CSPcms.dll) ..... 46
4.2.4 Option 3: IIS and CGI Modules with NSD (nph-CSPcgi.exe) ..... 48

4.2.5 Using the ISAPI Filter (CSPmsf1.dll) ..... 49
4.2.6 IIS Application Protection Levels ..... 51
4.2.7 IIS Application Pools and Web Gardens ..... 52
**Appendix B: Instructions for Obtaining a Security Certificate ..... 55**
Enabling SSL ..... 55
Assigning an SSL Server Certificate to a Web Site ..... 55
Installing a CA Certificate ..... 56

# Introduction

The Indianapolis VAMC developed the Class 3 Beneficiary Travel (BT) Dashboard to assist users in creating travel claims and in making faster, more accurate decisions on mileage reimbursement. The VHA Chief Business Office requested the BT Dashboard package be implemented as part of the Cost Efficiency Initiative, which is one of the VA Secretary's 16 Major Transformation Initiatives (T-16).

The BT Dashboard is a web-based application designed to be used along with the existing VistA Beneficiary Travel Claim option in concurrent sessions for a patient. BT Dashboard calculates the driving mileage from the patient's address to a configured set of institutions. Using the Beneficiary Travel Claim menu, the application automatically synchronizes with travel claims as claims are created in VistA. BT Dashboard also displays patient appointments, notes, orders, consults, and past claims.

The locally-developed BT Dashboard package was accepted by OIT as a priority for conversion from Class 3 (local use) to Class 1 (VHA-wide use). The BT Dashboard package was installed and tested in production at thirteen VAMC facilities. This included individual VAMC web server installations, as well as several VAMCs in Region 1 where a single, centralized, web server was used.

1. The travel clerk opens a VistA session using the Beneficiary Travel Claim menu.
2. The travel clerk opens a BT Dashboard session.
3. The travel clerk enters a new travel claim into VistA.
4. BT Dashboard synchronizes with the claim, extracts the patient's address from VistA, and calculates the distance between the patient's home address and each VAMC and CBOC in the area using the Bing Maps API.
5. BT Dashboard display:
    a. Patient name
    b. Patient address
    c. Service connection percentage
    d. Scheduled appointments and the status of each appointment, notes, orders, consults, and claims
    e. Clinical inventory list of each facility within the area
    f. Mileage to configured facilities

No data is entered through BT Dashboard. BT Dashboard only displays mileage and other information. The travel clerk enters the mileage generated by BT Dashboard at the appropriate prompt while entering a travel claim in VistA.

# Pre-installation Considerations

This document presents instructions for installing BT Dashboard with examples using a test account.

> **Note:** The screen captures in this guide depict InterSystems Caché®5.23 on VMS. Your Caché environment will most likely be higher and your operating system may be something other than VMS.

Install and test this software in test accounts prior to installation in production accounts. The test installation is depicted in this document.

Depending on your organization and the allocation of responsibilities between your local and/or regional IT staff and BT supervisors, or ADPAC's, installation may require the coordinated work of three or more people to accomplish the activities listed below. Centralized regional servers will be used with all facilities in a region sharing a single server. Service Delivery and Engineering (SDE) will assign a Service Line Manager to identify and direct server-related installation activities.

1. VistA Patch DGBT*1*19 should be installed and parameters entered per patch instructions prior to following the steps in this installation guide.
2. Download the DGBT BENEFICIARY TRAVEL DASHBOARD 1_0.ZIP file from Anonymous.
3. Create a new directory on the VistA server (requires access at the operating system level, i.e. VMS, Linux, etc.; may require a system manager or regional IT support).
4. Create/configure Caché Server Pages application (requires access to Caché Cube System Management Portal; may require a system manager or regional IT support).
5. Import BT Dashboard source code XML (requires use of Caché Studio; may require a system manager or regional IT support).
6. Update the Privacy Impact Assessment (PIA); an ISO or Privacy Officer should review.

The Caché client needs to be installed on the web server. Obtaining the executable may be necessary. Obtain the Caché Installer from your VistA system manager who may need to download it from the national Anonymous software distribution servers. (The system manager can guarantee that the version matches the VistA Caché production version.)

- Users do not have to log off the system during installation.
- BT Dashboard software does not have to be installed during off-peak hours.

# Before Installing BT Dashboard

A fully operational web server (Windows Server 2003 with IIS 6.0 or Apache 2.059) and the current version of Caché are pre-requisites to installing this software.

> **Note:** The pre-installation considerations are potential actions to be taken before sites install this software. If these steps were accomplished by previously installing a CSP application and configuring a CSP Gateway, proceed to the Minimum Required VistA Packages section of this document.

1. Set up and configure a web server for a test environment and a web server for a production environment. This should not be the same server that is used for the Console Management System (CMS).
   - The appropriate facility or regional server manager should identify or set up a Windows server (physical or virtual).
   - The appropriate facility or regional server manager should install either IIS or Apache.
   - Current version of Caché with client (including Studio, System Management Portal) is needed. Running the Caché executable (client) on the web server will install the CSP component, which allows you to configure the gateway.
2. Add your VistA server in the CSP Gateway and test the connection.

> **Note:** Vista credentials will be needed to log on to the Vista Server. This step may require coordination between a VistA system manager and a facility or regional server manager).

# Minimum Required VistA Packages

BT Dashboard requires that the following software is installed and fully-patched.

| **Package** | **Namespace** | **Minimum Version** |
|---|---|---|
| Beneficiary Travel | DGBT | 1.0 |
| Kernel | XU | 8.0 |
| MailMan | XM | 8.0 |
| VA FileMan | DI | 22.0 |
| RPC Broker | XWB | 1.1 |
| Registration | DG | 5.3 |

# Minimum Server Requirements

- Windows Server 2003 or higher
- IIS 6.0 or higher or Apache 2.059 or higher

  **Note:** A dual monitor setup for travel clerks is most convenient, but dual monitors are not mandatory.

- VHA Caché Cube for Windows CSP Gateway

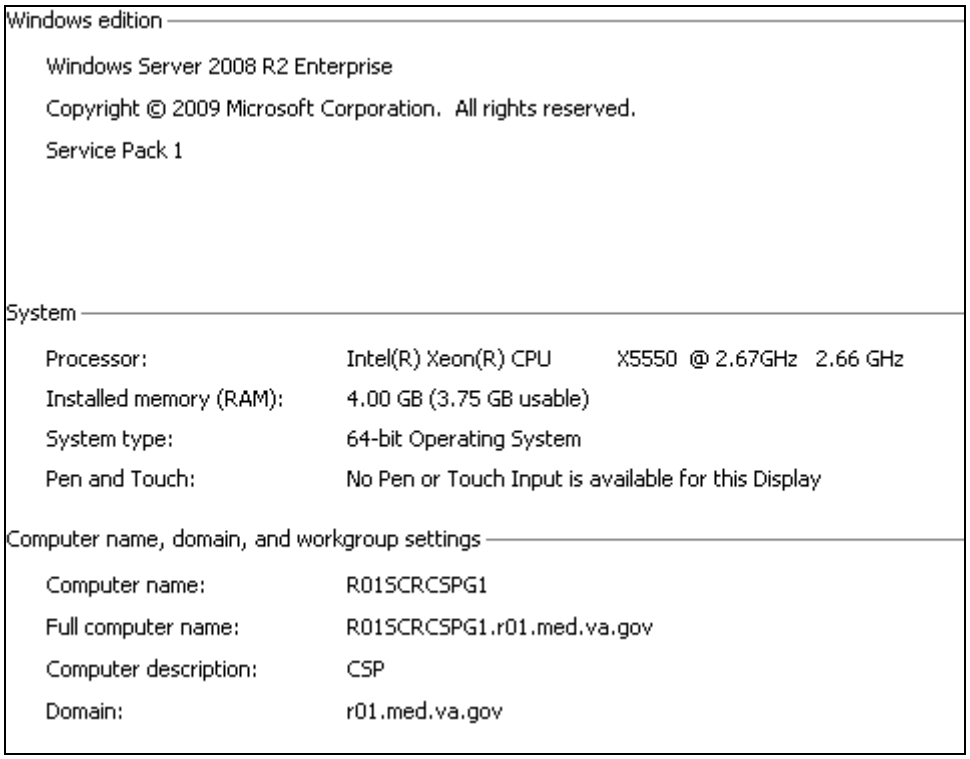
  **Note:** The version of Caché installed on the web server should be at least the highest version that any VAMC sharing the server is using in production.

**Suggestions for Servers**

- VM or physical machine
- Dual CPU
- 4 GB of RAM memory
- 40 GB HD

During testing, several VAMCs shared a single regional web server running Windows 2008 Server, IIS v7, and Caché 2011. For installation on a Windows box, this region suggested using IIS rather than Apache to take advantage of the greater availability of Windows server experts.

**Sample informational display of web server hardware used in testing**



Windows edition

Windows Server 2008 R2 Enterprise

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

| | |
|---|---|
| Processor: | Intel(R) Xeon(R) CPU X5550 @ 2.67GHz 2.66 GHz |
| Installed memory (RAM): | 4.00 GB (3.75 GB usable) |
| System type: | 64-bit Operating System |
| Pen and Touch: | No Pen or Touch Input is available for this Display |

Computer name, domain, and workgroup settings

| | |
|---|---|
| Computer name: | R01SCRCSPG1 |
| Full computer name: | R01SCRCSPG1.r01.med.va.gov |
| Computer description: | CSP |
| Domain: | r01.med.va.gov |

# Installation

## Step 1: VistA patch DGBT*1*19 should be installed before the web server installation

1. Load and install DGBT*1*19 **per instructions in the patch**. This patch includes an updated DGBTE routine, the **Edit the BT Dashboard Configuration file** [DGBT BENE TRAVEL CONFIG EDIT] option (attached to the **Beneficiary Travel Menu** option), and the following two files:

| File | Description |
|---|---|
| BENEFICIARY TRAVEL CONFIG File (#392.5) | The BENEFICIARY TRAVEL CONFIG file stores the application configuration, including the primary institution, a list of VA institutions to track, and a list of additional facilities to track. |
| BENEFICIARY TRAVEL DASHBOARD AUDIT (#392.51) | The BENEFICIARY TRAVEL DASHBOARD AUDIT file stores actions within the Beneficiary Travel Dashboard application. |

2. Download the DGBT BENEFICIARY TRAVEL DASHBOARD 1_0.ZIP file from Anonymous (see the Software and Documentation section of this guide for more information).
3. After installing the patch, follow the directions on the patch for adding one entry to the Beneficiary Travel Config File (#392.5) and for populating the file with institution, specialty, and other data.

## Step 2: Vista-side Operating System and Caché Installation: Create two directories

Once the installation is complete, the URL of the Beneficiary Travel Dashboard will look similar to:
**http:// <*webserver*>/csp/bt/dgbtDashboard.csp**

This step is required for each facility's VistA server, regardless of whether a centralized web server or local web server is used.

Create two directories on your VistA Server (VMS, Linux, Windows, etc.) to share the .csp files, one for test and one for production.

**VMS Example (your path should conform to national standards)**

| Environment | Path | Permissions |
|---|---|---|
| Production | XXX_CACHÉ$:[XXX.CSP.BT]<br>**Note:** This is a logical reference example, where XXX indicates the 3-character site identifier | S:RWED, O:RWED, G:RWED, W: NONE |

**Note:** When using a Linux or a Windows operating system, adjust the pathname appropriately.

The owner should be the production VistA account that users use to sign onto VistA.

$ CREATE/DIRECTORY/OWNER=**xxxVISTA** disk$:[directory]

The format is **xxx**VISTA, where **xxx** indicates the 3-character site identifier.
Examples:

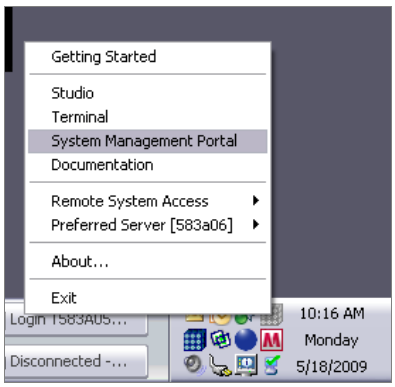
- **MAC**VISTA – Northern California Health Care
- **TAM**VISTA – Tampa VAMC
- **BAL**VISTA – Baltimore VAMC

# Step 3: Vista-side Operating System and Caché Installation: Create a CSP Application

## Before Creating a CSP Application

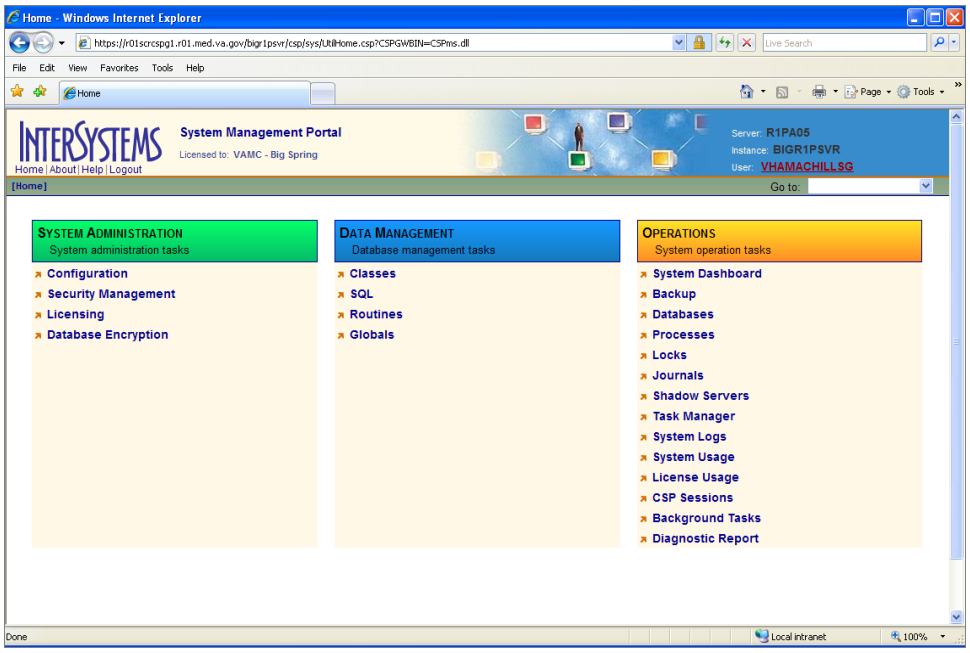
Use the System Management Portal to create a Caché Server Pages (CSP) application.

1. Right click **Caché Cube** and select **System Management Portal**.
   Security Management Portal page displays.



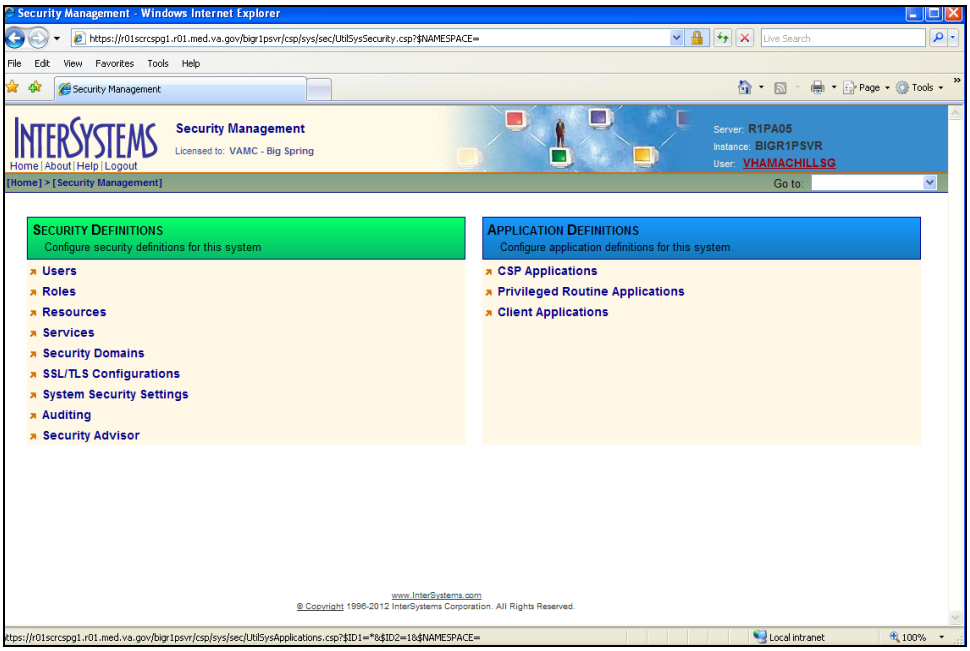

**Getting Started>System Management Portal**

2. Access the database server System Management Portal of the site.



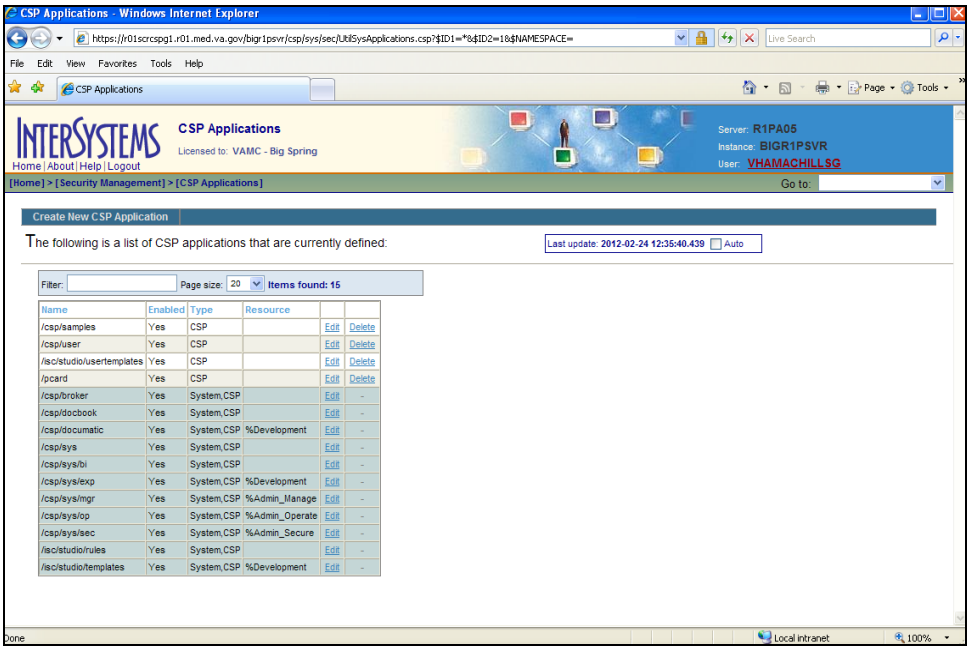

**InterSystems System Management Portal window**

3. To access the Security Management option, double-click the **Security Management** link. Security Management page displays.



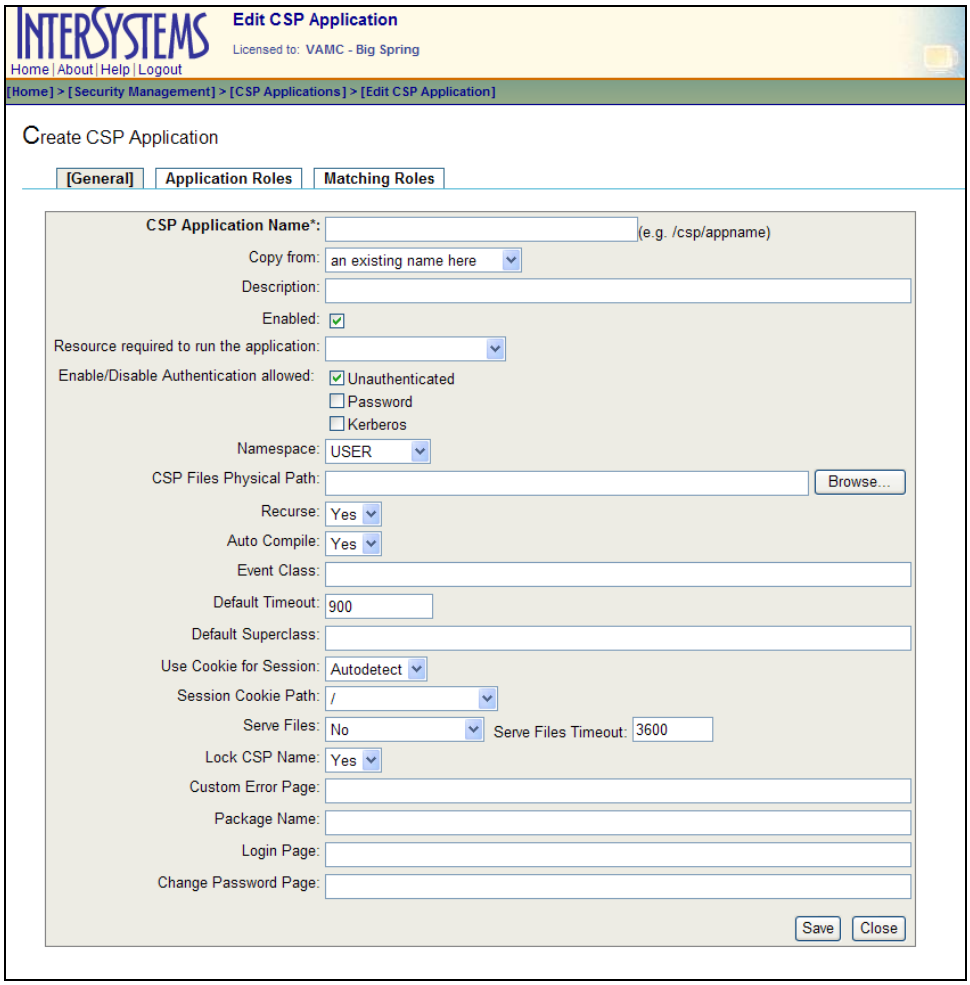

**InterSystems Security Management window**

4. To access the CSP Applications option, double-click the **CSP Applications** link. CSP Applications page displays.




**InterSystems CSP Applications window**

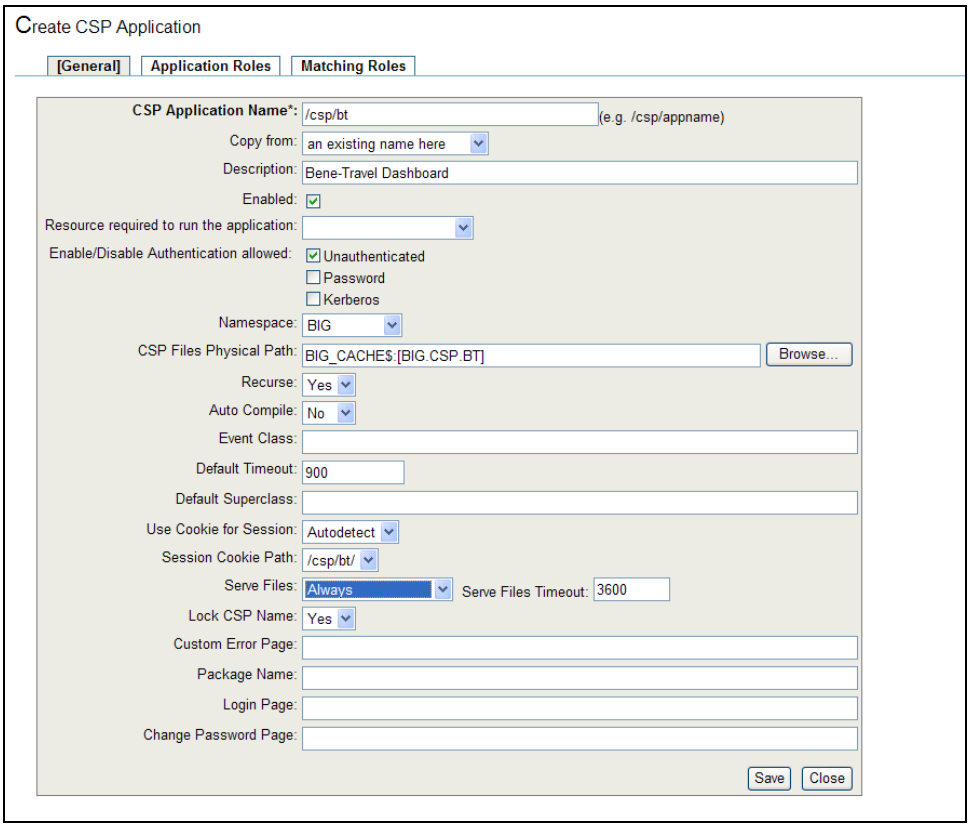
5. To add a CSP application to this specific Caché instance, click **Create New CSP Application** link. Edit CSP Application page displays.




**InterSystems Edit CSP Application page**

## Configuring a CSP Application

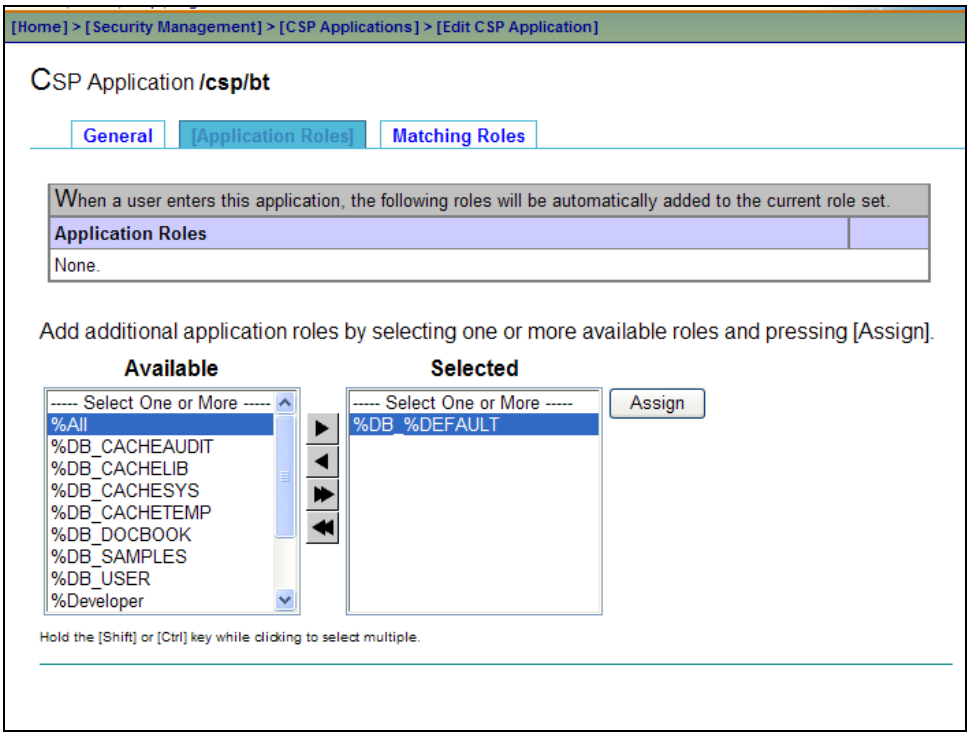
1. Configure the CSP application.
   Use national data center standards for the Caché superserver port, for the default production namespace, and for the CSP Files Physical Path.
   - The example is from the Big Spring Caché VistA environment.
   - Depending on the version of Caché that is running, if you see the Hyperevent Implementation field, select the **Select** on server option.
   - The **Namespace** and **CSP Files Physical Path** of a site will vary and be specific to that configuration.
   - The CSP Files Physical directory is created by this procedure, if it does not exist.




**InterSystems Create CSP Application page**

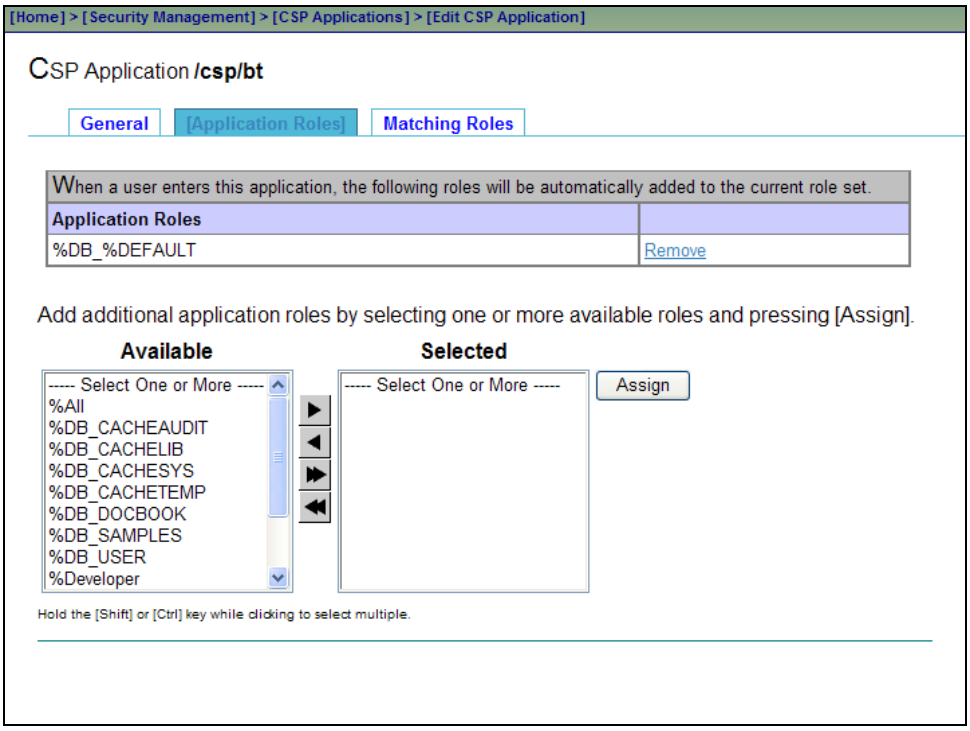
2. On the Create CSP Application page, click the **Save** button.
   The CSP application is saved.
3. Click the **Application Roles** tab to attach an Application Role to this CSP application.

4. On the Application Roles tab, double-click the **%DB_%Default** role in the **Available** drop-down list to move it to the **Selected** drop-down list.




**InterSystems CSP Application/csp/bt>Application Roles tab**

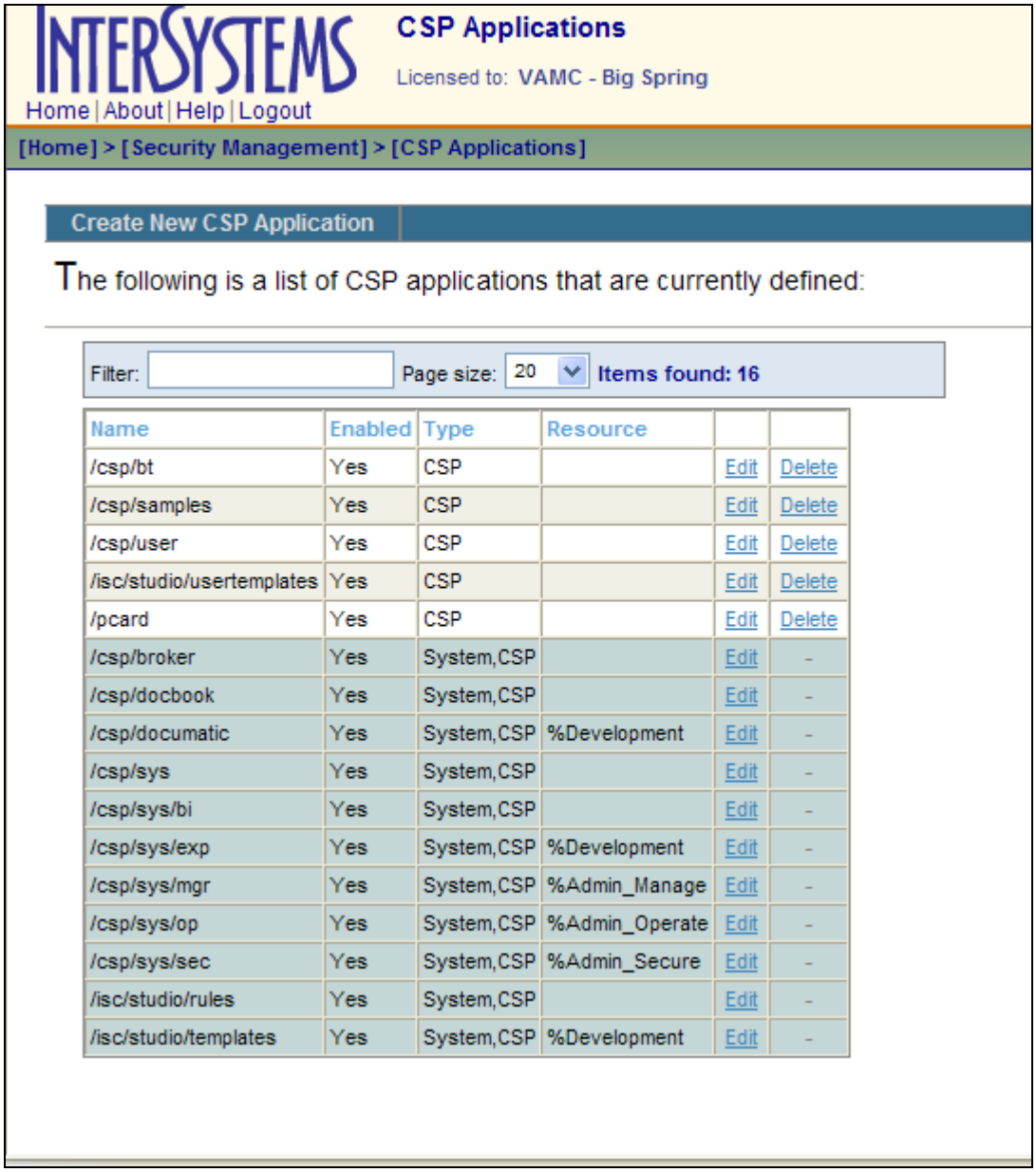
5. To add the role to the CSP application, click the **Assign** button.
   **%DB_%Default** displays in the Application Roles list.




**InterSystems CSP Application/csp/bt with the application role assigned**

## Configured CSP Application

The CSP application is now configured for this specific Caché instance.




| Name | Enabled | Type | Resource | | |
|---|---|---|---|---|---|
| /csp/bt | Yes | CSP | | Edit | Delete |
| /csp/samples | Yes | CSP | | Edit | Delete |
| /csp/user | Yes | CSP | | Edit | Delete |
| /isc/studio/usertemplates | Yes | CSP | | Edit | Delete |
| /pcard | Yes | CSP | | Edit | Delete |
| /csp/broker | Yes | System,CSP | | Edit | - |
| /csp/docbook | Yes | System,CSP | | Edit | - |
| /csp/documatic | Yes | System,CSP | %Development | Edit | - |
| /csp/sys | Yes | System,CSP | | Edit | - |
| /csp/sys/bi | Yes | System,CSP | | Edit | - |
| /csp/sys/exp | Yes | System,CSP | %Development | Edit | - |
| /csp/sys/mgr | Yes | System,CSP | %Admin_Manage | Edit | - |
| /csp/sys/op | Yes | System,CSP | %Admin_Operate | Edit | - |
| /csp/sys/sec | Yes | System,CSP | %Admin_Secure | Edit | - |
| /isc/studio/rules | Yes | System,CSP | | Edit | - |
| /isc/studio/templates | Yes | System,CSP | %Development | Edit | - |

**InterSystems CSP Applications page with list of defined applications**

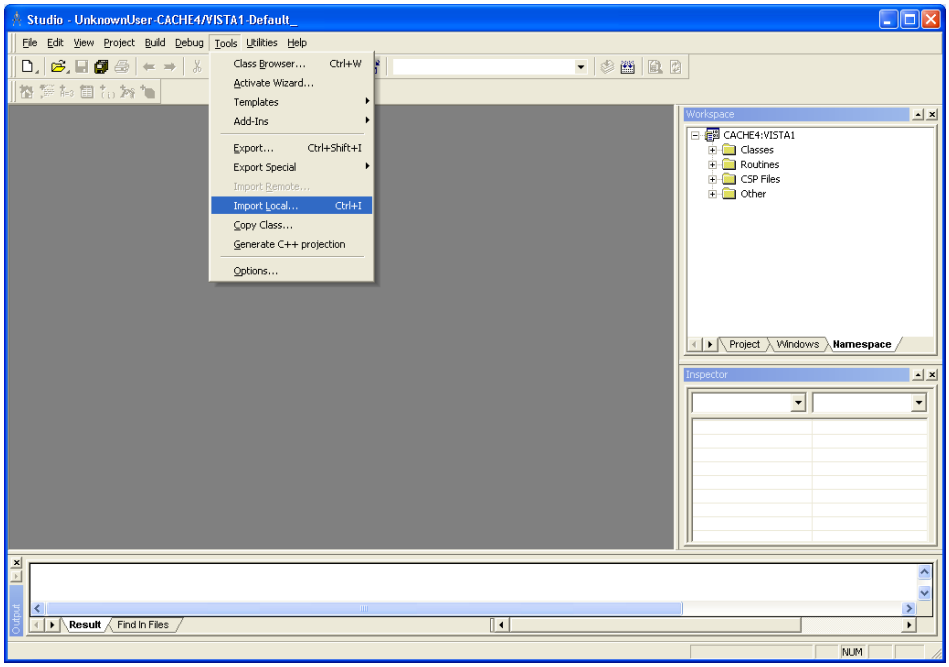
6. To return to the CSP Applications, click the **CSP Applications** link.
7. Log off the System Management Portal.

# Step 4: Vista-side Operating System and Caché Installation: Import the Source Code XML

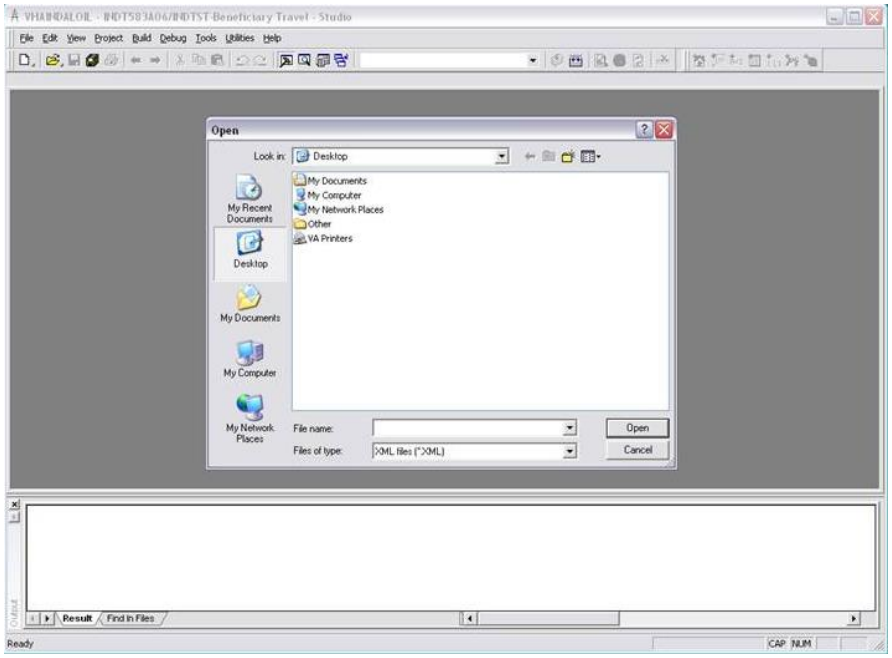
Use Caché Studio to import the source code XML.

**Note:** Caché Studio should be connected to your VistA server in your station's namespace.

1. Click the **Tools menu** and select **Import Local**.

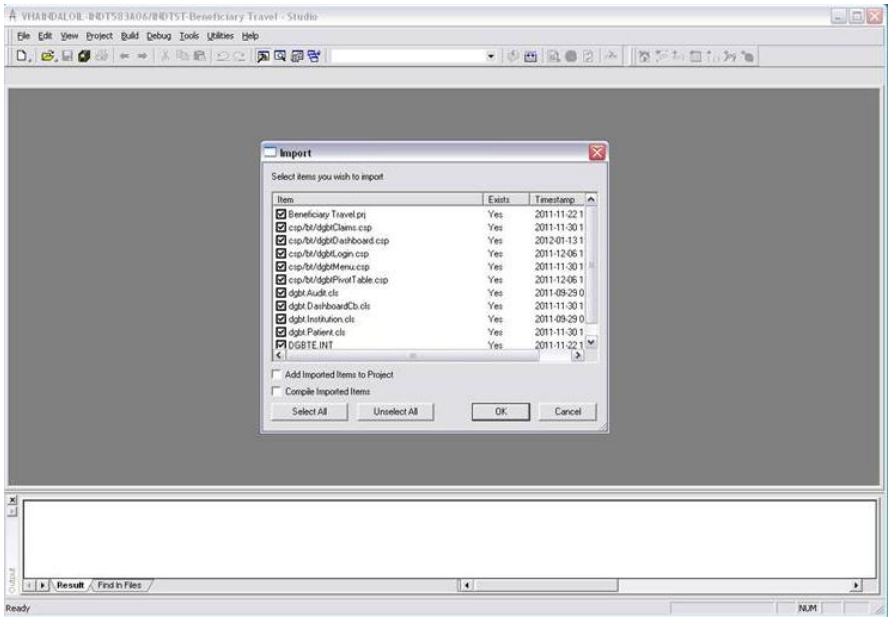



**Caché>Studio>Tools>Import Local**




**Beneficiary Travel – Studio Open window**

2. Browse to the XML source code file included with the installation files.
3. Click the **Open** button.



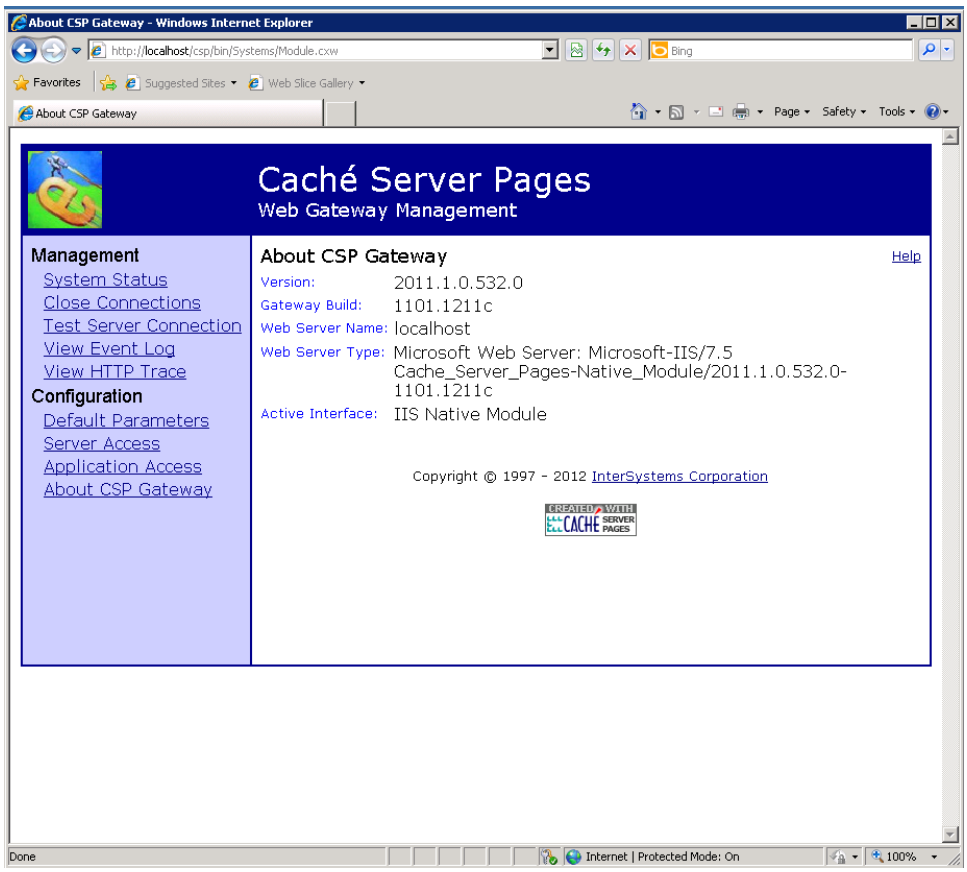

**Beneficiary Travel – Studio Import window**

4. Ensure the **Add Imported Items to Project** checkbox is **not** selected.
5. Click the **OK** button to import the **Beneficiary Travel Dashboard .csp and .cls** project files.

**Note:** After the xml is loaded, two statuses display in the Appointment table separated by a **"^"**. The first status comes from the CPRS cover sheet and the second comes from Appointment Management.

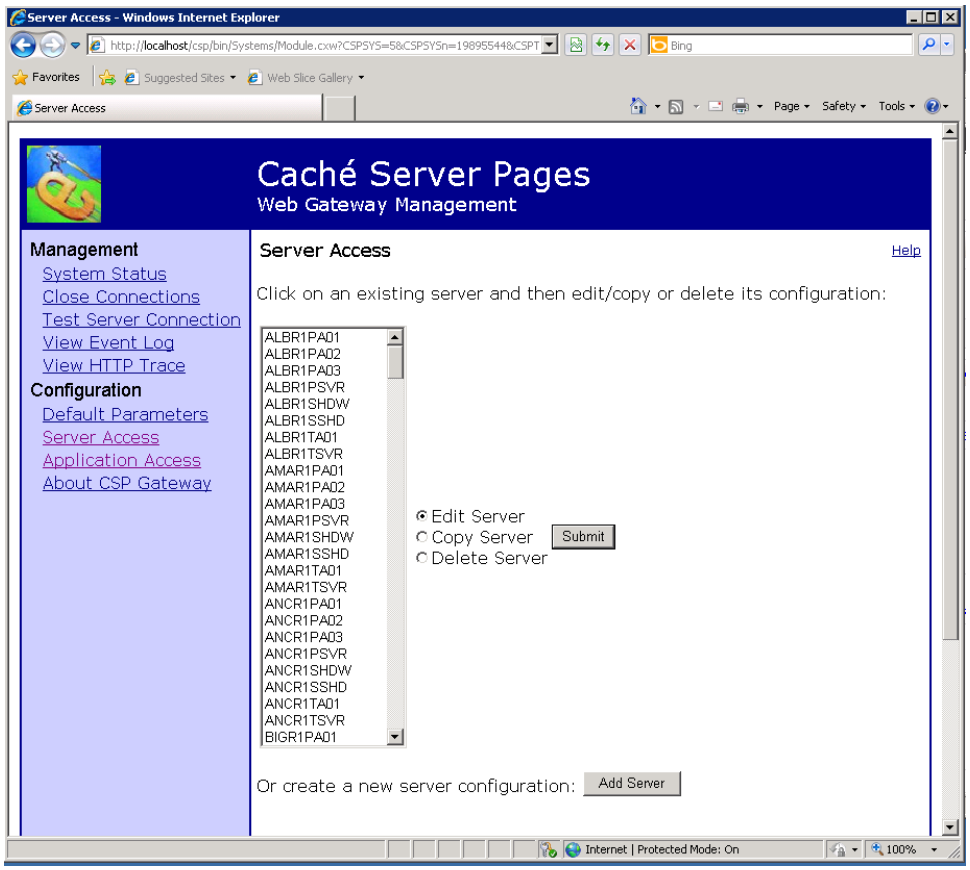
# Step 5: Web Server: Configure a Shared Web Server

1. Access CSP Gateway via a web browser. (http://localhost/csp/bin/Systems/Module.cxw)



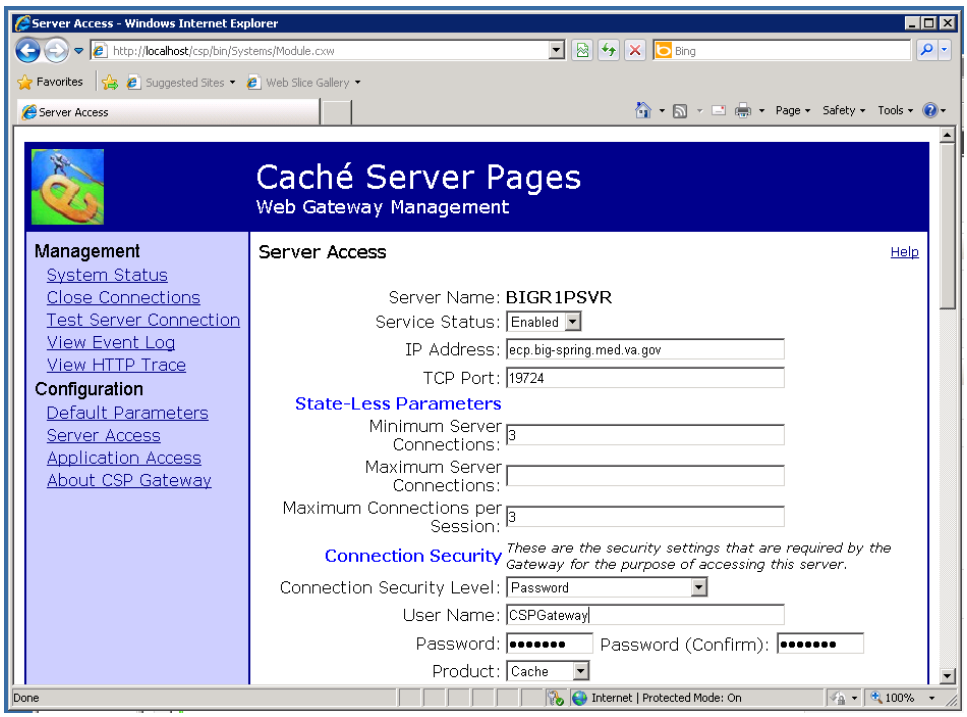

**Caché Server Pages, About CSP Gateway page**

2. Select **Server Access** to add the site's VistA Database server instance.




**Caché Server Pages, Server Access page**

3. The following example uses the Big Spring production database instance.
   a. Enter the server name, IP address/Fully Qualified Domain Name (FQDN), Caché SuperServer Port, Username, and Password information.
   b. Save the configuration.

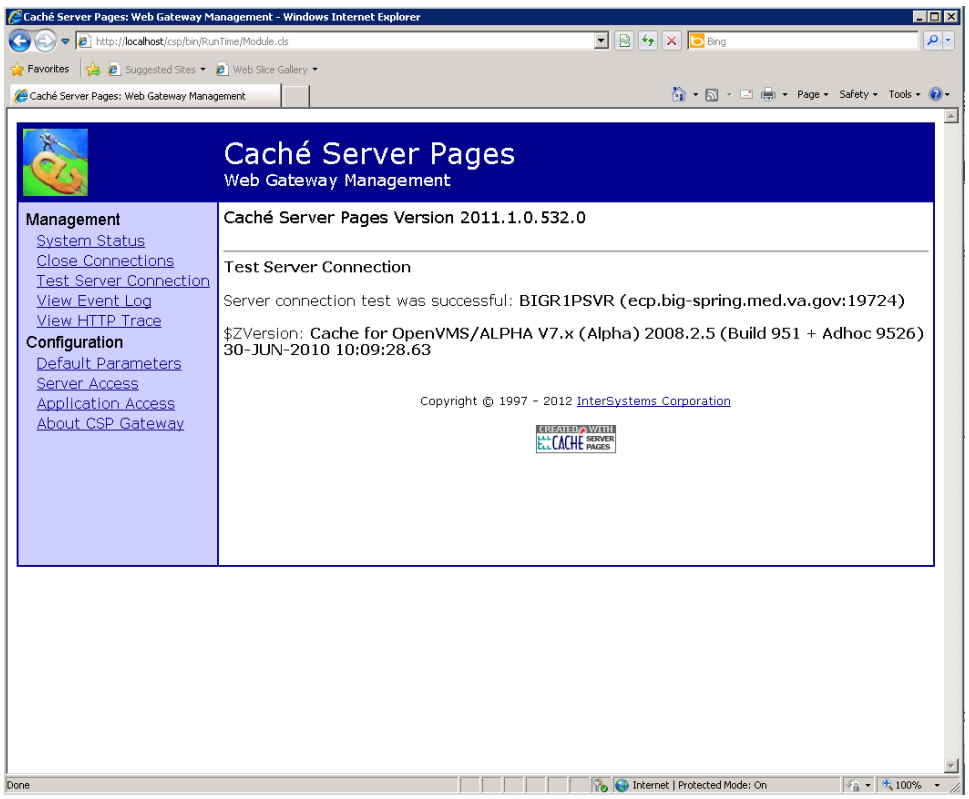



**Caché Server Pages, Server Access page with configuration information**

4. Test the new entry via the Test Server Connection option.

**Caché Server Pages, Test Server Connection page**

5. Verify the server connection test is successful.
   - When all pertinent information is entered and valid for the remote server, the following page displays.
   - If the test is unsuccessful, correct the entry and try the test again. You may need to reset the password of the remote Caché account.

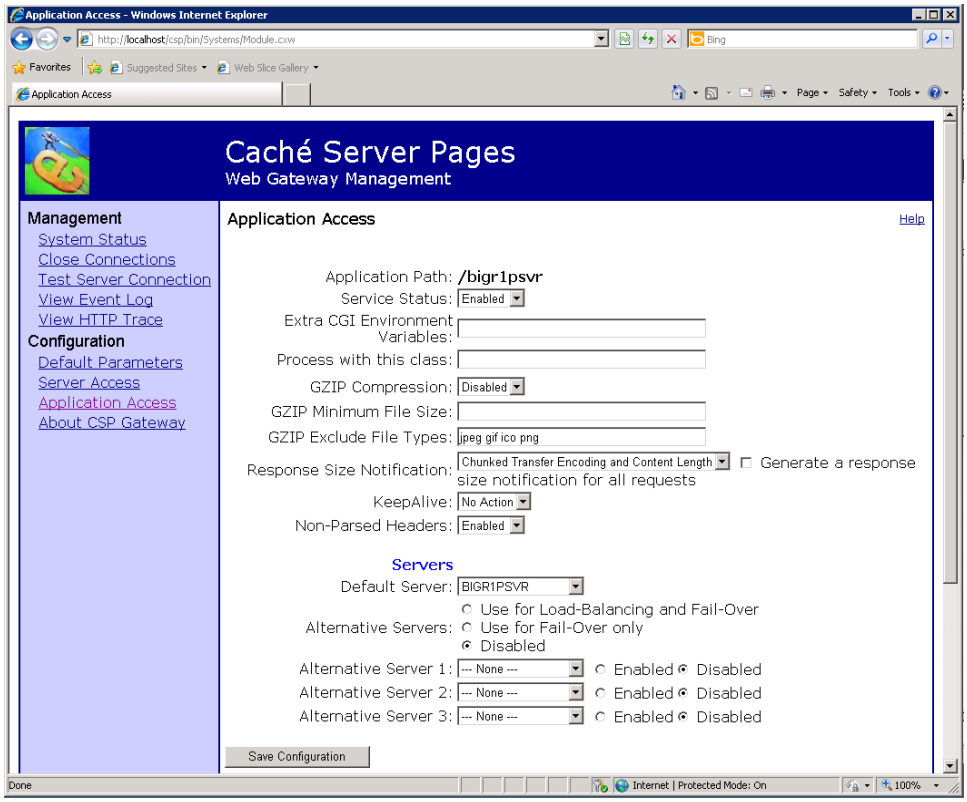



**Caché Server Pages, Server connection test successful page**

6. After a successful server connection test, add an **Application Access** entry for the newly created **Server Access** entry.

7. Enter the name of the site's database instance in lowercase proceeded by a "/".

   **Note:** Be sure you select the appropriate server to map to this application.




**Caché Server Pages, Application Access page**

8. Repeat the steps 1-7 for additional sites that are serviced by this CSP Gateway.

   **Note:** Each site is independent and does not affect the others. Adding additional sites is the same process as adding the first one. However, all sites are affected when the CSP Gateway or the web services are shutdown/restarted.

## Step 6: Windows Server for IIS: Configure/Setup a Remote Web Server Using Caché Server Pages

**Note:** A server manager may assume that Cache is installed on the IIS box, when the web server is configured for CSP Gateway.
The Cache CSP Gateway component must be loaded on the IIS box. After Cache is loaded, the appropriate individual can work on adding Cache instances to CSP Gateway, as well as mapping the HANDLERs.

There are some mappings that are required for IIS to hand off CSP pages to the CSP Gateway. Also some files are best loaded on the web server for caching/less data transmitted from VistA (some BT images).

Web server mappings for CSP Gateways are documented in the Cache documentation. For convenience, Section 4: Web Servers for Microsoft Windows, Section 4.1: Microsoft Internet Information Services Version 7 (IIS v7), and Section 4.2: Microsoft Internet Information Services Version 6 (IIS v6) or Earlier are provided in Appendix A of this installation guide on page 25.

**Note:** In order to activate Secure HTTP (HTTPS), you must obtain a security certificate and load it onto the Web server in IIS. Only web servers require the certificate; the client aspect is built into all web browsers. Instructions for obtaining a security certificate are in Appendix B on page 55.

## Step 7: Copy the bt Folder

Copy and paste the bt folder included in the zip file into the CSP folder of the Cache Installation, e.g., `C:\InterSystems\Cache\CSP`.

## Step 8: Test the URL

Test the URL via a web browser. REDACTED where bigr1psvr is the CSP Gateway application that connects you to the database.

# Additional Information

If you have any questions concerning the implementation of this application, contact the VA Service Desk at 1-888-596-4357 or directly log a Remedy ticket via Remedy Requester application using:
Category: Applications-VistA
Type: Beneficiary Travel
Item: An appropriate BT Dashboard item can be selected from the list

# Software and Documentation

REDACTED

BT Dashboard software and documentation files are available in the following names and formats:

| Title | File Name | FTP Mode |
|---|---|---|
| DGBT Beneficiary Travel | DGBT BENEFICIARY TRAVEL DASHBOARD 1_0.ZIP<br>**Note:** This zip file contains:<br>• **DGBT Beneficiary Travel Dashboard xml** (source code for csp and cls files)<br>• **bt** folder to be placed in the **<cache root>/CSP** folder on the web server | binary |
| Beneficiary Travel (BT) Dashboard Installation Guide | DGBT_1_19IG.DOCX<br>DGBT_1_19IG.PDF | |
| Beneficiary Travel (BT) Dashboard User Manual | DGBT_1_19UM.DOCX<br>DGBT_1_19UM.PDF | |
| Beneficiary Travel (BT) Technical Manual | DGBT_1_19TM.DOC<br>DGBT_1_19TM.PDF | |
| Beneficiary Travel (BT) Dashboard Release Notes | DGBT_1_19RN.DOCX<br>DGBT_1_19RN.PDF | |

BT manuals are available in MS Word (.doc) format and the Portable Document Format (.pdf) on the **VA Software Documentation Library** under Clinical, Beneficiary Travel
http://www.va.gov/vdl/

# Attention: Facility ISOs and Privacy Officers Update your existing site Privacy Impact Assessments (PIA)

You must add the following information to the appropriate Minor Application tab of your existing site PIA.

- Tab 10 is for a minor application that gets security controls from VistA.
- Tab 11 is for a standalone minor application.

| | |
|---|---|
| **Name** | Beneficiary Travel (BT) Dashboard |
| **Description** | BT Dashboard calculates the driving mileage from the patient's address to a configured set of institutions. |
| **Comments** | |
| **Is PII collected by this minor application?** | No |
| **Does this minor application store PII?** | No |
| **If yes, where?** | N/A |
| **Who has access to this data?** | Users with the Claim Enter/Edit [DGBT BENE TRAVEL SCREEN] VistA option (usually travel clerks) |

# Appendix A: IIS Instructions for Using Cache for Remote Web Servers from the *CSP Gateway Configuration Guide*

## Section 4: Web Servers for Microsoft Windows

This section describes how to configure Web Servers from Microsoft and Apache on systems running Windows. Normally you select to configure your Web server to work with CSP when you install Caché. If you do not choose this option during the installation, you can run the Caché installation again and select to install the CSP Gateway components only. Or you can choose to configure your Web server manually to work with CSP. To configure your Web server manually to work with CSP on a system running Windows, use the instructions in this chapter.

If you are using an IIS Web server, you need to follow the directions in this chapter for your configuration to map file extensions to be served by the CSP Gateway.

All Microsoft Web servers can be extended by means of a high-performance API, the Internet Server Application Programming Interface (ISAPI). You can extend the Web server using *ISAPI extensions* implemented as Windows DLLs.

Several connectivity options are available for Apache. The CGI-based solution is the easiest option to install and configure.

The Apache Group also provides support for extensions implemented as dynamically-linked modules (DLLs) and a means through which ISAPI extensions, developed for Microsoft's Web servers, can be utilized.

### Section 4.1: Microsoft Internet Information Services Version 7 (IIS v7)

In this build, the Microsoft ISAPI extensions (CSPms.dll, CSPmsSys.dll and CSPcms.dll) have been adapted such that they can work directly to the Native Modules interface in IIS v7. This is the Web server supplied with Windows Vista and post-2003 releases of Windows Server. This new version is a significant upgrade. This section describes the key differences between the new and old versions of IIS relevant to CSP.

**Note:** These instructions use the Windows Vista Business version. The specifics on your operating system may differ slightly.

IIS v7 is constructed using a modular architecture as opposed to the "one monolithic Web server executable does everything" approach used in previous incarnations. The idea is that customers, at installation time, select only the functionality they need from the list of capabilities supplied by Microsoft. The Web server is constructed using a modular approach. Modules can be freely added to (or taken away from) an existing IIS v7 installation. In other words, IIS v7 is architecturally similar to Apache.

Third party companies (such as InterSystems) can add functionality to the Web server by creating custom modules working to the new *Native Modules API*. The old ISAPI interface (for extensions and filters) which we have relied on in the past for supporting the CSP Gateway, has been deprecated in favor of this API. However, in the interests of backward compatibility, Microsoft supplies a module to support the ISAPI interface. Older versions of the CSP Gateway work through this module.

Microsoft encourages vendors of ISAPI-based applications to rework them so that they can use the Native Module API directly. It is envisaged that suitably reworked modules perform and scale better than their ISAPI-based equivalents.

Microsoft has replaced the IIS configuration "metabase" with a new XML-based configuration schema. Basically, there is a core Web server configuration held in a single file which sets default properties for the whole installation. Defaults held centrally can be overridden in individual *web.config* files that can be used to customize the configuration for each virtual documents root and subdirectories thereof.

Improved security is a key feature of IIS v7 and many of the extra complications in configuring CSP to work with this new server are related to tightened security.

The remainder of this section describes how to configure CSP to work through IIS v7. The configuration procedures for both the new Native Module API and older ISAPI extension based approach are described. Later versions of the CSP Gateway DLLs concurrently support both the new Native Modules interface and older ISAPI interface. Therefore, later versions of what were the IIS ISAPI DLLs (CSPms.dll, CSPmsSys.dll, and CSPcms.dll) work with both IIS v7 (as Native Modules) and previous versions of IIS (as ISAPI extensions).
The examples in this section assume that CSP Gateway Web server components are installed in:
C:\cache-install-dir\csp\
Amend the following steps for your specific installation directory.

## 4.1.1 Installation

Install the CSP Gateway components and the CSP static files as follows:
1. NSD Module (if required)
• CSPnsd.exe
• CSPnsdSv.exe
The default location for these modules is:
C:\cache-install-dir\csp
Given that this location is later mapped to a Web server virtual root it is better, from a security perspective, to install these components in a separate location. For example:
C:\cache-install-dir\nsd
To avoid disrupting existing Gateway installations on upgrading Caché, the installation procedures (for Caché v5.1 and later) place these modules in the following common location. This location is not related to a particular Caché configuration.
C:\Inetpub\CSPGateway\nsd
Run the NSD from within its home directory, C:\Inetpub\CSPGateway\nsd. The configuration file (CSP.INI) and Event Log (CSP.LOG) are written in this directory for NSD-based connectivity options.
2. Native Modules, ISAPI, and CGI Modules (if required). All of the modules listed below are not required for all connectivity options. Refer to the sections describing each option to see which are actually required.
• CSPms.dll (Runtime module)
• CSPmsSys.dll (Systems Management module)
• CSPcms.dll (ISAPI/Native module client to the NSD – if supplied)
• CSPcgi.exe (Runtime module)
• nph-CSPcgi.exe (Copy of CSPcgi)
• CSPcgiSys.exe (Systems Management module)
• nph-CSPcgiSys.exe (Copy of CSPcgiSys)
• CSPmsf1.dll (ISAPI filter – if supplied)
The default location for these modules is:
C:\cache-install-dir\csp\bin
In order to avoid disrupting existing Gateway installations on upgrading Caché, the installation procedures for Caché v5.1 (and later) place these modules in the following common location. This location is not related to a particular Caché configuration.
C:\Inetpub\CSPGateway
The original location (C:\cache-install-dir\csp\bin) is used to hold the Gateway components required for serving the Management Portal for the specific instance of Caché.
The configuration file (CSP.INI) and Event Log (CSP.LOG) are written in this directory for non NSD-based connectivity options.
3. HyperEvents Components
• CSPBroker.js
• CSPBroker.class
• CSPBroker.jar
• cspbrokerBeanInfo.class(Caché version 5.1 and later)
• CSPxmlhttp.js(Caché version 5.1 and later)
The default location for these files is:
C:\cache-install-dir\csp\broker
4. Miscellaneous static resources used by the CSP Samples
A number of static Web resources (such as image files) are required by the CSP Samples. The default location for

these files is:
C:\cache-install-dir\csp\samples
5. Miscellaneous static resources used by the Caché Management Portal (Caché v5.1 and later)
A number of static Web resources (such as image files) are required by the Management Portal. The default location for these files is:
C:\cache-install-dir\csp\sys

## 4.1.2 Determining the Supported Interfaces

As mentioned in the introduction, later versions of the CSP Gateway DLLs support both the new IIS v7 Native Modules interface and the older ISAPI interface. Before configuring IIS to recognize and use the CSP Gateway, check which interfaces are supported by the DLLs supplied with your distribution.
This applies to the following DLLs:
• CSPms.dll
• CSPmsSys.dll
• CSPcms.dll
All versions of these modules support the ISAPI interface. Check whether your Gateway DLLs can operate as IIS v7 Native Modules by looking at the version information in the DLL properties. (In Windows Explorer, right-click the DLL and select
**Properties**). If the **Interface** property is:
**IIS ISAPI and IIS Native Module**
then the DLL supports the old ISAPI and new Native Module interfaces. If the **Interface** property is not defined or is **IIS**
**ISAPI**, then get newer DLLs from InterSystems, or install and use the Microsoft ISAPI emulation module instead.
Later versions of Windows (Vista and later) do not display all file properties by default so the supported interfaces are also listed in the main file description field. For example:
Native module supported:
```
CSP for IIS-ISAPI/NativeModule (1107)
```
Native module not supported:
```
CSP for IIS-ISAPI (1107)
```
The InterSystems development reference for upgrading these DLLs to work as Native Modules for IIS v7 is: CMT466.

## 4.1.3 Installing the ISAPI and CGI Services (If Required)

**Note:** Install these services if they are required. These services are required to support configuration Options 2, 3, 4 and 5 only. These ISAPI and CGI services are not required if the new Gateway Native Modules solution is used (Option 1).
IIS v7 does not, by default, run **ISAPI extension**, **ISAPI filters**, or **CGI modules**. If these services are required in order to run applications that depend on these interfaces, you must install them.
Note that, with the **ISAPI extensions** service installed, all versions of the CSP Gateway that have ever been built (even those shipped with Caché v4) work with IIS v7.
Install these legacy services through the Windows Control Panel.
1. Open the Windows Control Panel.
2. Select **Programs and Features** and select **Turn Windows Features on or off**.
3. Navigate to **Internet Information Services** and expand **World Wide Web Services** and **Application Development Features**.
Select **ISAPI Extensions**. Also select **ISAPI Filters** and **CGI**, if these additional services are required. Click **OK**
4. In the Windows **Control Panel**, open **Administrative Tools** and **Internet Information Services (IIS) Manager**.
5. In the left panel, highlight **[MACHINE_NAME] ([machine_name]\[user_name])**
6. In the middle panel, double-click the **Modules** icon.
7. In the right panel, click **Add Native Module**.
8. In the left panel, expand the top level, expand **Web Sites** and expand **Default Web Site**
```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

9. In the middle panel, double-click **Handler Mappings**.
10. In the middle panel, highlight the **ISAPI-dll** handler.
11. In the right panel, click **Edit Handler Permissions**.
12. Select **Execute** and click **OK**. This allows ISAPI extensions to be invoked through direct calls to the name of the ISAPI DLL.

## 4.1.4 Setting Permissions for the Gateway Components

Regardless of which CSP Gateway configuration option you choose, appropriate permissions should be assigned to all Web resources held outside the standard IIS documents root (for example, C:\inetpub\wwwroot).
IIS v7 does not, by default, allow the user of a Web application to access anything outside the scope of the pre-configured documents root unless you assign Read and Execute permissions for those external resources to the following user/groups:
**[machine_name]\IIS_IUSRS**
And:
**[machine_name]\Users**
It should be noted that **IIS_IUSRS** represents the user (group) under which IIS worker processes operate. It essentially replaces the more familiar **IUSR_[machine_name]** user group found in earlier versions of IIS. Applications controlled through IIS (such as the CSP Gateway) operate with the level of privilege assigned to **IIS_IUSRS**.
For CSP, resources external the Web server's root usually include the following:
Gateway binary components:
C:\inetpub\CSPGateway
Static file components:
*cache-install-dir*\CSP\
Permissions can be manually assigned to these folders via Windows Explorer as follows:
1. Right click the folder name and select **Properties**.
2. Click the **Security** tab.
3. Click **Edit**.
4. Click **Add**.
5. In the **Enter the object names to** text box enter:
`[machine_name]\IIS_IUSRS`
6. Click **Check Names** and **OK**.
7. Select **[machine_name]\IIS_IUSRS** in the **Group or User names** window, then:
8. Assign **Read & Execute** permissions in the **Permissions** window.
9. Click **Apply** and **OK**.
10. Repeat the above process for the **[machine_name]\Users** user group.
As with previous versions of IIS, full read and write permissions for the Gateway configuration and event log files (CSP.ini
and CSP.log) should be assigned to the IIS user group. For example, at the Windows command prompt, enter:

```
cacls CSP.ini /E /G IIS_IUSRS:F
cacls CSP.log /E /G IIS_IUSRS:F
```

Of course, this can also be done via Windows Explorer.

## 4.1.5 Configuring the CSP Application Path

This section describes the procedure for configuring the CSP application path (such as /csp) in IIS v7. These procedures are common to all CSP Gateway configuration options.
As with previous version, IIS v7 is configured in the **Internet Information Services (IIS) Manager** control panel. Subdirectories configured under the documents root can either be classed as **Virtual** or **Applications**. **Virtual** subdirectories (or aliases) are mapped to physical equivalents (windows directories). The same applies to subdirectories classed as **Applications** except that, in addition to defining the physical equivalent, you can associate the application with a particular application pool (the default of which is **DefaultAppPool**).
Since CSP applications are served through the CSP Gateway, the hosting subdirectories (such as/csp) should be configured as **Applications**.

In a default CSP configuration, the /csp application path is mapped to the physical location *install-dir*\CSP. All the static files are located under this root (/csp/broker…).

1. Open the **Internet Information Services (IIS) Manager**.
2. In the left panel, expand the top level to reveal the **Web Sites** section, then the **Default Web Site** section. Highlight the **Default Web Site** section:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

3. In the right panel, click **View Applications**.
4. Again in the right panel click **Add Application**.
5. In the **Add Application** dialogue, enter:

Alias: **csp**
Physical path: *install-dir*\CSP\

6. Click **OK**.

If you are using a CSP Gateway solution based on (or involving) ISAPI or CGI (Options 2, 3, 4, 5), set up an application called /bin under the /csp application. Map this to the physical directory holding the Gateway binaries. For example:

Map application /csp/bin to C:\inetpub\CSPGateway

## 4.1.6 .Bitness — Running 32-bit Applications on 64-bit Servers

**Note:** This section applies to modules that are loaded into the address space of the hosting web serve: ISAPI Extensions and Native Modules (CSPms[Sys].dll and CSPcms.dll). CGI modules are not affected since they run as a detached process with respect to IIS.

With 64 bit Windows 2003 installations, IIS 6.0 could be configured to either run in 32 bit mode or 64 bit mode. The **Enable32bitAppOnWin64** metabase key could be toggled and all worker process would run in the selected bitness mode.

This setting applied to the whole IIS installation (that is, it was globally applied to all Application Pools managed by the server).

With IIS 7.0, the **Enable32bitAppOnWin64** setting has been moved down to the Application Pool level. Therefore it is now possible to set the bitness for a particular Application Pool. In other words, it is possible, within a single server installation, to configure one Application Pool to run native 64-bit applications and another to run 32-bit applications.

To access the bitness setting for an Application Pool, enter the IIS control panel:

1. Click **Application Pools** in the left hand panel.
2. Select the appropriate Application Pool.
3. Click **Advanced Settings** in the right hand panel.
4. The **Advanced Settings** dialogue appears. The **Enable 32-Bit Applications** setting is found in the **General** section. This can be set to `True` or `False`.

Incidentally, this configuration setting can be manipulated at the Windows Command line using the *appcmd* command.

For example:

```
appcmd set apppool \
/apppool.name:DefaultAppPool/enable32bitapponwin64:true
```

This sets the Application Pool `DefaultAppPool` to run in 32 bit mode.

It is also possible to list the Application Pools based on bitness using the *appcmd* command. For example, to list all the application pools running in 64 bit mode use the following command:

```
appcmd list apppools /enable32bitapponwin64:false
```

Finally, since application pools can be run in different bitness modes it is necessary to ensure that Native Modules (and ISAPI extensions) that are loaded by the Application Pool are themselves of the correct bitness for the pool. For example, if the hosting application pool is 64-bit then the 64-bit Gateway modules (such as CSPms[Sys].dll) must be used. If the hosting Application Pool is 32-bit then the 32-bit Gateway modules must be used instead.

The bitness check for individual modules is done via a *preCondition* in the module's web.config file. For the CSP Gateway, this file typically looks something like the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.webServer>
```

```
<handlers>
<add name="CSPGateway_All" path="*" verb="*" \
modules="CSPms" \
resourceType="Unspecified" \
preCondition="bitness64" />
</handlers>
<security>
<requestFiltering>
<hiddenSegments>
<remove segment="bin" />
</hiddenSegments>
</requestFiltering>
</security>
</system.webServer>
</configuration>
```

Note the bitness setting in the *precondition* clause. In this case bitness is set to `bitness64` which means that IIS checks for 64-bit Gateway modules operating in a 64-bit Application Pool.

If a 32-bit Application Pool is used then the 32-bit Gateway modules must be used and the *preCondition* set to `bitness32`.

If there is an inconsistency between the modules installed, the precondition clause, and/or the expectations of the hosting Application Pool, IIS returns an error condition similar to the one shown below.

```
Error:
The module(s) assigned to this handler mapping has the following preconditions that are not
present in the handler mapping:
bitness64
Runtime errors may occur if a handler mapping does not have a set of preconditions that are
equally as restrictive as, or more restrictive, than the module(s) assigned to the mapping.
Please ensure that this handler mapping has the correct preconditions, and that the
preconditions are not in conflict.
```

## 4.1.7 Request Filtering Module

Request Filtering is a built-in security feature that was introduced in IIS 7.0 (and later), and replaces much of the functionality that was previously available through the UrlScan add-on for IIS 6.0. All of the settings for the request filtering feature are located within the <requestFiltering> element in the main configuration file.

```
C:\Windows\System32\inetsrv\config\applicationHost.config
```

When request filtering blocks an HTTP request, IIS 7.0 returns an `HTTP 404` error to the client and supplement the HTTP status with a unique sub-status that identifies the reason that the request was denied. A list of the error codes returned is shown in the following table.

**HTTP Substatus Description**

404.5 URL Sequence Denied
404.6 Verb Denied
404.7 File Extension Denied
404.8 Hidden Namespace
404.10 Request Header Too Long
404.11 URL Double Escaped
404.12 URL Has High Bit Chars
404.13 Content Length Too Large
404.14 URL Too Long
404.15 Query String Too Long
404.18 Query String Sequence Denied
404.19 Denied by Filtering Rule

The code perhaps most relevant to CSP is 404.11 (URL Double Escaped). This is because of the extent to which the escape introduction character (%) is used in CSP file/resource names.

For example, consider the following URL:

```
/csp/user/%25DeepSee.UI.Dialog.finderDialog.zen
```

If the IIS request filter is configured to reject requests considered to contain double escaped entities this request fails with the following error:

```
HTTP Error 404.11 - Not Found
```

The request filtering module is configured to deny a request that contains a double escape sequence.

Explanation:

The problem lies in the `%25DeepSee` part of the file name (`%DeepSee`). Specifically, consider the first four bytes after the escape introduction character (%):

```
%25De
```

Because characters `D` and `e` are valid hexadecimal digits the request filter recognizes this sequence as a double escaped entity and, as a result, rejects the request.

The solution to this problem is to either avoid using the % character in file names or configure the web server's request filter to ignore what it would otherwise recognize as double escaped sequences.

The following command prevents the request filter from applying the double-escaping filer:

```
appcmd set config /section:requestfiltering /allowdoubleescaping:true
```

The `appcmd` is found in the following location:

```
C:\Windows\System32\inetsrv\
```

## 4.1.8 Note on Mapping CSP File Extensions

For any of the options below, you will tell the CSP Gateway what file extensions you want it to handle, either by file extension or by path. IIS7 has a utility called `Add Wildcard Script Mapping`. Do NOT use this utility for this file extension mapping process! Instead, use the utility called `Add Module Mapping for *`. If you use the `Add Wildcard Script Mapping` utility, you get an error.

## 4.1.9 Manual Step for Enabling URLs with /bin

If you installed the CSP Gateway using the Cache installer, this step was done automatically for you. If you are installing the CSP Gateway manually, you need to do this step. (See this external web site for more details and alternative ways to accomplish this http://weblogs.asp.net/owscott/archive/2008/03/05/iis7-blocks-viewing-access-to-files-in-bin-and-otherasp-net-folders.aspx.) To enable URLs that contain /bin, add the following location tag to your applicationHost.config file:

```
<location path="sitename.com/subfolder/bin/debug">
<system.webServer>
<security>
<requestFiltering>
<hiddenSegments>
<remove segment="bin" />
</hiddenSegments>
</requestFiltering>
</security>
</system.webServer>
</location>
```

## 4.1.10 Option 1: (Recommended) Using the Native Modules (CSPms*.dll)

This is the preferred (and default) configuration option. It uses the new Native Modules interface supplied with IIS v7. This option provides the best performance.

Configure the Web server so that it recognizes CSP requests (files of type .csp, .cls, and .zen) and passes them to the CSP Gateway for processing. Include any additional files that might be required for your installation (such as, for example, special CSP resources needed for DeepSee).

### 4.1.10.1 Registering the Native Modules

DLLs: CSPms.dll and CSPmsSys.dll

Before these modules can be used they must be registered with IIS. This is done in the **Internet Information Services (IIS) Manager** control panel.

1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, highlight: **[MACHINE_NAME] ([machine_name]\[user_name])**

3. In the middle panel, double-click the **Modules** icon.
4. In the right panel, click **Add Native Module** (or **Configure Native Modules**).The precise wording depends on the build of IIS in use.
5. Click **Register** and enter the following in the **Register Native Module** dialogue:
Name: **CSPms**
Path: C:\inetpub\CSPGateway\CSPms.dll
Click **OK**.
6. In the left panel, expand the top level and expand **Web Sites**, and **Default Web Site**. Highlight **Default Web Site**:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

7. In the right panel, click **Add Native Module**.
8. Select **CSPms** (and **CSPmsSys** where appropriate) and click **OK**.

### 4.1.10.2 Mapping the CSP File Extensions

Map the CSP file extensions to the CSP Gateway Native Modules as follows:

**Extension Native Module Binary**

*.csp CSPms C:\inetpub\CSPGateway\CSPms.dll
*.cls CSPms C:\inetpub\CSPGateway\CSPms.dll
*.zen CSPms C:\inetpub\CSPGateway\CSPms.dll
*.cxw CSPms C:\inetpub\CSPGateway\CSPms.dll

1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, expand the top level and expand **Web Sites**, then the **Default Web Site** section. Highlight **Default Web Site**:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

**Note:** This activates CSP for the whole web site. To restrict the use of CSP to specific virtual sub-directories (such as /csp/) focus control on the appropriate subdirectory (under **Default Web Site**) before creating the mappings. Repeat the process for each virtual subdirectory from which CSP content is to be served.
3. In the middle panel, double-click the **Handler Mappings** icon.
4. In the right panel, click **Add Module Mapping**.
5. In the **Add Module Mappings** dialogue, enter the following details:
Request Path: *.csp
Module: (select **CSPms** from the dropdown)
Name:CSPGateway_csp
6. Click **Request Restrictions**.
clear: **Invoke handler only if request is mapped to**
7. Click **OK** to return to the **Add Module Mappings** dialogue and click **OK** again.
8. Repeat the above process to add the following two Module Mappings:
Request Path: *.cls
Module: (select CSPms from the list)
Name:CSPGateway_cls
Request Path: *.zen
Module: (select CSPms from the list)
Name:CSPGateway_zen
Request Path: *.cxw
Module: (select CSPms from the list)
Name: CSPGatewayManagement

### 4.1.10.3 Registering Additional File Types with CSP

To configure additional file types to be processed by CSP, replicate the configuration created for the usual file extensions (that is,.csp,. .cls, .zen) for the new file extension(s).

If you need to serve other static files through the CSP Gateway or need to access the Management Portal through this web server, add mappings for file types .jpg, .gif, .png, and .js.
To map requests for all files to CSP for a given path, set up the following wildcard entry for that path:
**Extension Native Module Binary**
* CSPms C:\inetpub\CSPGateway\CSPms.dll

### 4.1.10.4 Operating and Managing the Gateway

To access the CSP Gateway's systems management suite, point your browser at the following location:
http://<ip_address>/csp/bin/Systems/Module.cxw
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension. For example:
http://<ip_address>/csp/samples/menu.csp
If you see an unauthorized user error message, refer to the security notes in the section CSP Gateway and Security.

## 4.1.11 Option 2: Using the ISAPI Modules (CSPms*.dll)

Use this option if your CSP Gateway DLLs are unable to support the Native Module interface (Option 1). This is the default (and best performing) solution that was supplied for earlier versions of IIS.
IIS v7 does not, by default, run **ISAPI extensions**, **ISAPI filters** or **CGI modules**. This option requires the **ISAPI extensions** service.
Follow the instructions in the section Installing the ISAPI and CGI Services (If Required) for installing and configuring the ISAPI extensions service.
The Web server should be configured such that it recognizes CSP requests (files of type .csp, .cls, and .zen) and passes them to the CSP Gateway for processing.

### 4.1.11.1 Enabling the ISAPI Extensions

DLLs: CSPms.dll and CSPmsSys.dll
Before these extensions can be used they must be registered with IIS as being "Allowed" applications. This is done in the **Internet Information Services (IIS) Manager** control panel.
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, highlight**[MACHINE_NAME] ([machine_name]\[user_name])**
3. In the middle panel, double-click **ISAPI and CGI Restrictions**.
4. In the right panel, click **Add**.
5. In the **Add ISAPI or CGI Restriction** dialogue, enter the following details:
ISAPI or CGI Path: C:\inetpub\CSPGateway\CSPms.dll
Description: CSPGatewayRunTime
Allow extension path to execute: Select
Click **OK**

### 4.1.11.2 Mapping the CSP File Extensions

Choose *one* of the following configuration methods:
1. Serve all content (including static content) from Cache. Map * to the CSP Gateway. Follow the file map procedure in
the section "Registering Additional File Types with CSP" in this book.
2. Serve static content from the web server. Map *only* files of type .csp, .cls, .zen, .cxw to the CSP Gateway.
If you are serving static files from the Web server, map the CSP file extensions to the CSP Gateway ISAPI extensions as follows:
**Extension Binary**
*.csp C:\inetpub\CSPGateway\CSPms.dll
*.cls C:\inetpub\CSPGateway\CSPms.dll
*.zen C:\inetpub\CSPGateway\CSPms.dll
*.cxw C:\inetpub\CSPGateway\CSPms.dll
1. Open the **Internet Information Services (IIS) Manager** window.

2. In the left panel expand the top level to reveal the **Web Sites** section, then the **Default Web Site** section. Highlight the **Default Web Site** section:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

**Note:** This activates CSP for the whole web site. To restrict the use of CSP to specific virtual sub-directories (such as /csp/) focus control on the appropriate subdirectory (under **Default Web Site**) before creating the mappings. Repeat the process for each virtual subdirectory from which CSP content is to be served.

3. In the middle panel, double-click the **Handler Mappings** icon.
4. In the right panel, click **Add Script Map**.
5. In the **Add Script Map** dialogue, enter:

Request Path: *.csp
Executable: C:\inetpub\CSPGateway\CSPms.dll
Name: CSPGateway_csp

6. Click **Request Restrictions**.

Clear: **Invoke handler only if request is mapped to**
Click **OK** to return to **Add Script Map** dialogue.
Click **OK**.

7. At this point you may be prompted as follows:

"Would you like to enable this ISAPI extension? If yes, we add your extension as an "Allowed" entry in the ISAPI and CGI Restrictions list. If the extension already exists we allow it."

Click **Yes**.

You can later find the list of allowed applications as follows:
In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
In the middle panel, double-click **ISAPI and CGI Restrictions**.
If the Gateway ISAPI components are not included in the list of allowed applications then add them (as you would have done for IIS v6):
You can add text of your own choice in the **Description** field. For example:

```
CSPGatewayManagement for CSPmsSys.dll
CSPGatewayRunTime for CSPms.dll
```

8. Repeat the above process: Use the **Add Script Map** dialogue to enter the following two mappings:

Request Path: *.cls
Executable: C:\inetpub\CSPGateway\CSPms.dll
Name: CSPGateway_cls
Request Path: *.zen
Executable: C:\inetpub\CSPGateway\CSPms.dll
Name: CSPGateway_zen
Request Path: *.cxw
Executable: C:\inetpub\CSPGateway\CSPms.dll
Name: CSPGatewayManagement

### 4.1.11.3 Operating and Managing the Gateway

To access the CSP Gateway's systems management suite, point your browser at one of the following locations:
http://<ip_address>/csp/bin/Systems/Module.cxw
http://<ip_address>/csp/bin/CSPmsSys.dll
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension. For example:
http://<ip_address>/csp/samples/menu.csp
If you see an unauthorized user error message, refer to the section "CSP Gateway and Security."

## 4.1.12 Option 3: Using a Native Module with the NSD (CSPcms.dll)

IIS v7 does not, by default, run **ISAPI extensions**, **ISAPI filters**, or **CGI modules**. This option requires the **CGI modules** service for running the Gateway Management module (nph-CSPcgiSys.exe).

Follow the instructions in the section for installing the CGI service, Installing the ISAPI and CGI Services (If Required.
Configure the Web server so that it recognizes CSP requests (files of type .csp, .cls, and .zen) and passes them to the CSP Gateway for processing.

### 4.1.12.1 Registering the Runtime Native Module

DLL: CSPcms.dll
Before this module can be used it must be registered with IIS. This is done in the **Internet Information Services (IIS) Manager** control panel.
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
3. In the middle panel, double-click the **Modules** icon.
4. In the right panel, click **Add Native Module**.
5. Click **Register** and enter the following details in the **Register Native Module** dialogue:
Name: CSPcms
Path: C:\inetpub\CSPGateway\CSPcms.dll
Click **OK**.
6. In the left panel expand the top level to reveal the **Web Sites** section, then the **Default Web Site** section. Highlight the **Default Web Site** section:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

7. In the right panel, click **Add Native Module**.
8. In the **Add Native Module** dialogue select **CSPcms** then click **OK**.

### 4.1.12.2 Enabling the CGI module for Gateway Management

Executable: nph-CSPcgiSys.exe
Before this module can be used it must be registered with IIS as being an Allowed application. This is done in the **Internet**
**Information Services (IIS) Manager** control panel.
1. Open the **Internet Information Services (IIS) Manager**.
2. In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
3. In the middle panel, double-click the **ISAPI and CGI Restrictions** icon.
4. In the right panel, click **Add**.
5. In the **Add ISAPI or CGI Restriction** dialogue, enter:
ISAPI or CGI Path: C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
Description: CSPGatewayManagement
Allow extension path to execute: Select
Click **OK**.

### 4.1.12.3 Mapping the CSP File Extensions

Choose *one* of the following configuration methods:
1. Serve all content (including static content) from Cache. Map * to the CSP Gateway. If you are configuring CSP so that the Cache server serves all static files, then follow the file map procedure in the section "Registering Additional File Types with CSP" in this book.
2. Serve static content from the web server.
Map *only* files of type .csp, .cls, .zen, .cxw to the CSP Gateway.
If you are serving static files from the Web server, map the CSP file extensions to the CSP Gateway Modules as follows:
**Extension Native Module Binary**
*.csp CSPms C:\inetpub\CSPGateway\CSPms.dll

*.cls CSPms C:\inetpub\CSPGateway\CSPms.dll
*.zen CSPms C:\inetpub\CSPGateway\CSPms.dll
*.cxw C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, expand the top level to reveal the **Web Sites** section, then the **Default Web Site** section. Highlight the **Default Web Site** section:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

**Note:** This activates CSP for the whole web site. To restrict the use of CSP to specific virtual sub-directories (such as /csp/) focus control on the appropriate subdirectory (under **Default Web Site**) before creating the mappings. Repeat the process for each virtual subdirectory from which CSP content is to be served.
3. In the middle panel, double-click the **Handler Mappings** icon.
4. In the right panel, click **Add Module Mapping**.
5. In the **Add Module Mappings** dialogue, enter:
Request Path: *.csp
Module: Select CSPcms
Name: CSPGateway_csp
6. Click **Request Restrictions**.
clear: **Invoke handler only if request is mapped to**
Click **OK** to return to the **Add Module Mappings** dialogue.
Click **OK**.
7. Repeat the above process to add the following Module Mappings:
Request Path: *.cls
Module: Select **CSPcms**
Name: CSPGateway_cls
and
Request Path: *.zen
Module: Select **CSPcms**
Name: CSPGateway_zen
8. In the left panel, highlight the **Default Web Site** section:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

9. In the middle panel, double-click the **Handler Mappings** icon.
10. In the right panel, click **Add Script Map**.
11. In the **Add Script Map** dialogue, enter:
Request Path: *.cxw
Executable: C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
Name: CSPGatewayManagement
12. Click **Request Restrictions**.
clear: **Invoke handler only if request is mapped to**
Click **OK** to return to the **Add Script Map** dialogue.
Click **OK**.
13. You may be prompted as follows: “Would you like to enable this ISAPI extension? If yes, we add your extension as
an “Allowed” entry in the ISAPI and CGI Restrictions list. If the extension already exists we allow it.”
Click **Yes**.
You can later find the list of allowed applications as follows:
In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
In the center panel, double-click the **ISAPI and CGI Restrictions** icon.
If the Gateway Management CGI module is not included in the list of allowed applications, add it (as you would have
done for IIS v6):
You can add text of your own choice in the **Description** field. For example:

```
CSPGatewayManagement for nph-CSPcgiSys.exe
```

### 4.1.12.4 Operating and Managing the Gateway

This connectivity option depends on the CSP Gateway's Network Service Daemon (NSD).
Start the CSP NSD as described in the section, *Starting the NSD*.
Although CSP pages are served through the higher-performing module (CSPcms.dll), the Gateway's management suite is accessed through the CGI module dedicated to this purpose (nph-CSPcgiSys.exe).
To access the CSP Gateway's Systems Management suite, point your browser at one of the following locations:
http://<ip_address>/csp/bin/Systems/Module.cxw
http://<ip_address>/csp-bin/nph-CSPcgiSys
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension. For example:
http://<ip_address>/csp/samples/menu.csp
If you see an unauthorized user error message, refer to the section *CSP Gateway and Security*.

## 4.1.13 Option 4: Using an ISAPI Module with the NSD (CSPcms.dll)

Use this option if your CSP Gateway DLLs are unable to support the Native Module interface (Option 2).
IIS v7 does not, by default, run **ISAPI extensions**, **ISAPI filters** or **CGI modules**. This option requires both the **ISAPI extensions** and the **CGI modules** service.
Follow the instructions in section for installing and configuring the ISAPI extensions and CGI service.
The Web server should be configured such that it recognizes CSP requests (files of type .csp, .cls, and .zen) and passes them to the CSP Gateway for processing.

### 4.1.13.1 Enabling the Runtime ISAPI Extension

DLLs: CSPcms.dll
Before this extension can be used it must be registered with IIS as being "Allowed" applications. This is done in the **Internet Information Services (IIS) Manager** control panel.
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, highlight: **[MACHINE_NAME] ([machine_name]\[user_name])**
3. In the middle panel, double-click the **ISAPI and CGI Restrictions** icon.
4. In the right panel, click **Add**.
5. In the **Add ISAPI or CGI Restriction** dialogue, enter:
ISAPI or CGI Path: C:\inetpub\CSPGateway\CSPcms.dll
Description: CSPGatewayRunTime
Allow extension path to execute: Select
Click **OK**

### 4.1.13.2 Enabling the CGI module for Gateway Management

Executable: nph-CSPcgiSys.exe
Before this module can be used it must be registered with IIS as being an "Allowed" application. This is done in the **Internet Information Services (IIS) Manager** control panel.
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, highlight: **[MACHINE_NAME] ([machine_name]\[user_name])**
3. In the middle panel, double-click the **ISAPI and CGI Restrictions** icon.
4. In the right panel, click **Add**.
5. In the **Add ISAPI or CGI Restriction** dialogue, enter:
ISAPI or CGI Path: C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
Description: CSPGatewayManagement
Allow extension path to execute: Select
Click **OK**.

### 4.1.13.3 Mapping the CSP File Extensions

Choose *one* of the following configuration methods:
1. Serve all content (including static content) from Cache. Map * to the CSP Gateway. If you are configuring CSP so that the Cache server serves all static files, then follow the file map procedure in the section "Registering Additional File Types with CSP" in this book.
2. Serve static content from the web server.
Map *only* files of type .csp, .cls, .zen, .cxw to the CSP Gateway.
If you are serving static files from the Web server, map the CSP file extensions to the CSP Gateway Modules as follows:

**Extension Binary**
*.csp C:\inetpub\CSPGateway\CSPcms.dll
*.cls C:\inetpub\CSPGateway\CSPcms.dll
*.zen C:\inetpub\CSPGateway\CSPcms.dll
*.cxw C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, expand the top level and expand**Web Sites**. Highlight **Default Web Site** .:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

**Note:** This activates CSP for the whole web site. To restrict the use of CSP to specific virtual sub-directories (such as /csp/) focus control on the appropriate subdirectory (under **Default Web Site**) before creating the mappings. Repeat the process for each virtual subdirectory from which CSP content is to be served.
3. In the middle panel, double-click **Handler Mappings**.
4. In the right panel, click **Add Script Map**.
5. In the **Add Script Map** dialogue, enter:
Request Path: *.csp
Executable: C:\inetpub\CSPGateway\CSPcms.dll
Name: CSPGateway_csp
6. Click **Request Restrictions**.
clear: **Invoke handler only if request is mapped to**
Click **OK** to return to the 'Add Script Map' dialogue.
Click **OK**.
7. At this point you may be prompted as follows:
"Would you like to enable this ISAPI extension? If yes, we add your extension as an "Allowed" entry in the ISAPI and CGI Restrictions list. If the extension already exists we allow it."
Click **Yes**.
You can later find the list of allowed applications as follows:
In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
In the middle panel, double-click the **ISAPI and CGI Restrictions** icon.
If the Gateway ISAPI module is not included in the list of allowed applications then it should be added (as you would have done for IIS v6):
You can add text of your own choice in the **Description** field. For example:

```
CSPGatewayRunTime for CSPcms.dll
CSPGatewayManagement for nph-CSPcgiSys.exe
```

8. Repeat the above process: Use the **Add Script Map** dialogue to enter the following two mappings:
Request Path: *.cls
Executable: C:\inetpub\CSPGateway\CSPcms.dll
Name: CSPGateway_cls
Request Path: *.zen
Executable: C:\inetpub\CSPGateway\CSPcms.dll
Name: CSPGateway_zen
Request Path: *.cxw
Executable: C:\inetpub\CSPGateway\nph-CSPcgiSys.exe

Name: CSPGatewayManagement

### 4.1.13.4 Operating and Managing the Gateway

This connectivity option depends on the CSP Gateway's Network Service Daemon (NSD).
1. Start the CSP NSD as described in the section dedicated to this service.
Although CSP pages are served through the higher-performing ISAPI module (CSPcms.dll), the Gateway's management suite is accessed through the CGI module dedicated to this purpose (nph-CSPcgiSys.exe).
To access the CSP Gateway's Systems Management suite, point your browser at one of the following locations:
http://<ip_address>/csp/bin/Systems/Module.cxw
http://<ip_address>/csp-bin/nph-CSPcgiSys
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension. For example:
http://<ip_address>/csp/samples/menu.csp
If you see an unauthorized user error message, refer to the section "CSP Gateway and Security."

## 4.1.14 Option 5: Using the CGI Modules with the NSD (nph-CSPcgi*.exe)

In most cases, the all-inclusive Native Module-based solution (Option 1) is the option of choice, and is the implementation that gives the best performance. The CGI/NSD hybrid is useful for cases where it is necessary, for operational reasons, to manage the Gateway independently of the hosting Web server. For example, if multiple instances of the Web server are to share the same Gateway installation. In option 1 each instance of the core Web server process binds to its own instance of the Gateway.
Another factor in choosing this approach might be that the in-house requirements of your Web master (or ISP) dictate that all Web server extensions are implemented using the CGI protocol.
IIS v7 does not, by default, run **ISAPI extensions**, **ISAPI filters** or **CGI modules**. This option requires the **CGI modules** service.
Follow the instructions in section for installing and configuring the CGI service.
Configure the Web server so that it recognizes CSP requests (files of type .csp, .cls, and .zen) and passes them to the CSP Gateway for processing.

### 4.1.14.1 Enabling the CGI Modules

Executables: nph-CSPcgi.exe and nph-CSPmsSys.exe
Before these modules can be used they must be registered with IIS as being "Allowed" applications. This is done in the **Internet Information Services (IIS) Manager** control panel.
1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
3. In the middle panel, double-click the **ISAPI and CGI Restrictions** icon.
4. In the right panel, click **Add**.
5. In the **Add ISAPI or CGI Restriction** dialogue, enter:
ISAPI or CGI Path: C:\inetpub\CSPGateway\nph-CSPcgi.exe
Description: CSPGatewayRunTime
Allow extension path to execute: Select
Click **OK**.
6. Repeat the above steps for nph-CSPcgiSys.exe, entering the following details in the **Restrictions** dialogue:
ISAPI or CGI Path: C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
Description: CSPGatewayManagement
Allow extension path to execute: Select

### 4.1.14.2 Mapping the CSP File Extensions

Choose *one* of the following configuration methods:
1. Serve all content (including static content) from Cache. Map * to the CSP Gateway. If you are configuring CSP so

that the Cache server serves all static files, then follow the file map procedure in the section "Registering Additional File Types with CSP" in this book.
2. Serve static content from the web server.
Map *only* files of type .csp, .cls, .zen, .cxw to the CSP Gateway.
If you are serving static files from the Web server, map the CSP file extensions to the CSP Gateway CGI Modules as follows:

**Extension Binary**

*.csp C:\inetpub\CSPGateway\nph-CSPcgi.exe
*.cls C:\inetpub\CSPGateway\nph-CSPcgi.exe
*.zen C:\inetpub\CSPGateway\nph-CSPcgi.exe
*.cxw C:\inetpub\CSPGateway\nph-CSPcgiSys.exe

1. Open the **Internet Information Services (IIS) Manager** window.
2. In the left panel expand the top level to reveal the **Web Sites** section, then the **Default Web Site** section. Highlight the **Default Web Site** section:

```
[MACHINE_NAME] ([machine_name]\[user_name])
Web Sites
Default Web Site
```

**Note:** This activates CSP for the whole web site. To restrict the use of CSP to specific virtual sub-directories (such as /csp/) focus control on the appropriate subdirectory (under **Default Web Site**) before creating the mappings. Repeat the process for each virtual subdirectory from which CSP content is to be served.
3. In the middle panel, double-click the **Handler Mappings** icon.
4. In the right panel, click **Add Script Map**.
5. In the **Add Script Map** dialogue, enter:
Request Path: *.csp
Executable: C:\inetpub\CSPGateway\nph-CSPcgi.exe
Name:CSPGateway_csp
6. Click **Request Restrictions**.
Clear: **Invoke handler only if request is mapped to**
Click **OK** to return to the **Add Script Map** dialogue.
Click **OK**.
7. At this point you may be prompted as follows: "Would you like to enable this ISAPI extension? If yes, we add your extension as an "Allowed" entry in the ISAPI and CGI Restrictions list. If the extension already exists we allow it."
Click **Yes**.
8. You can later find the list of allowed applications as follows:
In the left panel, highlight:
**[MACHINE_NAME] ([machine_name]\[user_name])**
In the middle panel, double-click the **ISAPI and CGI Restrictions** icon.
If the Gateway CGI components are not included in the list of allowed applications then add them (as you would have done for IIS v6):
You can add text of your own choice in the **Description** field. For example:

```
CSPGatewayManagement for nph-CSPcgiSys.exe
CSPGatewayRunTime for nph-CSPcgi.exe
```

9. Repeat the above process: Use the **Add Script Map** dialogue to enter the following two mappings:
Request Path: *.cls
Executable: C:\inetpub\CSPGateway\nph-CSPcgi.exe
Name: CSPGateway_cls
Request Path: *.zen
Executable: C:\inetpub\CSPGateway\nph-CSPcgi.exe
Name: CSPGateway_zen
Request Path: *.cxw
Executable: C:\inetpub\CSPGateway\nph-CSPcgiSys.exe
Name: CSPGatewayManagement

### 4.1.14.3 Operating and Managing the Gateway

This connectivity option depends on the CSP Gateway's Network Service Daemon (NSD).

1. Start the CSP NSD as described in the section dedicated to this service.
To access the CSP Gateway's Systems Management suite, point your browser at one of the following locations:
http://<ip_address>/csp/bin/Systems/Module.cxw
http://<ip_address>/csp-bin/nph-CSPcgiSys
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension. For example:
http://<ip_address>/csp/samples/menu.csp
If you see an unauthorized user error message, refer to the section CSP Gateway and Security.

## 4.1.15 Restarting IIS

This section describes what happens when IIS is restarted via the various control panels:
Most configuration changes can be made in real-time to an active IIS installation. However, the **Internet Information Services (IIS) Manager** control panel provides stop, start, and restart options. These are useful for the refreshing the Web server configuration but does not result in an active Gateway installation being reinitialized (the Gateway DLLs is not reloaded).
As with previous versions of IIS, if you want to force IIS to restart, so that the Gateway modules are reloaded, then you have to restart the **World Wide Web Publishing** service via the main Windows **Services** control panel.

## 4.1.16 Troubleshooting

This section describes problems that commonly occur in configuring third-party modules (both Native and ISAPI) to work with IIS.
The most common problem likely to be encountered is that, after reconfiguring, requests to IIS fail with the following error:

```
Service Unavailable
HTTP Error 503. The service is unavailable.
```

This usually indicates that the default **Application Pool** has terminated.

1. Open the Internet Information Services (IIS) Manager window.
2. In the left panel expand the top level to reveal the Application Pools section.

**[MACHINE_NAME] ([machine_name]\[user_name])**
**Application Pools**

3. Check that the Default Application Pool (`DefaultAppPool`), or whatever application pool your server is configured to use, is marked with a Status of **Started**.
4. Restart the application pool if necessary (using the options in the right panel).
5. If problems persist, look for clues in the main **Windows Event Log**: the **Applications** section. In particular, check for the following error message:

```
Failed to find the RegisterModule entrypoint in the module DLL
C:\inetpub\CSPGateway\CSPms.dll. The data is the error.
```

This, for example, indicates that the version of Gateway DLLs that you are using do not implement the Native Modules interface. Either obtain later DLLs from InterSystems or configure the Gateway to work through the conventional ISAPI interface.
As with all software, restarting often clears transient problems: To completely restart IIS, restart the **World Wide Web Publishing** service via the main Windows Services control panel.
Do not use the `Add Wildcard Script Map` utility to map file extensions. If you do, you may see this error:

```
The specified module required by the handler is not in the modules list. If you
are adding a script map handler mapping, the IsapModule or the CgModule must in
the modules list.
```

Instead use `Add Module Mapping for *` to map file extensions using a wildcard.
If URLs with /bin in them are not working, see the section Manual Step for Enabling URLs with /bin

# Section 4.2: Microsoft Internet Information Services Version 6 (IIS v6) or Earlier

IIS is supplied with the server-oriented Windows Operating Systems (such as Windows NT Server/2000/2003). Windows XP Professional, though predominantly a client-oriented Operating System, also includes the IIS server. A Web server is not supplied with Windows XP Home edition.
This book assumes that the CSP Gateway components are installed in the following directory:
C:\Inetpub\CSPGateway
If your CSP Gateway Web server components are installed in a different directory, amend the directions in the following sections, as appropriate.

## 4.2.1 Installing with Microsoft Web Servers (All Connectivity Options)

If you have an IIS Web Server and you are choosing to install the CSP components manually, follow the instructions in this section. Then, according to the option that applies to your installation, follow the instructions in one of the following sections.
Install the CSP Gateway components and the CSP static files as follows:
1. NSD Module (if required)
• CSPnsd.exe
• CSPnsdSv.exe
The default location for these modules is
C:\Inetpub\CSPGateway\nsd
The NSD should be run from within this directory (its home directory). The configuration file (CSP.INI) and Event Log (CSP.LOG) are written in this directory for NSD-based connectivity options.
2. ISAPI and CGI Modules (if required). All of the modules listed below are not required for all connectivity options.
Refer to the sections describing each option to see which are actually required.
• CSPms.dll (Runtime module)
• CSPmsSys.dll (Systems Management module)
• CSPcms.dll (ISAPI client to the NSD – if supplied)
• CSPcgi.exe (Runtime module)
• nph-CSPcgi.exe (Copy of CSPcgi)
• CSPcgiSys.exe (Systems Management module)
• nph-CSPcgiSys.exe (Copy of CSPcgiSys)
• CSPmsf1.dll (ISAPI filter – if supplied)
The default location for these modules (that is, the default location for the Management Portal Gateway components for the specific instance of Caché) is:
*cache-install-dir*\csp\bin
To avoid disrupting existing Gateway installations on upgrading Caché, the installation procedures place these modules in the following common location. This location is not related to a particular Caché configuration.
C:\inetpub\CSPGateway
The configuration file (CSP.INI) and Event Log (CSP.LOG) are written in this directory for non-NSD-based connectivity options.
3. HyperEvents Components
• CSPBroker.js
• CSPBroker.class
• CSPBroker.jar
• cspbrokerBeanInfo.class
• CSPxmlhttp.js
The default location for these files is
*cache-install-dir*\csp\broker
4. Miscellaneous static resources used by the CSP Samples

A number of static Web resources (such as image files) are required by the CSP Samples. The default location for these files is *cache-install-dir*\csp\samples
5. Miscellaneous static resources used by the Caché Management Portal
A number of static Web resources (such as image files) are required by the Management Portal. The default location for these files is:
*cache-install-dir*\csp\sys

## 4.2.2 Option 1 (Recommended): IIS and ISAPI Modules (CSPms.dll)

If you are using the ISAPI modules with the IIS Web server, follow the directions in this section:
Configure the Web server so that it recognizes CSP requests (files of type .csp, .cls, and .zen) and passes them to the CSP Gateway for processing.

### 4.2.2.1 Internet Information Services with ISAPI

If you are running any version of IIS using the ISAPI modules, follow these directions:
1. Open the **Internet Services Manager**, which in most versions of Windows is in Administrative Tools.
2. Expand the **Web Sites** folder and navigate to **Default Web Site**.
3. Right-click **Default Web Site** and click **Properties**.
4. Click the **Home Directory** tab.
5. Click **Configuration**.
6. Click the **Mappings** tab.
7. Click **Add** to display the **Add/Edit Application Extension Mapping** dialog box and add the following record:
• Executable: \Inetpub\CSPGateway\CSPms.dll
• Extension: `csp`
• Verbs: Select **All Verbs**
• **Script engine** check box: Select
• **Check that file exists** check box: Clear
8. Repeat the above process to add the following record:
• Executable: \Inetpub\CSPGateway\CSPms.dll
• Extension: `cls`
• Verbs: Select **All Verbs**
• **Script engine** check box: Select
• **Check that file exists** check box: Clear
9. Repeat the above process to add the following record:
• Executable: \Inetpub\CSPGateway\CSPms.dll
• Extension: `zen`
• Verbs: Select **All Verbs**
• **Script engine** check box: Select
• **Check that file exists** check box: Clear
10. Repeat the above process to add the following record:
• Executable: \Inetpub\CSPGateway\CSPms.dll
• Extension: `cxw`
• Verbs: Select **All Verbs**
• **Script engine** check box: Select
• **Check that file exists** check box: Clear
11. Return to **Internet Information Services** and navigate to **Default Web Site** again.
12. Right-click **Default Web Site**, point to **New** and then click **Virtual Directory**. Create a virtual directory using the following information:
• Alias: `csp`
• Directory: *install-dir*\csp
• Access Permissions: Select the **Execute** check box
13. Click **Save** and restart IIS to apply your changes.

### 4.2.2.2 Internet Information Services Version 6 with ISAPI

If you are running IIS V6, follow the directions in the previous section and also the directions in this section:
This version of IIS is shipped with Windows Server 2003. To configure CSP to work with this server, register the CSP Gateway ISAPI DLLs (CSPms.dll and CSPmsSys.dll) as allowed Web service extensions.
**Important:** It is a common mistake to register the Gateway's modules, which are ISAPI extensions, as ISAPI filters.
If you register the modules as ISAPI filters, CSP does not work.
1. Open the **Internet Services Manager**.
2. Navigate to **Web Service Extensions**. This displays a list of currently configured extensions (or applications) in the right-hand panel.
3. Right-click **Web Services Extensions** and select **Add a new Web service extension**.
4. Enter `CSP Gateway` for the **Extension** name field.
5. Click **Add**.
6. Add CSPms.dll (including the full physical path to this DLL). Repeat the process for CSPmsSys.dll (Gateway builds 999 and earlier).
7. Select the **Set extension status to Allowed** check box.
8. Click **OK**.
Note that there is an option to allow users access to all ISAPI extensions: **Allow All unknown ISAPI extensions**. Enabling this option automatically enables access to the CSP Gateway's ISAPI modules. However, to maintain security it recommended that you follow the procedure above and grant additional access only to the CSP Gateway modules.
Later, you can perform the following additional operations on registered Web Service Extensions. IIS v6 lets you turn off aspects of access to CSP.

#### To Prohibit Access to CSP Web Gateway Management Page

Use this procedure to disable access to the CSP Web Gateway Management page available from the Management Portal.
Doing this prevents the possibility of unauthorized users gaining access the CSP Web Gateway Management page for an operational system. It is a quick and straightforward procedure for system administrators to re-enable access for a future period of time in order for configuration changes to be made to the Gateway.
1. Open the **Internet Services Manager** .
2. Navigate to **Web Service Extensions** to display a list of currently configured extensions (or applications) in the righthand panel.
3. In the right-hand window, double-click **CSP Gateway** to display the **Web Service Extension Properties** window.
4. Click the **Required Files** tab.
5. Click CSPmsSys.dll to select this file.
6. Click Prohibit; click **Apply**; click **OK**.
You can also use this procedure to prevent end-users from gaining access to CSP resources while significant changes are
being made to the Gateway configuration. In this case, the Gateway runtime module (CSPms.dll) should be marked as
`Prohibited` instead of the Systems Management module (CSPmsSys.dll).
To reactivate the CSP Gateway Systems Management module, at the last step, click **Allow** instead of **Prohibit**.

### 4.2.2.3 Security Settings with ISAPI

For many Windows installations (particularly Windows 2000 and later), the default privileges assigned to the IIS Web server are not sufficient to allow the CSP Gateway to read from and/or write to its configuration and log files (CSP.ini and CSP.log respectively).
You must, therefore, assign the Web server read/write privileges to the CSP Gateway files, or grant the Web server Administrator privileges. If you fail to do this, you may not be able to save your configuration changes through the CSP Web Gateway Management page.

File-access privileges can be modified through Windows Explorer. Alternatively, you can use the following two commands at the command prompt. Note that the CSP.ini and CSP.log files are in the the same directory as the Gateway binaries that the web server is configured to use. With ISAPI, this is typically Inetpub.

```
cacls c:\Inetpub\CSPGateway\CSP.ini /E /G IUSR_xxx:F
cacls c:\Inetpub\CSPGateway\CSP.log /E /G IUSR_xxx:F
```

Where `IUSR_xxx` is the Web server's user authority and the `xxx` component is usually the computer name (see the numbered procedure below to find the correct name).

The files that you are running the `cacls` command on must already exist. If they do not, use the `copy con` command (in a Windows Command Prompt window or DOS box) to create empty files:

```
Copy con c:\Inetpub\CSPGateway\CSP.ini
^Z
Copy con c:\Inetpub\CSPGateway\CSP.log
^Z
```

Each individual command line is terminated with carriage return. `^Z` refers to `Ctrl-Z`, which ends the `copy` command.

Example: Use the following commands to adjust the CSP Gateway configuration and log file access rights for a computer named BOSTON:

```
cacls c:\Inetpub\CSPGateway\CSP.ini /E /G IUSR_BOSTON:F
cacls c:\Inetpub\CSPGateway\CSP.log /E /G IUSR_BOSTON:F
```

You can find the specific name to use in the Internet Service Manager by navigating to the `Authentication methods` dialog as follows:

1. Open the **Internet Services Manager**.
2. Navigate to **Default Web Site**.
3. Right-click **Default Web Site** and select **Properties**
4. Click the **Directory Security** tab.
5. Click **Edit** under the **Anonymous access and authentication** control panel. This displays the **User Name in the Authentication methods** dialog box.

### 4.2.2.4 Registering Additional File Types with CSP

To configure additional file types to be processed by CSP, replicate the configuration created for the usual file extensions (that is,.csp,. .cls, .zen) for the new file extension(s).

If you need to serve other static files through the CSP Gateway or need to access the Management Portal through this web server, add mappings for file types .jpg, .gif, .png, and .js.

To map requests for all files to CSP for a given path, set up the following wildcard entry for that path:

Executable: c:\cache-install-dir\csp\bin\CSPms.dll
Extension: .* (dot asterisk)
All Verbs: Check
Script engine: Check
Check that file exists: UnCheck

If the above does not work for your operating system, do the following:

1. Open the **Internet Services Manager**.
2. Navigate to **Default Web Site**, right-click and select **Properties**.
3. Select the **Home Directory** tab and click **Configuration**.
4. Under **Mappings** tab, insert an asterisk.
5. For Executable, select CSPms.dll and uncheck the **Verify that file exists**.

### 4.2.2.5 Operating and Managing the Gateway with ISAPI

To access the CSP Web Gateway Management page, enter one of the following URLs in your browser:

```
http://localhost:<port_no>/csp/bin/Systems/Module.cxw
http://localhost:<port_no>/csp/bin/CSPmsSys.dll.
```

If you see an `Unauthorized User` error message, refer to the section on security considerations.

The CSP engine is automatically invoked for requested files with names that end in .csp or .cls. For example:

```
http://localhost:<port_no>/csp/samples/menu.csp
```

## 4.2.3 Option 2: IIS and ISAPI Module with NSD (CSPcms.dll)

If you are using the ISAPI modules with the NSD with the IIS Web server, follow the directions in this section.
In most cases, the all-inclusive ISAPI-based solution (Option 1) is the option of choice, and is the implementation that gives the best performance. The ISAPI/NSD hybrid, described here, is useful for cases where it is necessary, for operational reasons, to manage the Gateway independently of the hosting Web server; for example, if multiple instances of the Web server are to share the same Gateway installation. In Option 1, each instance of the core Web server process binds to its own instance of the Gateway.
Option 1 provides better performance than the CGI/NSD hybrid described in Option 3. The higher latency that results from the need to start new processes to serve each and every request is avoided in this implementation.

### 4.2.3.1 Internet Information Services with ISAPI and NSD

If you are running any version of IIS using the ISAPI modules with the NSD, follow these directions:
Follow the instructions for Option 1 with the exception that CSP files should be associated with CSPcms.dll instead of CSPms.dll (steps 7 and 8) and nph-CSPcgiSys.exe instead of CSPmsSys.dll (step 9).
• Executable: *install-dir*\csp\bin\CSPcms.dll
• Extension: `csp`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
• Executable: *install-dir*\csp\bin\CSPcms.dll
• Extension: `cls`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
• Executable: *install-dir*\csp\bin\CSPcms.dll
• Extension: `zen`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
• Executable: *install-dir*\csp\bin\nph-CSPcgiSys.exe
• Extension: `cxw`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
Refer to the following section for further information relating to version 6 of IIS (shipped with Windows 2003).

### 4.2.3.2 Internet Information Services Version 6 with ISAPI and NSD

If you are running IIS v6, using the ISAPI modules with the NSD, follow the directions in the previous section and also follow these directions:
Follow the instructions for Option 1 with the exception that the following executables should be registered as allowed for the CSP Gateway instead of CSPms.dll and CSPmsSys.dll.
• CSPcms.dll
• nph-CSPcgi.exe
• nph-CSPcgiSys.exe

#### To Prohibit Access to CSP

Mark the following executables as prohibited:
• CSPcms.dll
• nph-CSPcgi.exe

- nph-CSPcgiSys.exe

### To Prohibit Access to the CSP Gateway Systems Management Portal

Mark the following executables as prohibited:
• nph-CSPcgi.exe
• nph-CSPcgiSys.exe

### To Prohibit Access to the CSP Gateway Runtime Module

Mark the following executable as prohibited: CSPcms.dll

### 4.2.3.3 Operating and Managing the Gateway with ISAPI and NSD

This connectivity option depends on the CSP Gateway Network Service Daemon (NSD).
1. Start the CSP NSD as described in Operating the Network Service Daemon (NSD).
2. Restart Apache after making changes to its configuration file (httpd.conf).
The order in which you start Apache and the NSD is unimportant.
3. To access the CSP Gateway Systems Management Portal, point your browser at one of the following locations. Although CSP pages are served through the higher-performing module (mod_csp.so), the CSP Web Gateway Management Page is accessed through the CGI module dedicated to this purpose (nph-CSPcgiSys).
`http://localhost:<port_no>/csp/bin/Systems/Module.cxw`
`http://localhost:<port_no>/csp-bin/nph-CSPcgiSys`
If you see an `Unauthorized User` error message, refer to the section on security considerations.
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension. For example:
`http://localhost:<port_no>/csp/samples/menu.csp`

## 4.2.4 Option 3: IIS and CGI Modules with NSD (nph-CSPcgi.exe)

If you are using the CGI modules with the IIS Web server with the NSD, follow the directions in this section:
In most cases, the all-inclusive ISAPI-based solution (Option 1) is the option of choice, and is the implementation that gives the best performance. The CGI/NSD hybrid is useful for cases where it is necessary, for operational reasons, to manage the Gateway independently of the hosting Web server, for example, if multiple instances of the Web server are to share the same Gateway installation. In Option 1, each instance of the core Web server process binds to its own instance of the Gateway.
Another factor in choosing this approach might be that the in-house requirements of your Web master (or ISP) dictate that all Web server extensions are implemented using the CGI protocol.

### 4.2.4.1 Internet Information Services with CGI and NSD

If you are running any version of IIS using the CGI modules with the NSD, follow these directions:
Follow the instructions for Option 1 with the exception that CSP files should be associated with nph-CSPcgi.exe instead of CSPms.dll (steps 7 and 8) and nph-CSPcgiSys.exe instead of CSPmsSys.dll (step 9).
• Executable: *install-dir*\csp\bin\nph-CSPcgi.exe
• Extension: `csp`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
• Executable: *install-dir*\csp\bin\nph-CSPcgi.exe
• Extension: `cls`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
• Executable: *install-dir*\csp\bin\nph-CSPcgi.exe
• Extension: `zen`
• All Verbs: Select
• Script engine: Select

• Check that file exists: Clear
• Executable: *install-dir*\csp\bin\nph-CSPcgiSys.exe
• Extension: `cxw`
• All Verbs: Select
• Script engine: Select
• Check that file exists: Clear
Refer to the following section for further information relating to version 6 of IIS (shipped with Windows 2003).

### 4.2.4.2 Internet Information Services Version 6 with CGI and NSD

If you are running IIS V6, follow the directions in the previous section for all versions of IIS and also follow the directions in this section.
Follow the instructions for Option 1 IIS v6, except register the following executables as allowed for the CSP Gateway instead of CSPms.dll and CSPmsSys.dll:
• nph-CSPcgi.exe
• nph-CSPcgiSys.exe

#### To Prohibit Access to CSP

Mark the following executables as prohibited:
• nph-CSPcgi.exe
• nph-CSPcgiSys.exe

#### To Prohibit Access to the CSP Gateway Systems Management Module

Mark the following executable as prohibited: nph-CSPcgiSys.exe.

#### To Prohibit Access to the CSP Gateway Runtime Module

Mark the following executable as prohibited: nph-CSPcgi.exe.

### 4.2.4.3 Operating and Managing the Gateway with CGI

This connectivity option depends on the CSP Gateway's Network Service Daemon (NSD).
1. Start the CSP NSD as described in Operating the Network Service Daemon (NSD).
2. Restart Apache after making changes to its configuration (httpd.conf).
The order in which Apache and the NSD are started is unimportant.
3. To access the CSP Web Gateway Management page, point your browser at one of the following locations.
Although CSP pages are served through the higher-performing module (mod_csp.so), the CSP Web Gateway Management page is accessed through the CGI module dedicated to this purpose (nph-CSPcgiSys).
`http://localhost:<port_no>/csp/bin/Systems/Module.cxw`
`http://localhost:<port_no>/csp-bin/nph-CSPcgiSys`
If you see an `Unauthorized User` error message, refer to the section on security considerations.
The CSP engine is automatically invoked for requested files that contain a .csp, .cls, or .zen extension, such as
`http://localhost:<port_no>/csp/samples/menu.csp`

## 4.2.5 Using the ISAPI Filter (CSPmsf1.dll)

You can use this filter with all IIS connectivity options. It can be deployed to provide essential functionality in the following two areas.

### 4.2.5.1 Processing WebDAV Requests

The use of the filter is essential if CSP is used to implement WebDAV services.
Many Microsoft WebDAV clients include the `Translate: f` header in the HTTP request headers sent to the Web server with each and every request. IIS, on detecting this header directive, attempts to process the request directly without forwarding it on to any further ISAPI extensions (such as the CSP Gateway) which might otherwise have been called in the absence of this header. This behavior effectively prohibits CSP from processing WebDAV requests.
The `Translate: f` header is essentially a way of avoiding the overloading of the GET method in the WebDAV protocol.
HTTP GET usually means get (that is, run) the page; WebDAV clients expect this method to `get` the source to the page instead. IIS cannot possibly implement this latter functionality for CSP-based content because the physical content (or source code) is associated with the Caché server and not the Web server. Therefore, requests from a Microsoft WebDAV client working to a CSP-based WebDAV server through IIS fail with HTTP `Forbidden` or `File doesn't exist` errors.
The filter works around this problem by examining the incoming request stream and translating `Translate: f` header directives to `Translate: g`. IIS then passes the request on to the CSP Gateway, if appropriate.

### 4.2.5.2 Processing Multiline HTTP Request Headers

IIS does not correctly process header directives that are split over multiple lines. In fact the whole HTTP header block can become badly corrupted.
Recent tests demonstrated that in some cases the affected header block can become corrupted to the extent that it is not possible to always work around the problem in the Gateway code (that is, after the corruption had occurred). See the example below.
The filter corrects this problem by removing carriage-return-linefeeds (CRLs) from individual header directives before IIS has a chance to parse the header block.
Example of the problem: Consider the following request header block.

```
POST /csp/xds/XDSRequest.csp HTTP/1.1
Accept: text/html, text/plain, text/xml, image/gif, image/jpeg, */*
Content-Length: 1787
certAlias: unknowncert
SOAPAction: \"" Content-Type: multipart/related; type="text/xml";" \
boundary=--boundary
421.41176470588235291359.470588235294118--
User-Agent: HttpClient/1.4.2
Mozilla/4.0
Host: localhost
Connection: keep-alive
```

Notice that the content boundary (part of the content-type directive) has been completely misplaced. It has been found that the nature of this corruption is not consistent. The servicing of the request can completely fail depending on the nature of the damage caused and the misparsing that occurs as a result.

### 4.2.5.3 Installing the Filter

The filter operates on raw request data and must therefore be installed globally for the whole Web server:
1. Open the **Internet Services Manager**.
2. Navigate to **Web Sites**. Right-click this item and select **Properties**.
3. Click the **ISAPI Filters** tab.
4. Click **Add**.
5. Enter `CSP Gateway` for the **Filter** name.
6. Browse to CSPmsf1.dll for **Executable**.
7. Click **OK**.
8. Restart the **World Wide Web Publishing** service from the Windows **Services** control panel (not the Internet Information Services control panel). Alternatively, restart the computer.

## 4.2.6 IIS Application Protection Levels

To improve the resilience of the Web server environment, Microsoft introduced the concept of Application Protection Levels or Isolation Levels. The idea was to introduce varying degrees of separation between the Web server and Web applications implemented as ISAPI extensions. The goal was to reduce the impact that faulty ISAPI extensions could have on the hosting Web server. Examples of ISAPI extensions include the ASP engine, ASP.NET engine and, of course, the CSP Gateway modules.

To see the Application Protection settings for the CSP Gateway, perform the following:

1. Right-click the /csp and/or the /csp/bin virtual directories from the **Internet Services Manager**.
2. Click **Properties**.
3. Click the **Virtual Directory** tab.

This section contains the Application Protection level setting. IIS version 5 supports the following three Application Protection levels:

1. **Low (IIS Process)**: ISAPI extensions are run in-process in the core IIS executable: InetInfo.Exe. This setting offers the best performance, and is the default scenario under IIS version 4. The problem is that if the ISAPI extension crashes, IIS crashes as well and must be restarted. However, IIS version 5 has a reliable restart feature that automatically restarts a server when a fatal error occurs.
2. **Medium (Pooled)**: ISAPI extensions are run in an external process (dllhost.exe) with respect to the IIS core. This improves the reliability of the Web server because an ISAPI extension crash does not affect the hosting Web server. All ISAPI extensions operating at the Medium isolation level share the same external process, the net result being a Web site running with just two processes (the IIS core and the process hosting ISAPI extensions). IIS version 5 was the first version to supports this setting, which is also the default setting when a new virtual directory is created to host an IIS application.
3. **High (Isolated)**: Each ISAPI application is run in an external process with respect to the IIS core. Therefore if an individual ISAPI application crashes, neither IIS nor any other ISAPI applications is affected. Both IIS v4 and IIS v5 support this setting: under IIS4 the ISAPI extension hosting the application runs inside mts.exe, while under IIS5 it runs inside dllhost.exe. An individual application is defined in terms of its path under IIS (for example: /csp).

These Application Protection settings do not affect the operation of NSD-based Gateway configurations because the ISAPI module communicating with the NSD does not pool any persistent information or other resources (such as connections to Caché). All persistent resources are held in the NSD module. The ISAPI module communicating with the NSD is unaffected by changes in the way it is managed by IIS.

The non-NSD based Gateway configuration (CSPms.dll and CSPmsSys.dll) is more sensitive to changes in the way ISAPI extensions are managed in IIS because the pooling of persistent resources (such as connections to Caché) takes place in the extension itself. Low and Medium setting have no visible impact on the way the Gateway operates. However, with the High setting, the Gateway's systems management module (CSPmsSys.dll) loses the ability to communicate with the Run Time (CSPms.dll). This is because the two modules are viewed as separate applications and, as such, are isolated from one another – which, of course, is one of the key aims of this setting. The Gateway operates correctly at the High setting but with the following restrictions:

- IIS must be restarted for changes to the Gateway's configuration to take effect. This must be done by completely restarting the World Wide Web Publishing service from the main Windows Services control panel; not through the Internet Services Manager control panel.
- The Gateway's Systems Management form (System Status) cannot be used to monitor the connections used by CSP applications.
- Each CSP application (as defined by the Web path to the application) maintains its own pool of persistent connections to Caché.

It is envisaged that some of these restrictions will be completely or partially lifted in future versions of the CSP Gateway.

However, it should be remembered that the NSD-based configuration options are not subject to these restrictions because the core Gateway process is managed independently of IIS.

## 4.2.7 IIS Application Pools and Web Gardens

With IIS Version 6, Microsoft further improved the scalability and resilience of the overall Web server environment. IIS Version 6 delivers Web hosting services through an adjustable architecture that can be used to manage server resources with improved stability, efficiency, and performance. IIS separates applications into isolated pools of processes and automatically detects memory leaks, defective processes, and overutilized resources. When problems occur, IIS manages them by shutting down and redeploying faulty resources and connecting faulty processes to analytical tools.

IIS Version 6 can run in either of two mutually exclusive modes of operation:

• *Worker process isolation mode*. This is the default mode of IIS 6.0. It isolates key components of the World Wide Web Publishing Service (WWW service) from the effects of errant applications, and protects applications from each other by using the worker process architecture. Microsoft recommends that worker process isolation mode should be used unless there is a specific compatibility issue that makes the use of IIS 5 isolation mode necessary. Web sites that serve static content, simple ASP applications and CSP applications should be able to move to IIS 6.0 running in worker process isolation mode.

• *IIS 5.0 isolation mode*. With this mode, it is possible to run applications that are incompatible with worker process isolation mode because they were developed specifically for earlier versions of IIS. Applications that run correctly on IIS 5.0 should run correctly on IIS 6.0 in IIS 5.0 isolation mode. It is not necessary to use this mode for CSP applications.

Worker process isolation mode provides better default security for running Web applications than IIS 5.0 isolation mode.

By default, worker processes run with the Network Service identity. The Network Service account has lower access rights than the default account for IIS 5.0 isolation mode. Web applications that run in-process in IIS 5.0 application mode run as Local System. The Local System account can read, execute, and change most of the resources on the computer.

### 4.2.7.1 Application Pools

An application pool is a configuration that links one or more applications to a set of one or more worker processes. Because applications in an application pool are separated from other applications by worker process boundaries, an application in one application pool is not affected by problems caused by applications running in other application pools.

By creating new application pools and assigning Web sites and applications to them, it is possible to make the server more efficient and reliable. Applications working through pools are always available, even when a worker process serving a different application develops a fault.

Applications are defined by their path in IIS. For example: /csp

### 4.2.7.2 Web Gardens

For even greater reliability, it is possible to configure an application pool to be supported by multiple worker processes.

An application pool that uses more than one worker processes is called a Web garden. The worker processes in a Web garden share the requests that arrive for that particular application pool. If a worker process fails, another worker process can continue to process other requests.

It should be noted that Web gardens are different from Web farms. A Web garden is configured on a single server by specifying multiple worker processes for an application pool. Web farms use multiple servers for supporting a Web site.

Creating a Web garden for an application pool can enhance performance in the following situations:

• Robust processing of requests: When a worker process in an application pool is tied up (for example, when a script engine stops responding), other worker processes can accept and process requests for the application pool.

• Reduced contention for resources: When a Web garden reaches a steady state, each new TCP/IP connection is assigned, according to a round-robin scheme, to a worker process in the Web garden. This helps smooth out workloads and reduce contention for resources that are bound to a worker process.

### 4.2.7.3 Application Pools, Web Gardens, and CSP

Application Pool and Web Garden configurations do not affect the operation of NSD-based Gateway configurations because the ISAPI module communicating with the NSD does not pool any persistent information or other resources (such as connections to Caché). All persistent resources are held in the NSD module. The ISAPI module communicating with the NSD is unaffected by changes in the way it is managed by IIS.

The non-NSD based Gateway configuration (CSPms.dll and CSPmsSys.dll) is more sensitive to changes in the way ISAPI extensions are managed in IIS because the pooling of persistent resources (such as connections to Caché) takes place in the extension itself.

Application pools that are configured to use no more than one worker process have no visible impact on the way the Gateway operates within the context of a single Web application path (for example, /csp). However, for configurations where multiple worker processes are used (a Web Garden) the workload for the CSP Gateway is evenly distributed amongst all participating worker processes in the pool. Each worker process manages its own instance of the CSP Gateway modules.

This process management architecture does not pose a problem with respect to the way the Gateway operates but the following restrictions must be borne in mind:

• IIS must be restarted in order for changes to the Gateway's configuration to take effect. This must be done by completely restarting the World Wide Web Publishing service from the main Windows Services control panel; not through the Internet Services Manager control panel.

• The Gateway's Systems Management form (System Status) cannot be used to accurately monitor the connections used by CSP applications. At any given time the Systems Status reflects the status for the instance of the Gateway that happens to be attached to the current worker process (that is, the worker process that happens to service the Gateway's request).

• Each CSP application (as defined by the Web path to the application) maintains its own pool of persistent connections to Caché. Also, each worker process within an application pool maintains its own pool of persistent connections to Caché. This gearing should be remembered when configuring the maximum and minimum number of connections to Caché that the Gateway uses. These settings apply to each and every Gateway instance in the pool.

• State-aware sessions (preserve mode 1) cannot be used with Web Garden configurations because there is no control over the instance of the Gateway which is used to serve any particular request. The net result is that it's not possible to route state-aware requests to their dedicated Caché processes in these configurations.

It is envisaged that some of these restrictions will be completely or partially lifted in future versions of the CSP Gateway.

However, it should be remembered that the NSD-based options are not subject to these restrictions because the Gateway is managed independently of IIS.

Finally, the effect of certain worker process configuration parameters on the non-NSD version of the Gateway should be considered. In particular, the effect of the idle timeout and process recycling facility should be borne in mind.

### 4.2.7.4 Idle Timeout for Worker Processes

Often it is necessary to conserve system resources by terminating unused worker processes. It is possible to configure a worker process to gracefully close after a specified period of time. This feature can be used to better manage the resources when the processing load is heavy, when identified applications consistently fall into an idle state, or when new processing space is not available.

When a worker process is terminated, the instance of the Gateway that it manages also close and the pool of connections to Caché held by that Gateway instance is terminated. Of course, additional stateless connections can always be replaced in a way that is transparent to users of a CSP application but state-aware sessions (preserve mode 1) terminate when their hosting connection is closed.

### 4.2.7.5 Recycling Worker Processes

IIS can be configured to periodically restart worker processes, so that faulty Web applications can be recycled. This facility helps to ensure that application pools remain healthy and that any leaked system resources are recovered.

It is possible to configure worker processes to restart based on elapsed time, number of requests served, scheduled times and on the basis of memory usage.
The effect on the CSP Gateway of closing worker processes was discussed in the previous section (Idle Timeout). The same considerations apply here. Because CSP applications can only interact with the CSP Gateway through carefully managed channels, it is recommended that worker processes supporting the CSP applications should not be recycled.

***CSP Gateway Configuration Guide***
**Version 2011.1 30 June 2011**
**InterSystems Corporation**
**1 Memorial Drive**
**Cambridge MA 02142**
**www.intersystems.com**
**Caché Version 2011.1**
**30 June 2011 Copyright © 2011 InterSystems Corporation All rights reserved.**

# Appendix B: Instructions for Obtaining a Security Certificate

## Enabling SSL

**To create a certificate**

1. Ensure that Windows Server is installed on your computer.
2. Make sure that IIS is installed and enabled. For more information, see How to: Enable Internet Information Services (IIS).
3. Install Microsoft Certificate Services for your operating system, to allow creation of server authentication certificates.

   **Note:** You can also use the SelfSSL utility from the IIS resource kit to help create an SSL certificate and assign it to IIS. For more information, download the IIS 6.0 Resource Kit Tools.

4. Start Internet Explorer and browse to Microsoft Certificate Services, for example: http://MyCA/certsrv.
5. Click **Request a certificate**, then click **Next**.
6. Click **Advanced request**, then click **Next**.
7. Click **Submit a certificate request to this CA using a form**, then click **Next** to show the certificate request form.
8. Fill in the fully qualified domain name of the server machine, for example, sq101.adventureworks.com.
9. In the **Intended Purpose** (or **Type of Certificate Needed**) field, click **Server Authentication Certificate**.
10. For the cryptographic service provider (CSP), select **Microsoft RSA SChannel Cryptographic Provider**, **Microsoft Base Crypto Provider version 1.0**, or **Microsoft Enhanced Cryptographic Provider**. Do not select the **Microsoft Strong Cryptographic Provider**.
11. Select the **Use local machine store** box.
12. Ensure that **Enable strong private key protection** is not selected.
13. Click **Submit** to send the request.
14. If the certificate server automatically issues certificates, you can install the certificate now. Otherwise, you can install it after it has been issued by the CA administrator.

## Assigning an SSL Server Certificate to a Web Site

**To assign an SSL server certificate to a Web site**

1. In IIS Manager, expand the local computer, and then expand the Web Sites folder.
2. Right-click the Web site to which you want to assign the certificate and click **Properties**.
3. Select the **Directory Security** tab and under **Secure communications**, click **Server Certificate**.
4. In the **Web Server Certificate Wizard**, click **Assign an existing certificate**.
5. Follow the steps in the **Web Server Certificate Wizard**, which guides you through the process of installing a server certificate. After you have completed the wizard, you can view the information about the certificate by clicking the **View Certificate** button on the **Directory Security** tab of the Web sites **Properties** page.

# Installing a CA Certificate

**To install a CA certificate**

1. Start Internet Explorer and browse to Microsoft Certificate Services, for example: http://MyCA/certsrv.
2. Select **Check** on a pending certificate.
3. Click **Start**, and then click **Run**.
4. Type **mmc**, and then click **OK**.
5. On the **Console** menu, click **Add/Remove Snap-in**.
6. Click **Add**.
7. Click **Certificates** and then click **Add**.
8. Click **Computer account** and then click **Next**.
9. Ensure that Local computer:(the server computer) is selected and click **Finish**.
10. Click **Close**.
11. In the left pane tree view, expand **Certificates (Local Computer)**, expand **Personal**, and then select **Certificates**.
12. Verify that there is exactly one certificate with the fully qualified domain name that you specified. You can double-click to view details.