



RESOURCE AND PATIENT MANAGEMENT SYSTEM

IHS USER SECURITY AUDIT

(BUSIA)

Installation Guide and Release Notes

Version 1.0
September 2014

Office of Information Technology
Division of Information Technology
Albuquerque, New Mexico

Table of Contents

1.0	Release Notes	1
2.0	Installation Notes	2
2.1	Contents of Distribution	2
2.2	Required Resources	2
2.3	Before You Begin: Installation Issues	3
2.3.1	BMW v1.0 Patch 2 Installation Verification	3
2.3.2	BUSA Reporting Tool – Authorized Users	3
2.3.3	BUSA Package – Central Processing Unit (CPU) Capacity	3
2.3.4	BUSA Package – Disk Usage.....	3
3.0	Installation Instructions	4
3.1	Pre-KIDS Installation Setup Configuration	4
3.1.1	Prerequisites.....	4
3.1.2	Create a Database	4
3.1.3	Map the BUSA Globals to the New Database	12
3.2	KIDS Installation Instructions	20
3.2.1	Pre-Installation.....	21
3.2.2	BUSA Installation.....	21
4.0	Sample Installations	23
4.1	Sample Cache Install.....	23
5.0	Configuring the IHS USER SECURITY AUDIT Web Application	27
5.1	Enable System Authentication Options.....	27
5.2	Create New Web Application	28
5.3	Update Ensemble’s UnknownUser	31
6.0	Cache Server Page (CSP) Web Gateway Installation	35
6.1	Install Cache Shell.....	35
6.2	Configure IIS.....	42
6.3	Configure CSP Web Gateway	45
	Acronym List	53
	Contact Information	54

Preface

The purpose of this manual is to provide the user with the information required to install the IHS USER SECURITY AUDIT (BUSA) package.

1.0 Release Notes

The new BUSA package is a utility which enables user activity to be tracked. As a requirement for Meaningful Use (MU) stage two certification, all activity relating to patient data querying, adding, editing, copying, deleting, and printing must be logged.

The BUSA package also contains a web-enabled reporting interface which permits this logged data to be filtered, sorted and displayed.

2.0 Installation Notes

Prefix: BUSA

Current Version: 1.0

Note: Read entire notes file prior to attempting any installation

- All patches to Version 1.0 will be cumulative
- Make a copy of this distribution for offline storage.
- Print all notes and readme files.
- It is recommended that terminal output during the Kernel Installation and Distribution System (KIDS) installation be captured using an auxport printer attached to the terminal at which the user is performing the software installation or using a screen capture. This capture combined with the KIDS entry in the INSTALL file will ensure a printed audit trail should any problems arise.

2.1 Contents of Distribution

File	Description
busa0100.k	KIDS file
busa010i.pdf	Installation Guide and Release notes
busa010u.pdf	User Manual
busa010t.pdf	Technical Manual

2.2 Required Resources

Module/Software	Minimum Version
InterSystems Ensemble	v2012.2.0 or later
VA FileMan (DI)	v22.0 Patch 1003 or later
VA Kernel (XU)	v8.0 Patch 1015 or later
BMW.dat	v1.0 Patch 2 or later

2.3 Before You Begin: Installation Issues

2.3.1 BMW v1.0 Patch 2 Installation Verification

As noted in Section 2.2, to install the new BUSA application, the BMW v1.0 Patch 2 must be installed. As part of the BMW installation process, the BMW global must be properly mapped in the RPMS environment or the installation of the BUSA application will not be permitted to continue. For directions on how to map the BMW global, please see Appendix C of the *Practice Management Application Suite Version 1.0 Patch 2 Installation Guide and Release Notes*.

2.3.2 BUSA Reporting Tool – Authorized Users

During the installation process, the installer will be prompted to enter a list of users who are approved to use the reporting tool included with this package. This list of approved users should therefore be developed prior to installing this package. Also, since this reporting tool shows patient related activity, care should be taken to only provide access to the appropriate users.

2.3.3 BUSA Package – Central Processing Unit (CPU) Capacity

The BUSA Application Programming Interface (API) calls should not have a noticeable impact on the CPU capacity.

2.3.4 BUSA Package – Disk Usage

Since the BUSA application will log all user patient related activity, it will be a very large consumer of disk space. A detailed plan should therefore be developed to account for this need. See the installation configuration section for more information on mapping the BUSA storage globals in their own Cache '.dat' file(s).

3.0 Installation Instructions

3.1 Pre-KIDS Installation Setup Configuration

As noted in Section 2.3.4, the BUSAD and BUSAS globals should be placed in their own CACHE.DAT database file due to storage considerations. The following instructions show how to create a database and map these globals to that database. These instructions show the procedures for Ensemble 2012. Previous versions use the same procedures, but the screen displays will be different.

NOTE: These instructions should be performed before installing the initial BUSA patch. If this was not done then please check with support for instructions on how to copy this data to the new database after it has been setup.

3.1.1 Prerequisites

Before creating the database, locate a directory path on your server where there is sufficient storage available for the new database. Make sure that this directory path is included in your site's backup procedures so that this database backed up on a regular basis. For the examples below, we will use I:\E2012\BUSAGOLD4 as the directory path name.

Also, select a name for the new database, preferably one that includes "BUSA" and the RPMS namespace/database name that it is associated with. For the examples below, the original RPMS namespace and database name is GOLD4, so the database name to be used is BUSAGOLD4.

3.1.2 Create a Database

1. Navigate to the Ensemble Management Portal by selecting it from your list of Favorites in Internet Explorer, from a saved desktop icon, or by right-clicking the Ensemble Cube in your Windows System Tray and selecting **Management Portal**.

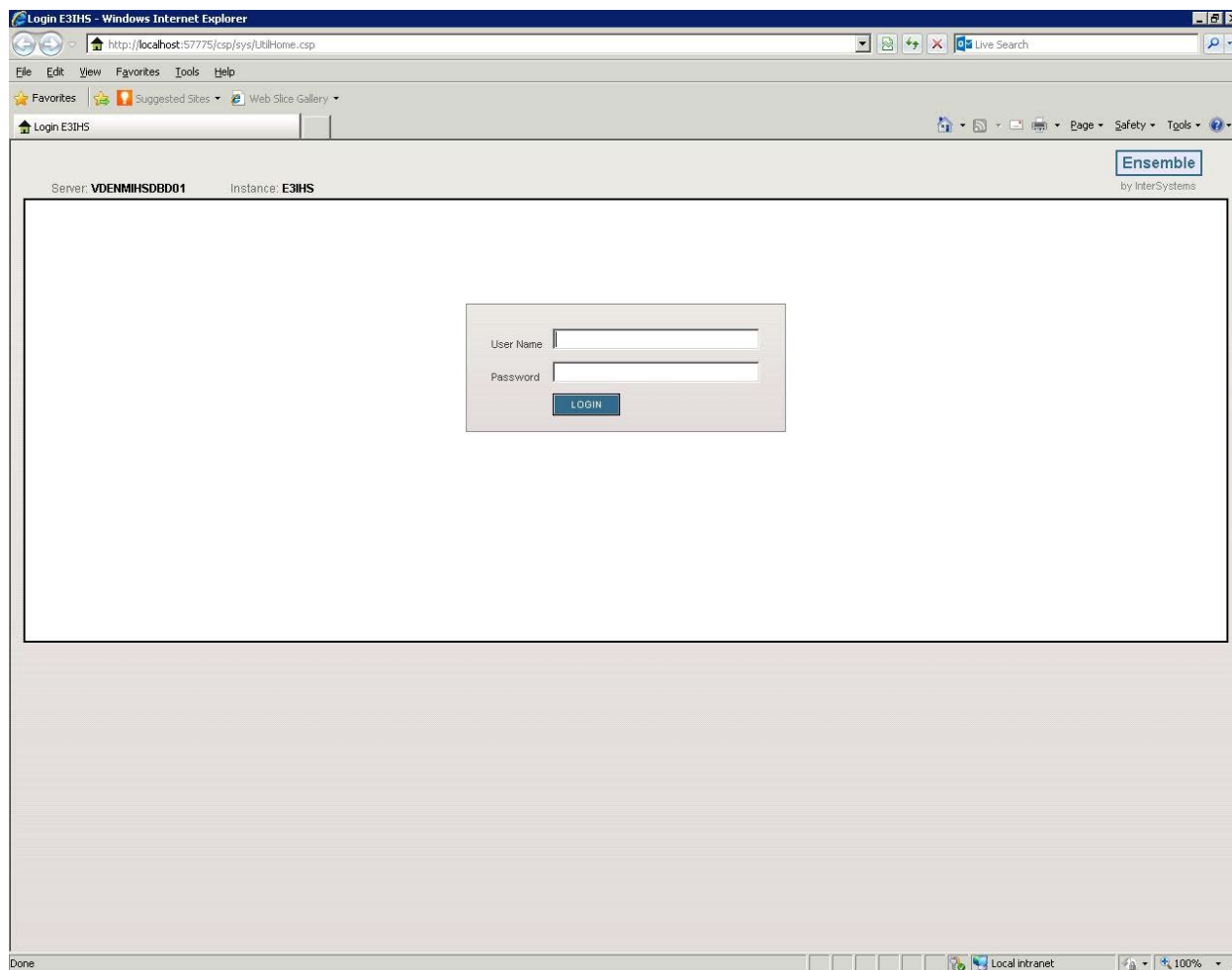


Figure 3-1: Navigate to the System Portal Page

2. Enter your username and password and click **LOGIN**.

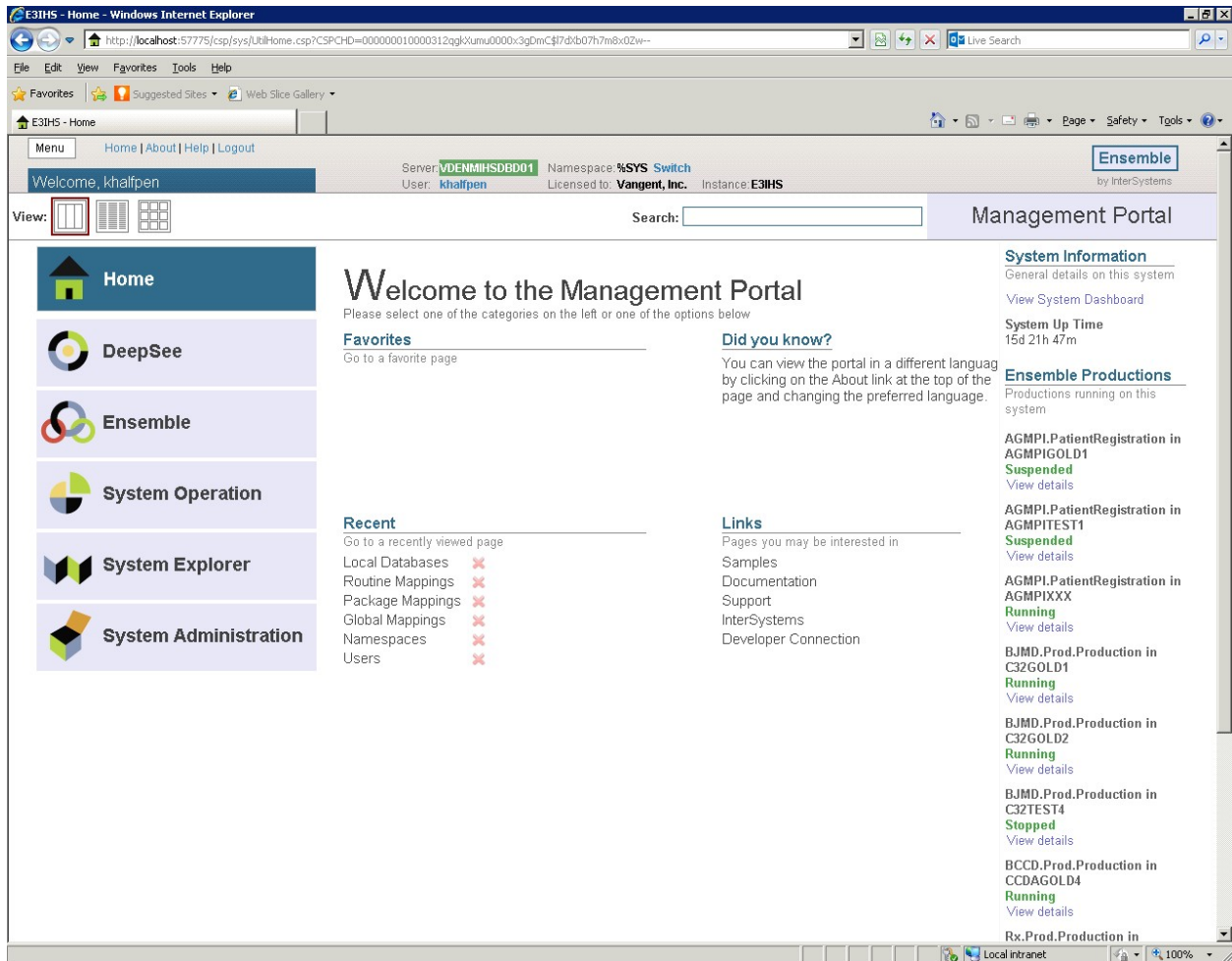


Figure 3-2: Main Management Portal Page

3. Click **System Administration** then **Configuration** and then **System Configuration**.

The screenshot displays the E3IHS Management Portal interface. The browser window title is "E3IHS - Home - Windows Internet Explorer". The address bar shows a local URL. The page header includes "Welcome, khalipen" and user information: "Server: VDENMIHSDEB01, User: khalipen, Namespace: %SYS Switch, Licensed to: Vangent, Inc., Instance: E3IHS".

The main content area is organized into three columns:

- Configuration »**: Security », Licensing », Encryption »
- System Configuration »**: Connectivity », Mirror Settings », Database Backup », CSP Gateway Management, SQL and Object Settings », Device Settings », National Language Settings », Zen Reports », Additional Settings »
- Local Databases**: Memory and Startup, Namespaces, Local Databases, Remote Databases, Journal Settings

The **Local Databases** section lists several production jobs:

Production Name	Status
AGMPI.PatientRegistration in AGMPIGOLD1	Suspended
AGMPI.PatientRegistration in AGMPITEST1	Suspended
AGMPI.PatientRegistration in AGMPIXXX	Running
BJMD.Prod.Production in C32GOLD1	Running
BJMD.Prod.Production in C32GOLD2	Running
BJMD.Prod.Production in C32TEST4	Stopped
BCCD.Prod.Production in CCDAGOLD4	Running
Rx.Prod.Production in	Running

Figure 3-3: Navigate to **Configuration, System Configuration, Local Databases**

4. Click **Local Databases** (You may also need to click a **GO** button, if prompted.)

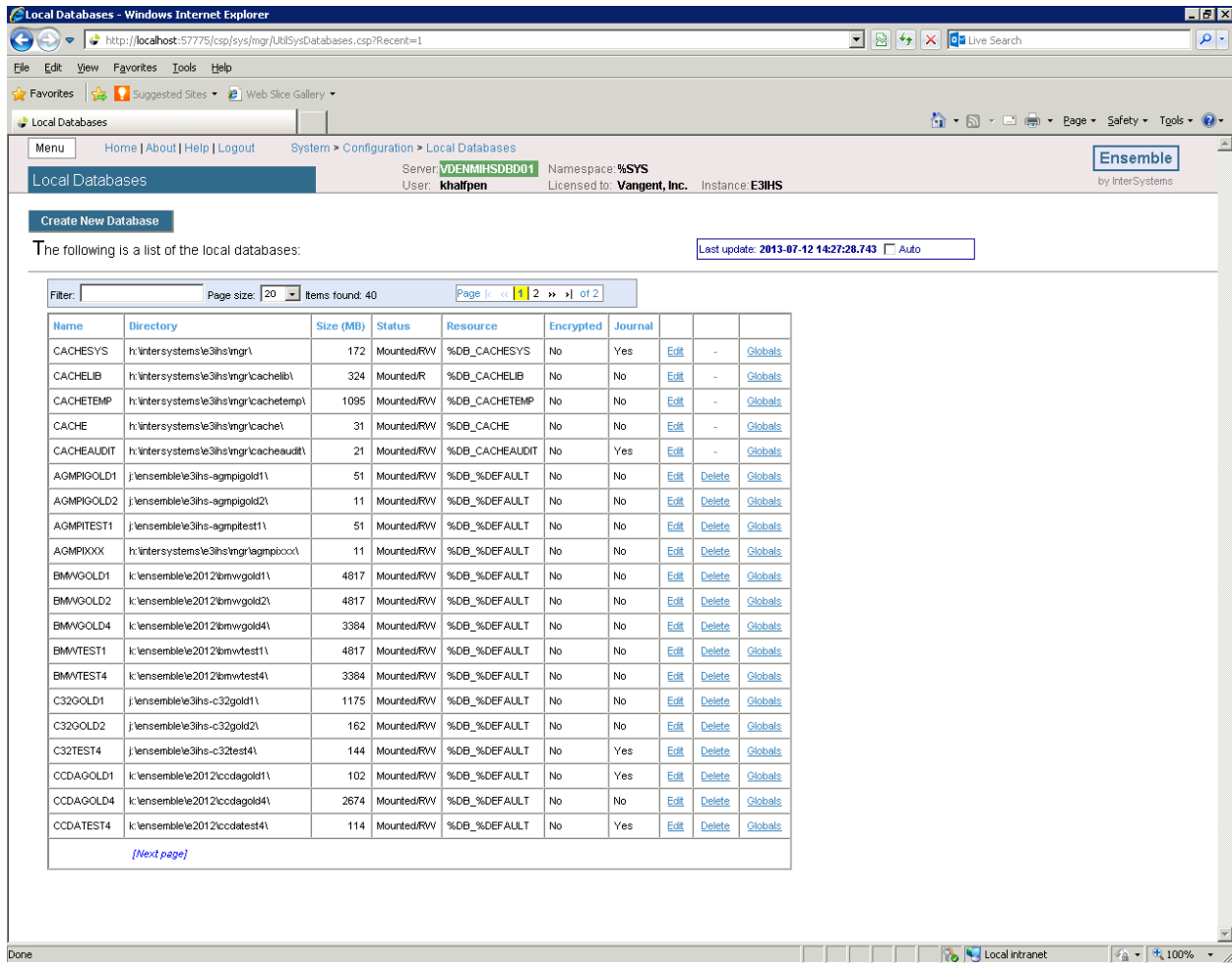


Figure 3-4: Sample Local Database Definitions Page

5. Click Create New Database.

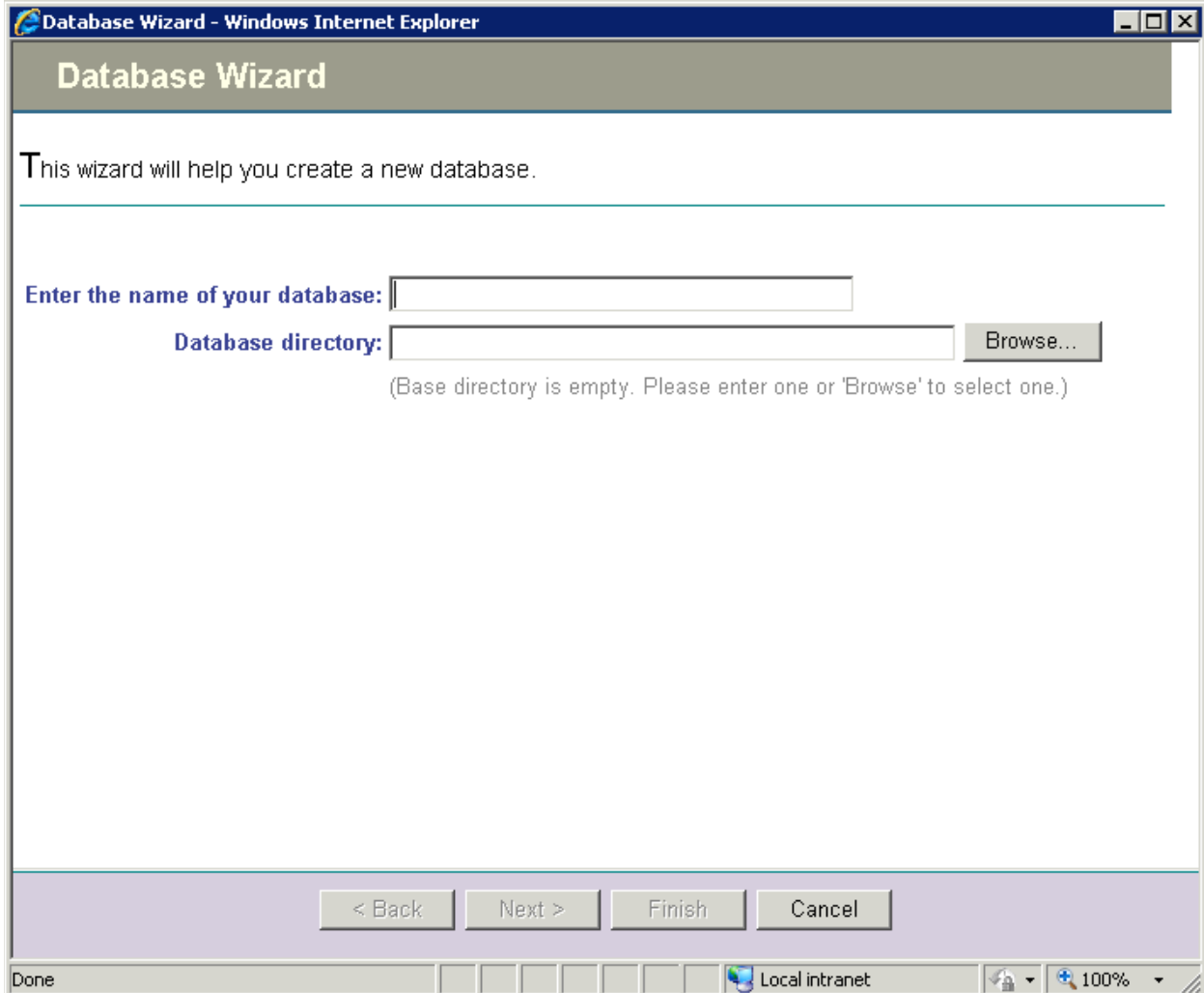


Figure 3-5: New **Database Wizard**

6. Enter the name of your database and either directly enter or browse for the directory (both items were described in the previous section).

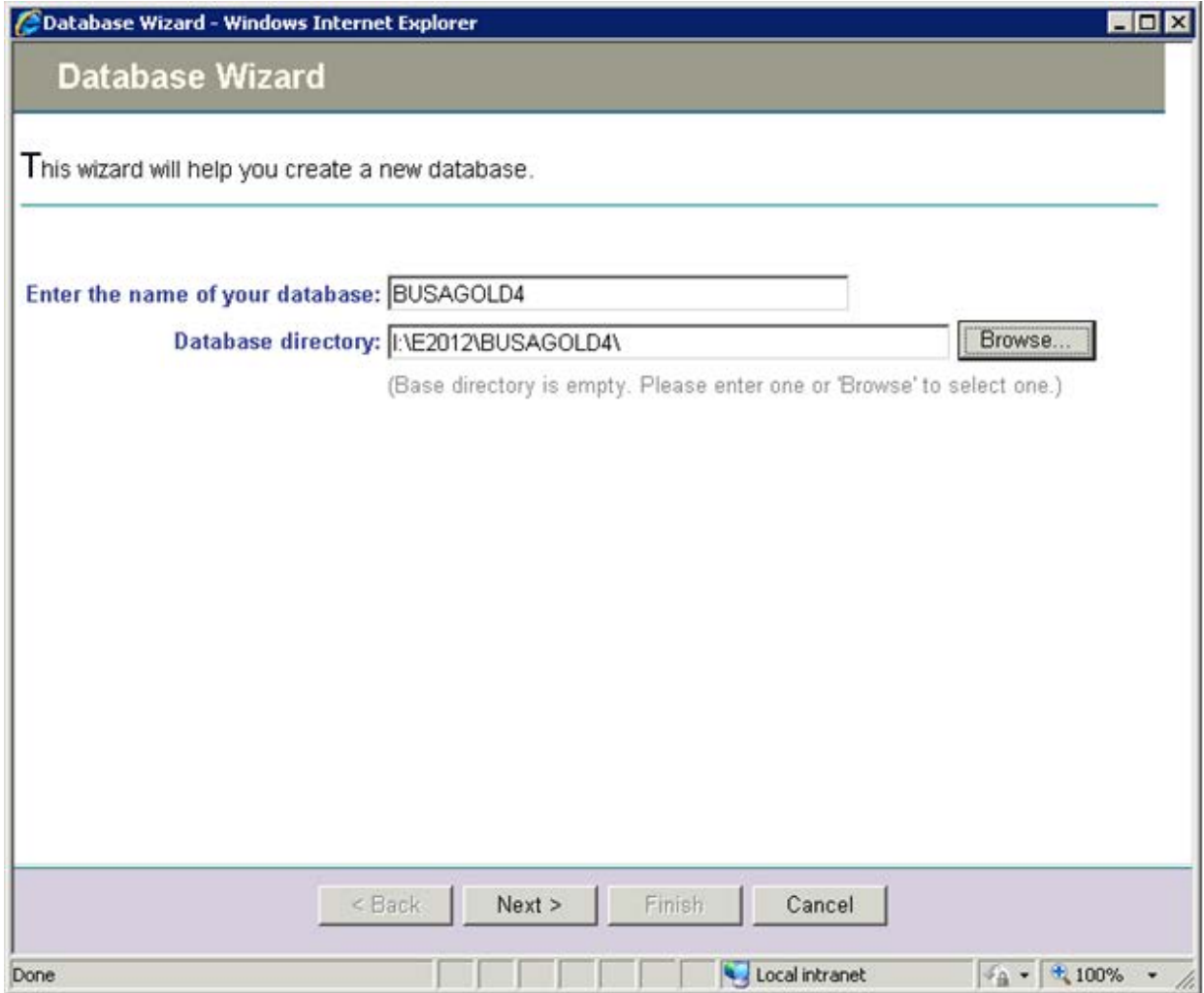


Figure 3-6: Sample New Database Settings

7. Click **Next**.

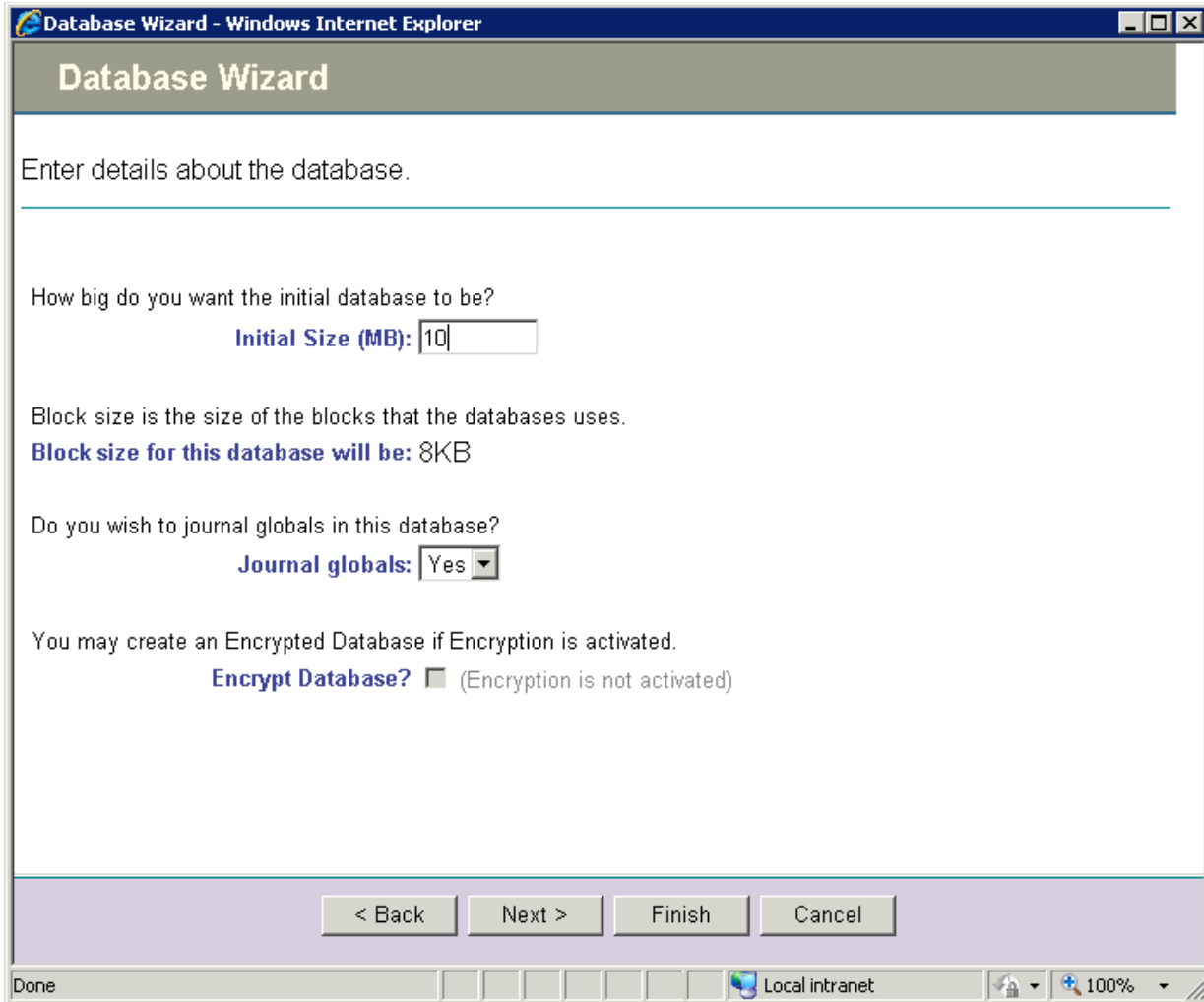


Figure 3-7: Additional Database Settings

8. Set the Initial Size to at least 10 (as shown). Larger sites with significant numbers of patients and visits may want to start with 100 or more.
9. Click **Finish**. The new database should be visible in the list.

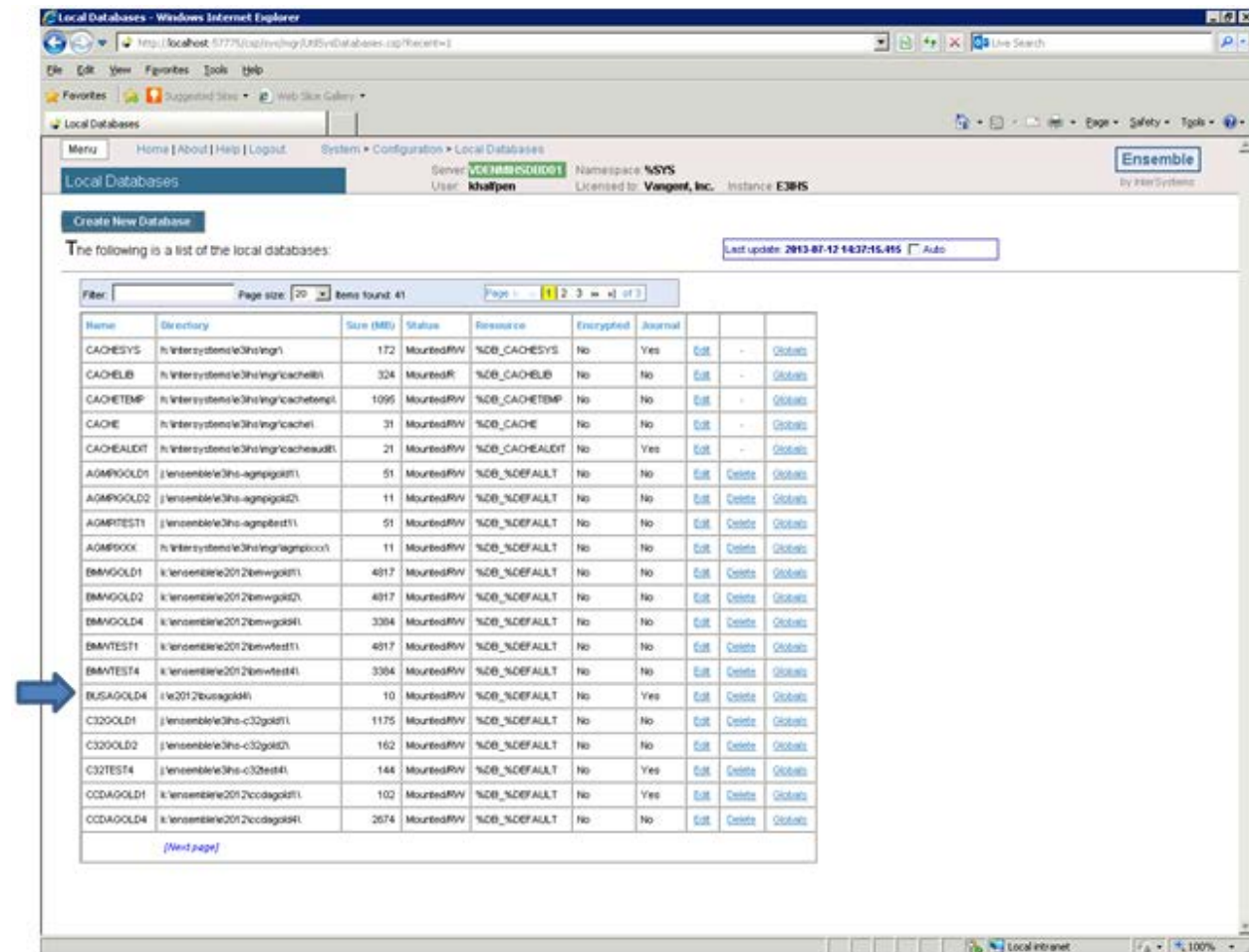


Figure 3-8: Database Listing Showing New Database

10. This completes the steps for creating a database.

3.1.3 Map the BUSA Globals to the New Database

1. Continuing from the previous section, click **Home** to return to the Home Page.

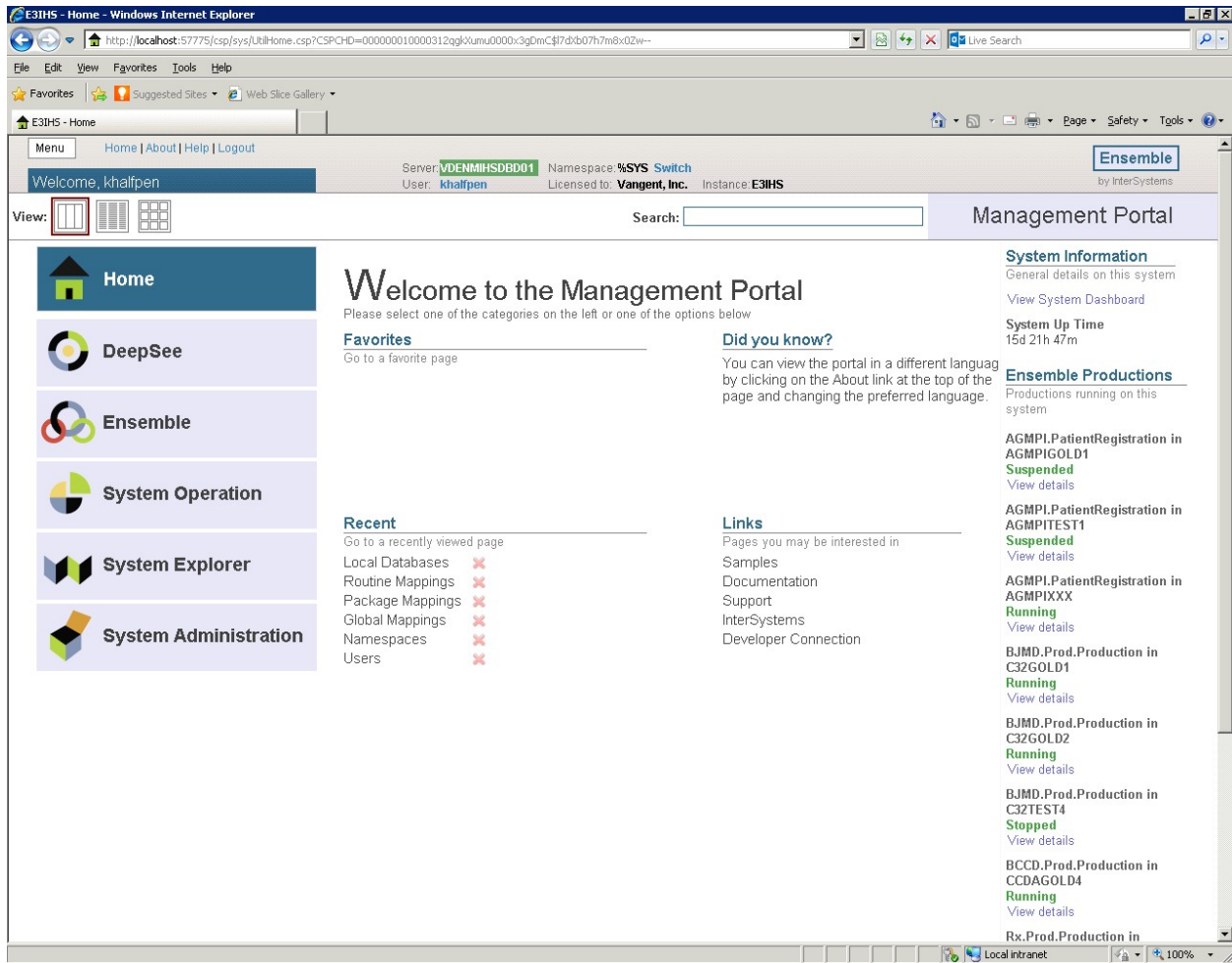


Figure 3-9: View of the Management Portal Main Page

2. Click **System Administration** then **Configuration** and then **System Configuration**.

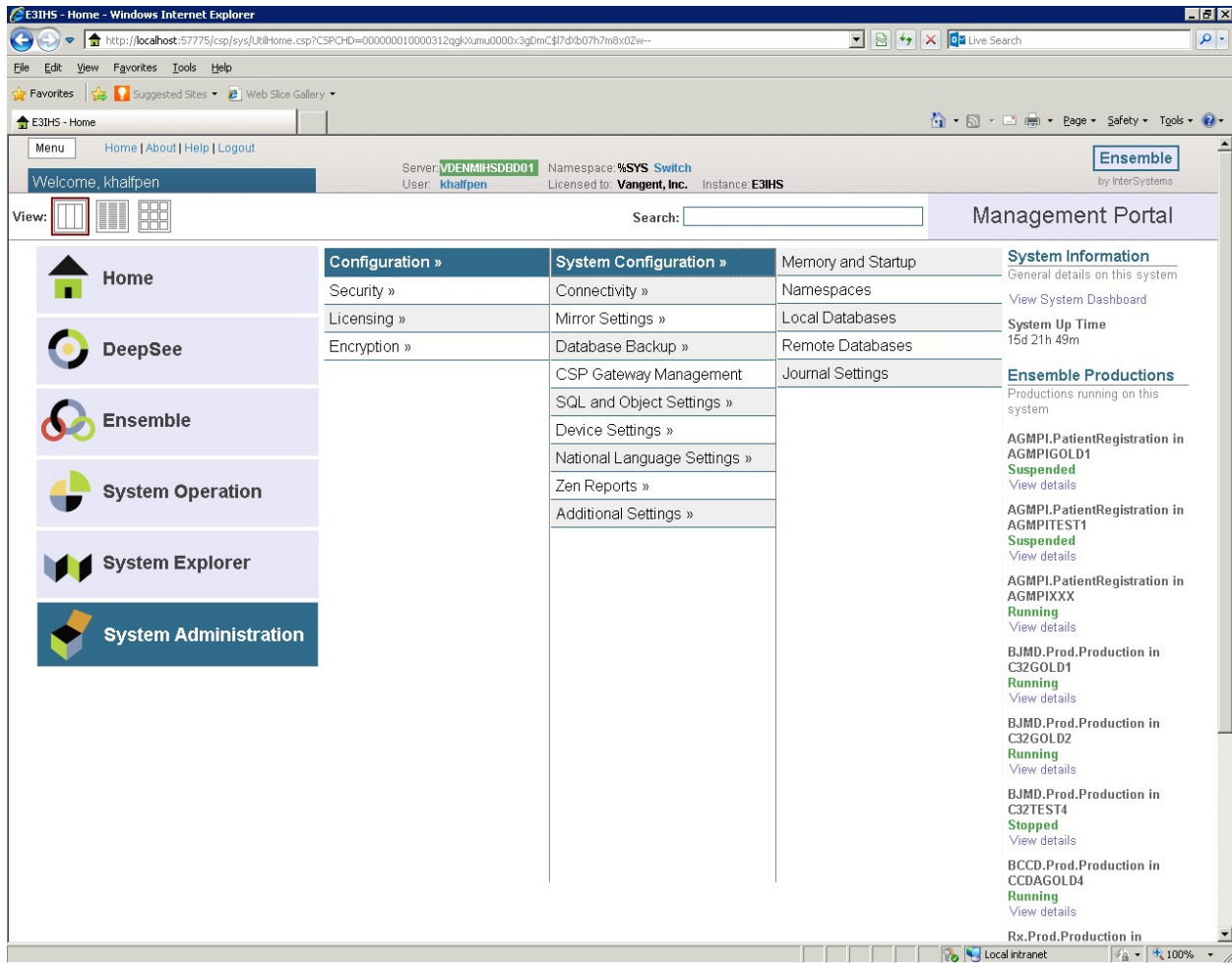


Figure 3-10: Selecting **Configuration, System Configuration, Namespaces**

3. Click **Namespaces** (You may also need to click a **GO** button, if prompted.)

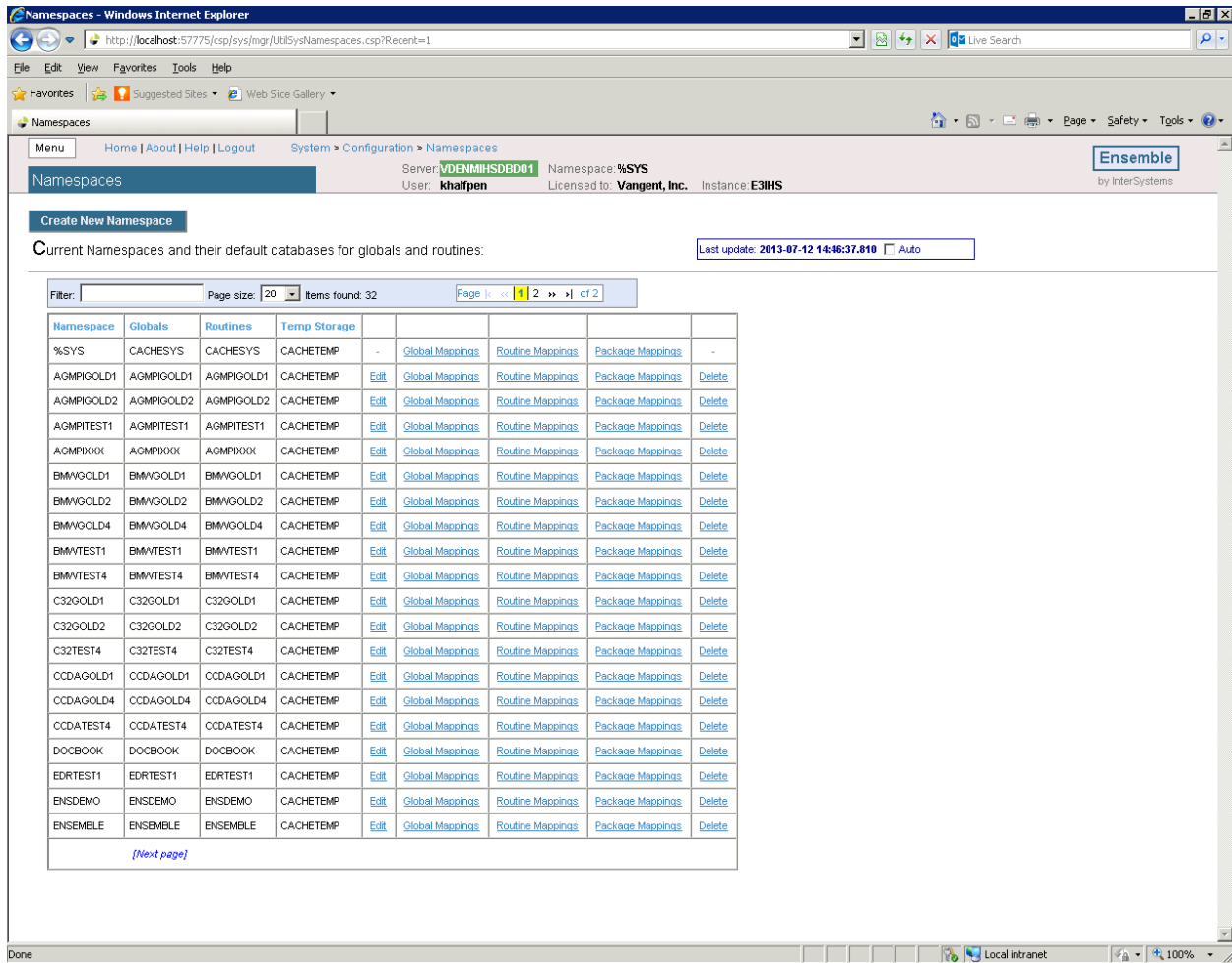


Figure 3-11: Sample Display of Defined Namespaces

4. Locate your main RPMS namespace. (You may have to click **Next Page** at the bottom to see additional pages of namespaces.) When you have located it, click **Global Mappings** on that line.

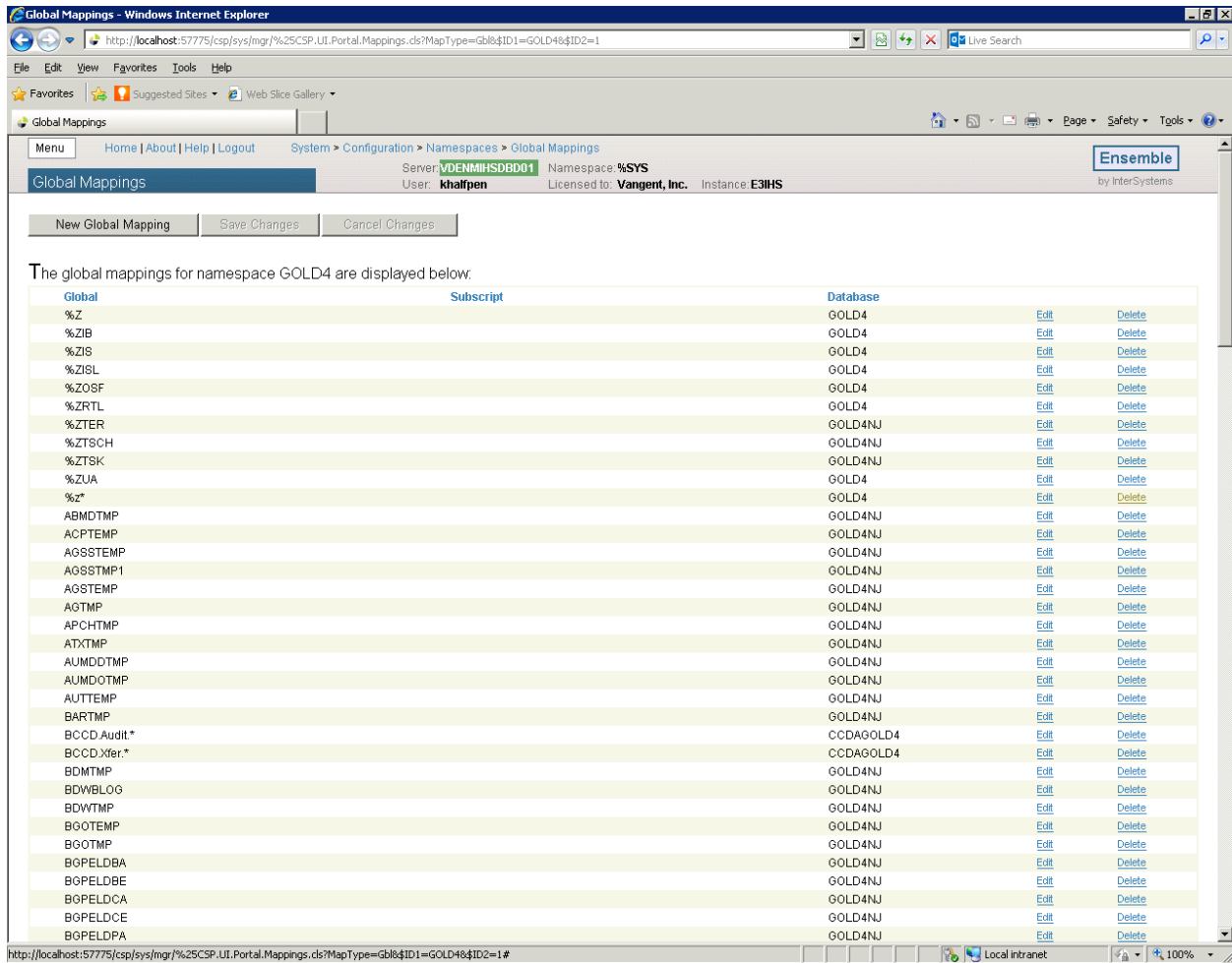


Figure 3-12: Sample **Global Mappings** page

5. Scroll down and make sure that there are no items currently listed in the Global column that begin with BUSA. If there are, then please check with support before proceeding.
6. Click **New Global Mapping**.

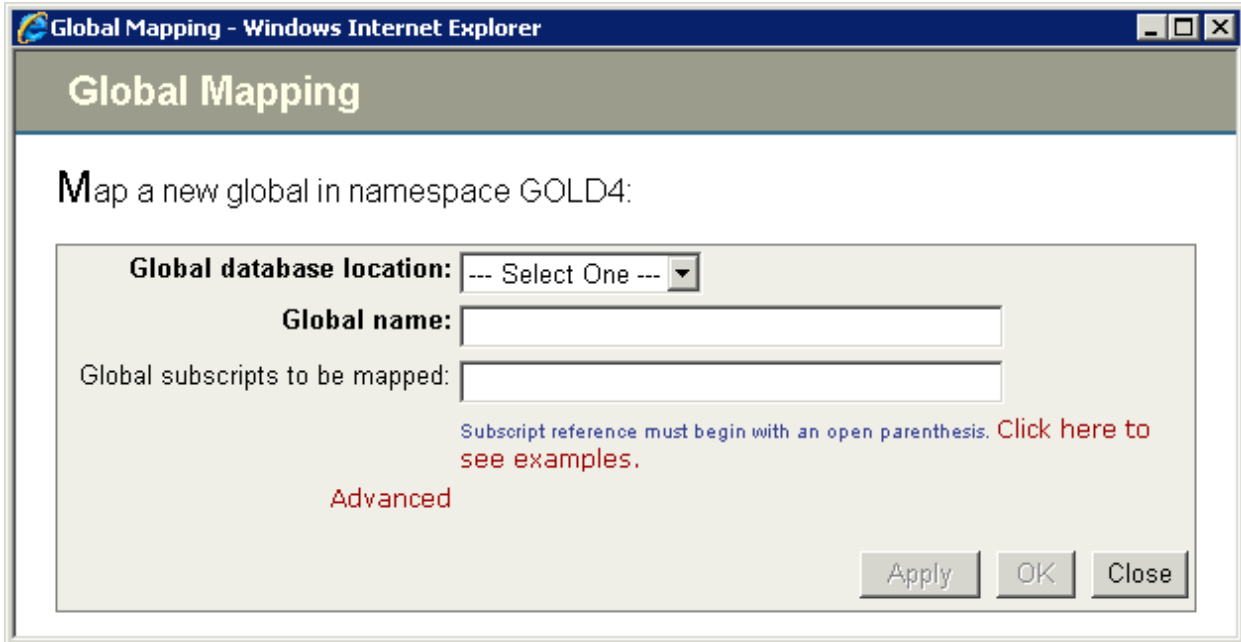


Figure 3-13: Global Mapping Wizard

7. In the **Global database location** drop-down box, select the database created in the previous section.
8. In the **Global name** box, type **BUSAD**.

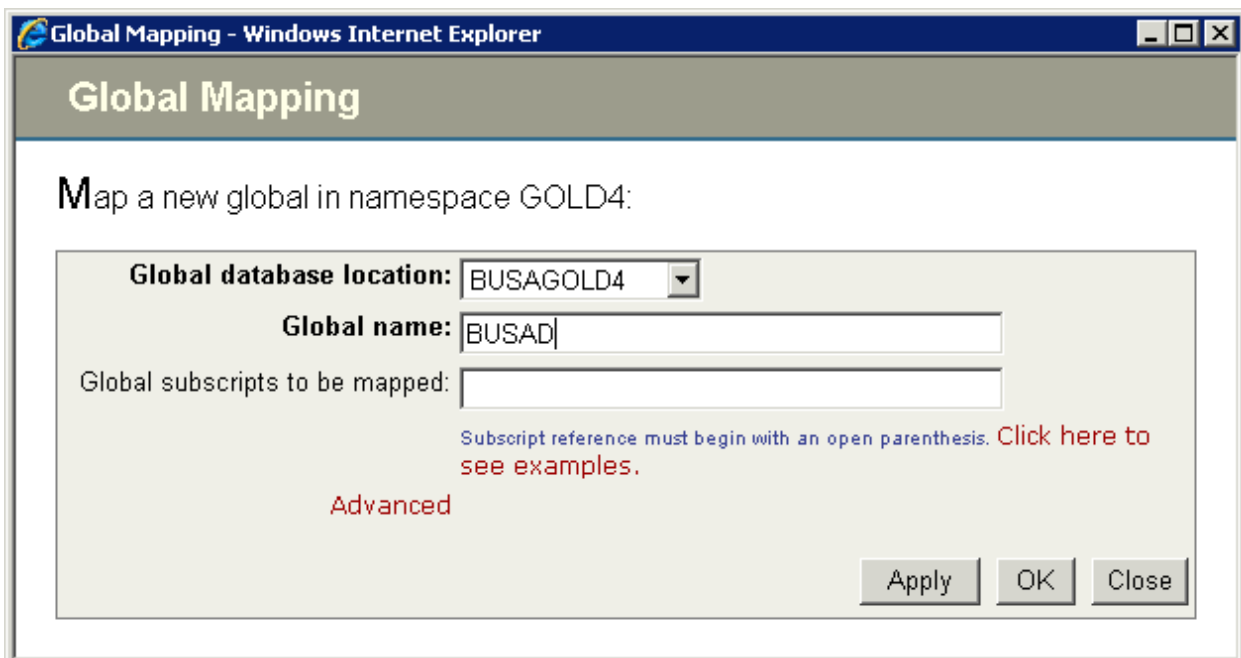
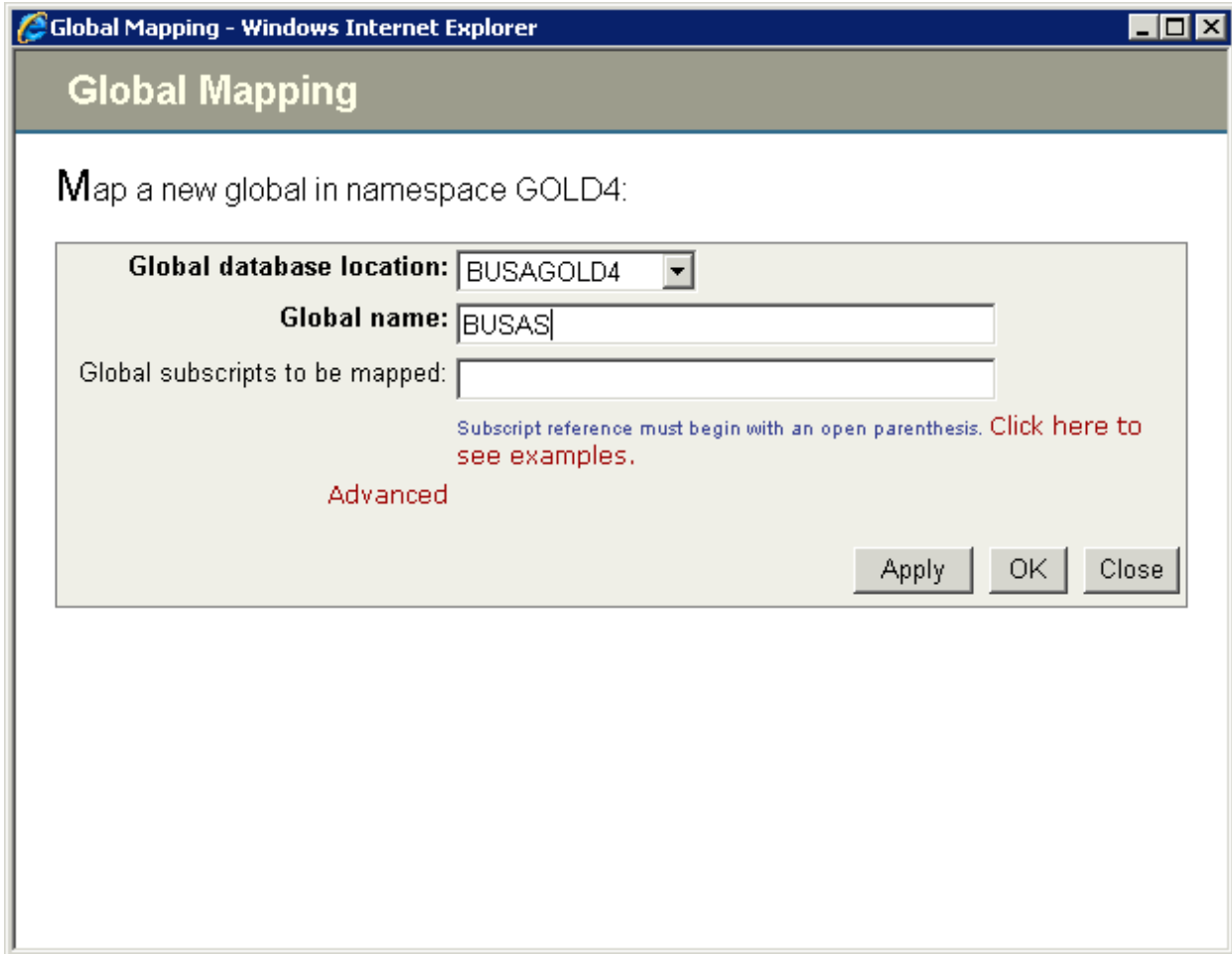


Figure 3-14: Sample Global Mappings Settings

9. Click **Apply**. (Note that the changes have not yet been saved.)

10. Change the Global name to **BUSAS**.



Global Mapping - Windows Internet Explorer

Global Mapping

Map a new global in namespace GOLD4:

Global database location: BUSAGOLD4

Global name: BUSAS

Global subscripts to be mapped:

Subscript reference must begin with an open parenthesis. [Click here to see examples.](#)

[Advanced](#)

Apply OK Close

Figure 3-15: Sample Global Mappings Settings - changing the Global name

11. Click **OK**. (Note that the changes have not yet been saved.)

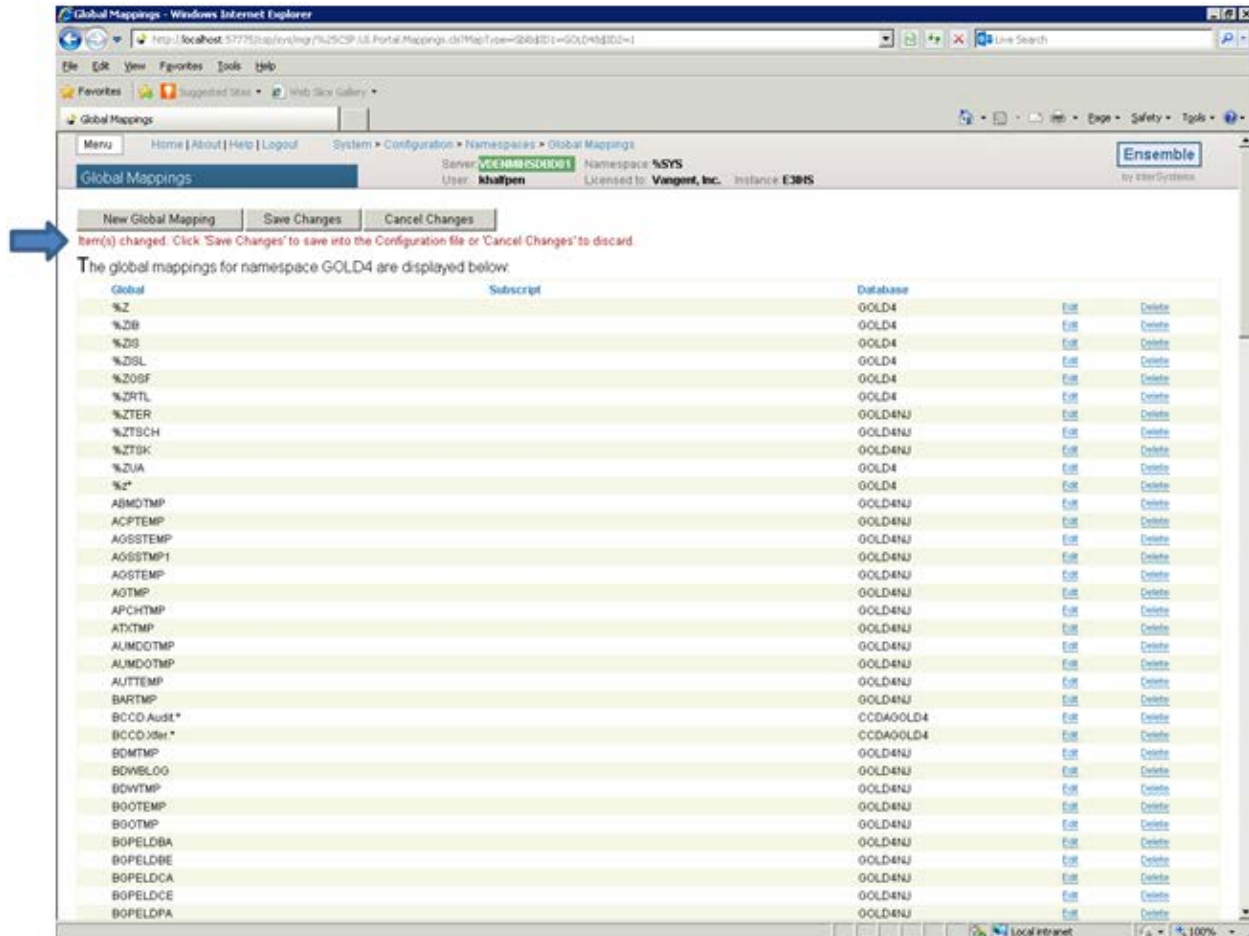


Figure 3-16: **Global Mappings** Display - Save Changes Step

- Click **Save Changes**. The new mappings should be visible in the list. (You may need to scroll down to locate them. See Figure 3-17 for display of new mappings.)

3.2.1 Pre-Installation

- If possible, initially load the software into a test account, then into the production account. There are no routines or globals to remove after the installation is complete.
- Refer to the BUSA Installation steps (Section 3.2) and its corresponding Sample BUSA Installation (Section 4.0) for the applicable prompts and user responses. User responses appear in bold type.

3.2.2 BUSA Installation

1. From the **KIDS** menu, select the **Installation** menu.
2. From the **XPD Main -> Installation** menu, select **Option 1: Load a Distribution**.
3. Type **busa0100.k** at the “Enter a Host File” prompt. Please note the file path might need to precede the file name with the appropriate host path. This is the file to retrieve from the appropriate software directory.
4. Type **Yes** (or press ENTER to accept the default) at the “Want to Continue with Load? YES//” prompt.
5. KIDS file busa0100.k contains the following installation file:
IHS USER SECURITY AUDIT 1.0
6. From the **Installation** menu, select **Option 2: Verify Checksums in Transport Global**. This option provides a mechanism for ensuring the integrity of your routines. This step verifies checksums for the components of the Transport global, and reports any errors uncovered.
7. Type **IHS USER SECURITY AUDIT 1.0** as the install name.

Optional: At this time, you can elect to exercise one of the following installation options. If you elect to use one of these, use IHS USER SECURITY AUDIT 1.0 as the install name.

- a. Back Up a Transport Global – this option creates a MailMan message that will back up all current routines on the system that would be replaced by this release. (Because this is a new release no files will be replaced.).
 - b. Compare Transport Global – this option allows you to view all changes that will result from the installation of this patch and compares them with the values currently loaded on the system (routines, data dictionaries, templates, etc.).
8. From the **Installation** menu, select the **Install Packages(s)** option.
 9. At the “Select Install Name prompt”, type **IHS USER SECURITY AUDIT 1.0**.

10. Respond to the following prompts as indicated:
 - a. At the “Want KIDS to Rebuild Menu Trees Upon Completion of Install? YES//” prompt, type **NO**.
 - b. At the “Want KIDS to INHIBIT LOGONs during the install?//YES” prompt, type **NO**.
 - c. At the “Want to DISABLE Scheduled Options, Menu Options and Protocols?// YES” prompt, type **NO**.
11. Type the device that will print the install messages.
12. At the “Enter the user to add/delete BUSA Reporting Access for User:” prompt, enter the list of approved users of the BUSA reporting tool.
13. Exit the **Installation** menu.

4.0 Sample Installations

4.1 Sample Cache Install

```

Select OPTION NAME: XPD MAIN Kernel Installation & Distribution System

Edits and Distribution ... Utilities ...
Installation ...
Patch Monitor Main Menu ...

You have 4 PENDING ALERTS
Enter "VA to jump to VIEW ALERTS option

Select Kernel Installation & Distribution System Option: Installation

1 Load a Distribution
2 Verify Checksums in Transport Global
3 Print Transport Global
4 Compare Transport Global to Current System
5 Backup a Transport Global
6 Install Package(s)
Restart Install of Package(s) Unload a Distribution

You have 4 PENDING ALERTS
Enter "VA to jump to VIEW ALERTS option

Select Installation Option: 1 Load a Distribution
Enter a Host File: C:\RPMS\busa0100.k  Type in the correct file path here

KIDS Distribution saved on Nov 05, 2013@19:58:24
Comment: IHS USER SECURITY AUDIT 1.0

This Distribution contains Transport Globals for the following Package(s): IHS USER
SECURITY AUDIT 1.0
Distribution OK!

Want to Continue with Load? YES// YES
Loading Distribution...

Build IHS USER SECURITY AUDIT 1.0 has an Environmental Check Routine
Want to RUN the Environment Check Routine? YES// YES
IHS USER SECURITY AUDIT 1.0
Will first run the Environment Check Routine, BUSA1PRE

Use INSTALL NAME: IHS USER SECURITY AUDIT 1.0 to install this Distribution.

1 Load a Distribution
2 Verify Checksums in Transport Global
3 Print Transport Global
4 Compare Transport Global to Current System
5 Backup a Transport Global
6 Install Package(s)
Restart Install of Package(s) Unload a Distribution

Select Installation Option: 2 Verify Checksums in Transport Global
Select INSTALL NAME: IHS USER SECURITY AUDIT 1.0 Loaded from Distribution
Loaded from Distribution 11/13/13@13:51:43
=> IHS USER SECURITY AUDIT 1.0 ;Created on Nov 05, 2013@19:58:24

```

```
This Distribution was loaded on Nov 13, 2013@13:51:43 with header of
IHS USER SECURITY AUDIT 1.0 ;Created on Nov 05, 2013@19:58:24
It consisted of the following Install(s): IHS USER SECURITY AUDIT 1.0
```

```
Want each Routine Listed with Checksums: Yes// YES
DEVICE: HOME// VT
```

```
PACKAGE: IHS USER SECURITY AUDIT 1.0 Nov 13, 2013 1:51 pm PAGE 1
-----
```

```
BUSA1PRE Calculated 7769799
BUSAACVR Calculated 1545256
BUSAAPI Calculated 16710103
BUSABQI Calculated 1009756
BUSACLAS Calculated 21482164
BUSAMAG1 Calculated 12323109
BUSAOPT Calculated 27951455
BUSARPC Calculated 117878520
BUSATRAN Calculated 6549672
BUSAUTIL Calculated 211041887
```

```
10 Routines checked, 0 failed.
```

```
1 Load a Distribution
2 Verify Checksums in Transport Global
3 Print Transport Global
4 Compare Transport Global to Current System
5 Backup a Transport Global
6 Install Package(s)
Restart Install of Package(s)
Unload a Distribution
```

```
Select Installation Option: 6 Install Package(s)
Select INSTALL NAME: IHS USER SECURITY AUDIT 1.0 Loaded from Distribution
Loaded from Distribution 11/13/13@13:51:43
=> IHS USER SECURITY AUDIT 1.0 ;Created on Nov 05, 2013@19:58:24
```

```
This Distribution was loaded on Nov 13, 2013@13:51:43 with header of
IHS USER SECURITY AUDIT 1.0 ;Created on Nov 05, 2013@19:58:24
It consisted of the following Install(s):
IHS USER SECURITY AUDIT 1.0
Checking Install for Package IHS USER SECURITY AUDIT 1.0
Will first run the Environment Check Routine, BUSA1PRE
```

```
Install Questions for IHS USER SECURITY AUDIT 1.0
```

```
Incoming Files:
```

```
9002319.01BUSA AUDIT LOG SUMMARY
9002319.02BUSA AUDIT LOG DETAIL
9002319.03BUSA AUDIT RPC DEFINITIONS (including data)
9002319.04BUSA SWITCH SETTINGS
9002319.05BUSA CACHE CLASS TRANSPORT (including data)
```

```
9002319.07BUSA RPC TRANSPORT LIST

Want KIDS to Rebuild Menu Trees Upon Completion of Install? NO// NO

Want KIDS to INHIBIT LOGONs during the install? NO// NO
Want to DISABLE Scheduled Options, Menu Options, and Protocols? NO// NO

Enter the Device you want to print the Install messages.
You can queue the install by enter a 'Q' at the device prompt. Enter a '^' to abort
the install.

DEVICE: HOME// VT
-----

Install Started for IHS USER SECURITY AUDIT 1.0 : Nov 13, 2013@13:52:02

Build Distribution Date: Nov 05, 2013

Installing Routines:
Nov 13, 2013@13:52:02

Running Pre-Install Routine: PRE^BUSA1PRE

Installing Data Dictionaries:
Nov 13, 2013@13:52:02

Installing Data:
Nov 13, 2013@13:52:02

Installing PACKAGE COMPONENTS:

Installing SECURITY KEY

Installing INPUT TEMPLATE

Installing REMOTE PROCEDURE

Installing OPTION
Nov 13, 2013@13:52:02

Running Post-Install Routine: POS^BUSA1PRE List started on 11/13/2013 13:52:02
Listing file H:\InterSystems\E3IHS\mgr\Temp\spb3KxKMfH5FjA.xml as xml
List finished successfully.

Load started on 11/13/2013 13:52:02
Loading file H:\InterSystems\E3IHS\mgr\Temp\8lKCnaziRxeXrg.xml as xml
Imported class: BUSA.MainReportPage
Imported class: BUSA.ReportingApp
Imported class: BUSA.Users, compiling 3 classes Compiling class BUSA.MainReportPage
Compiling class BUSA.ReportingApp

Compiling class BUSA.Users
Compiling table BUSA.Users
Compiling routine BUSA.MainReportPage.1
Compiling routine BUSA.ReportingApp.1
Compiling routine BUSA.Users.1
Load finished successfully.

Updating 9002319.05 Record
```

```
Enter the user to add/delete BUSA Reporting Access for
```

```
User: EVERETT,BRIAN E BEE
```

```
User set up for BUSA Reporting Access
```

```
Current approved BUSA Reporting Users
```

```
EVERETT,BRIAN E
```

```
Enter the user to add/delete BUSA Reporting Access for
```

```
User:
```

```
Updating Routine file...
```

```
Updating KIDS files...
```

```
IHS USER SECURITY AUDIT 1.0 Installed.
```

```
Nov 13, 2013@13:52:36
```

```
Not a VA primary domain
```

```
Install Completed
```

5.0 Configuring the IHS USER SECURITY AUDIT Web Application

Please note – it is recommended that the site use a standalone IIS or Apache™ web server with Secure Sockets Layer (SSL) configuration and not the private web server provided by InterSystems. The instructions here are meant to be used for testing purposes only.

Next, configure the security settings for the IHS USER SECURITY AUDIT (BUSA) application which was automatically created by the import and compile process.

5.1 Enable System Authentication Options

1. Sign on to the Ensemble System Management Portal
2. Select **System Administration** in the left column.
3. Select **Security >> System Security >> Authentication/CSP Session Options**.
4. The screen in Figure 5-1 will display.

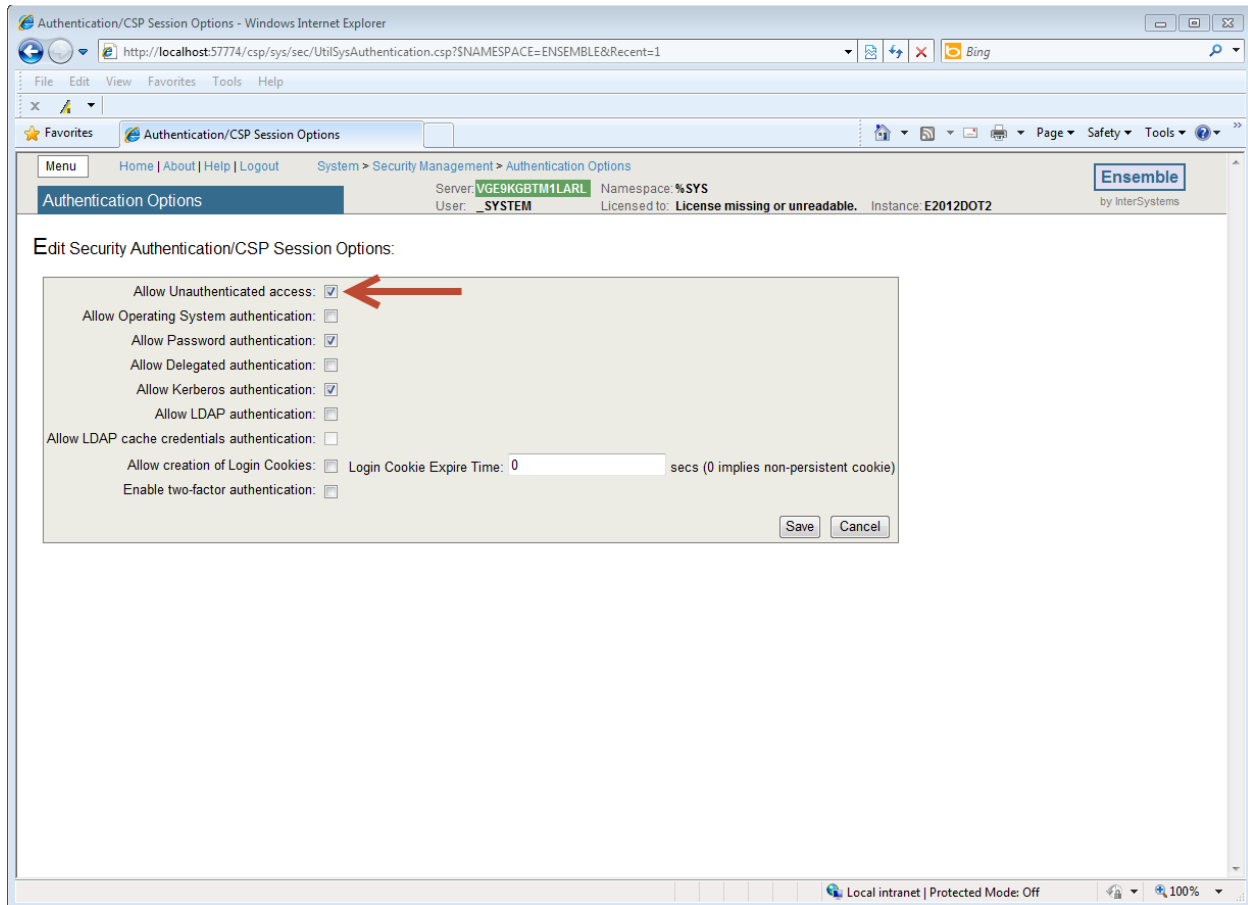


Figure 5-1: System Administration->Security->System Security->Authentication/CSP Options

1. Make sure that the “**Allow Unauthenticated access:**” box is checked then click “**Save.**” The change will take effect immediately.

5.2 Create New Web Application

1. Return to the main Ensemble Management Portal page. Select **Security >> Applications >> Web Applications** under **System Administration** in the left column. The **Web Applications** page similar to Figure 5-2 will display:

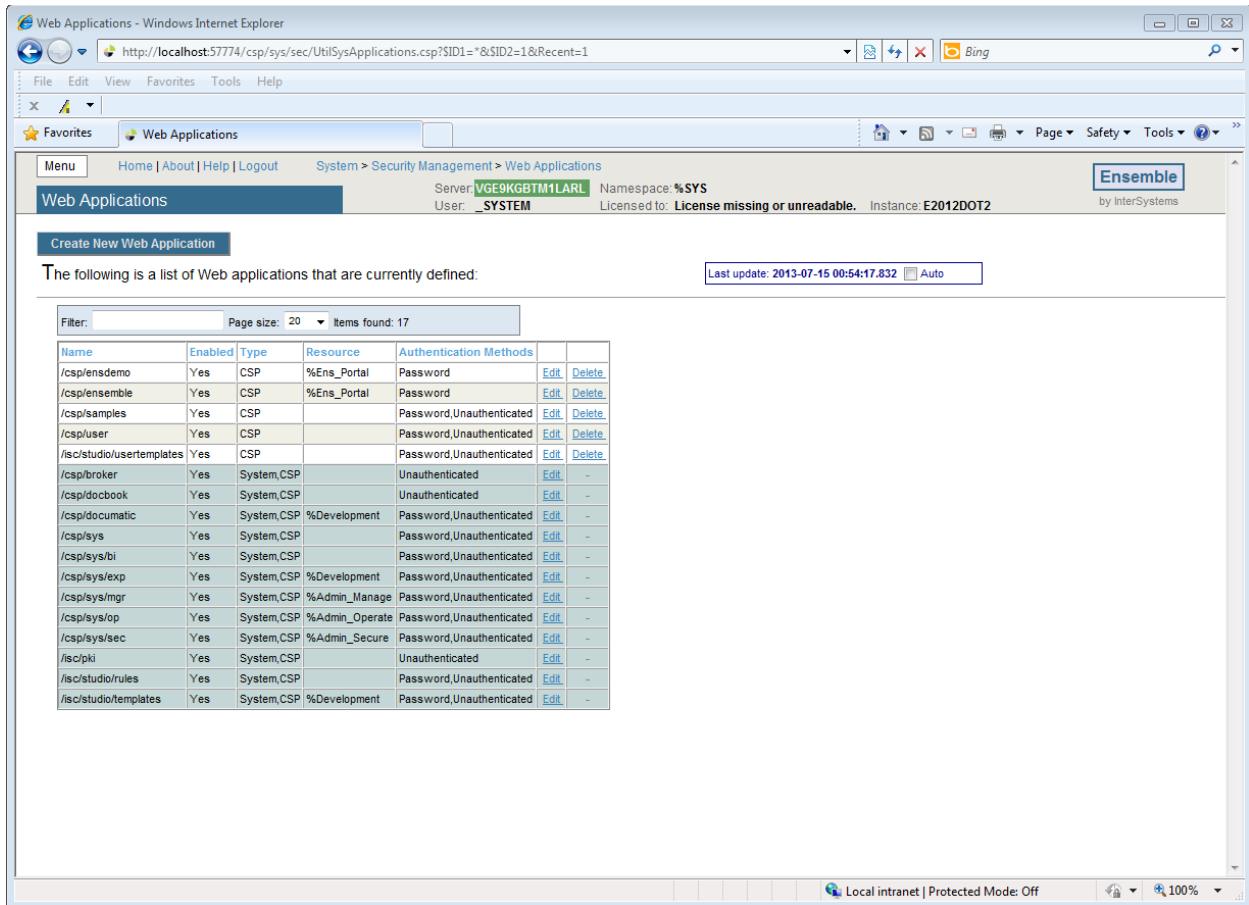


Figure 5-2: Web Applications screen

2. Select **Create New Web Application** and fill out the values similar to Figure 5-33.

Figure 5-3: **Edit Web Application** screen

3. For Web Application Name put in **/csp/busa**.
4. Description is **BUSA Audit**.
5. For Allowed Authenticated Methods make sure **Unauthenticated** is checked.
6. For **Namespace**, select the site's RPMS namespace
7. For **CSP Files Physical path**, locate the directory as <cacheinstance>/csp/<RPMSinstance> (see Figure 4-3)
8. For Login Page, type **BUSA.MainReportPage.cls**.

5.3 Update Ensemble's UnknownUser

1. Return to the main Ensemble Management Portal page. Select **Security >> Users** under **System Administration** in the left column. The Users page similar to Figure 5-4 will display:

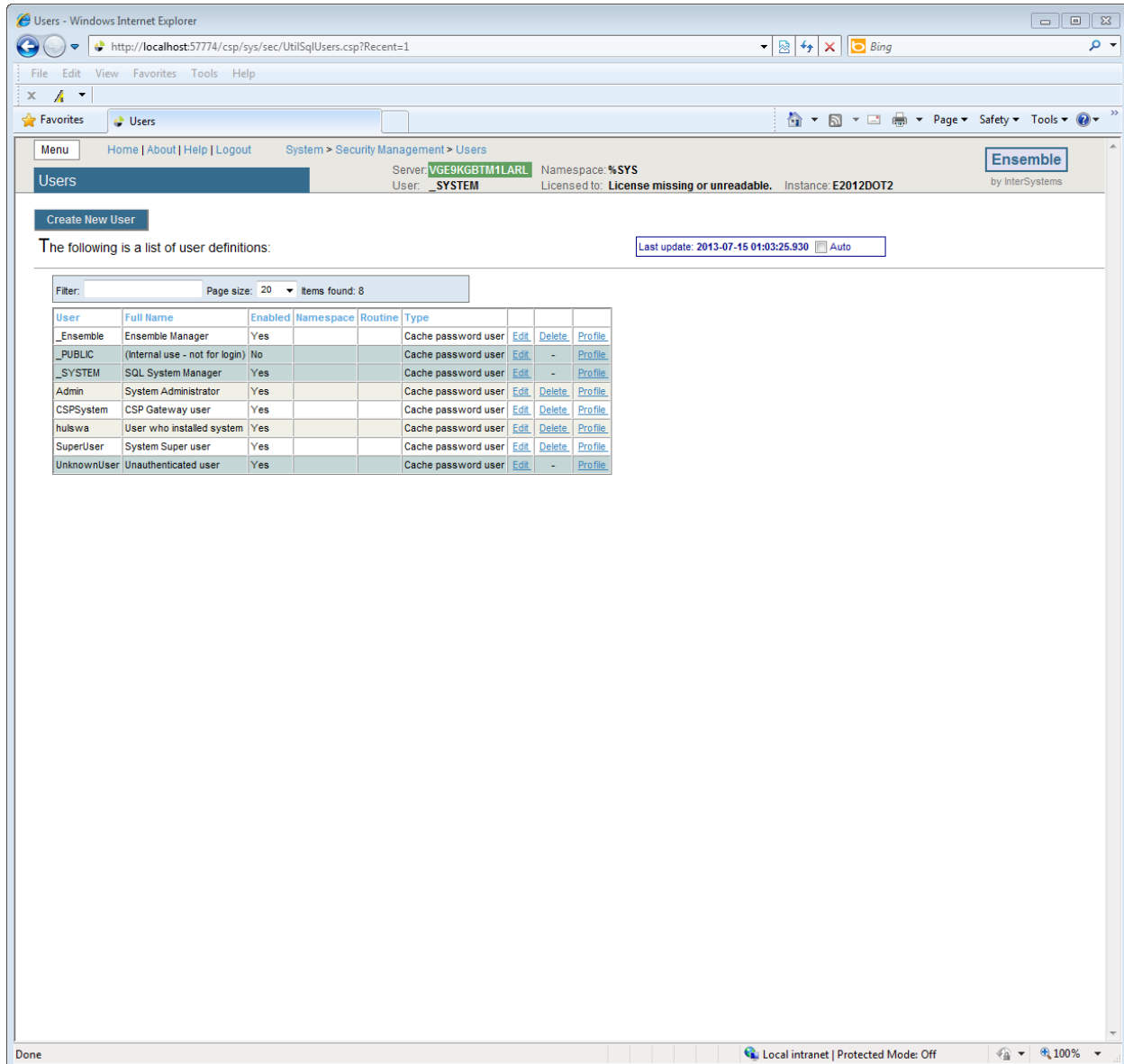
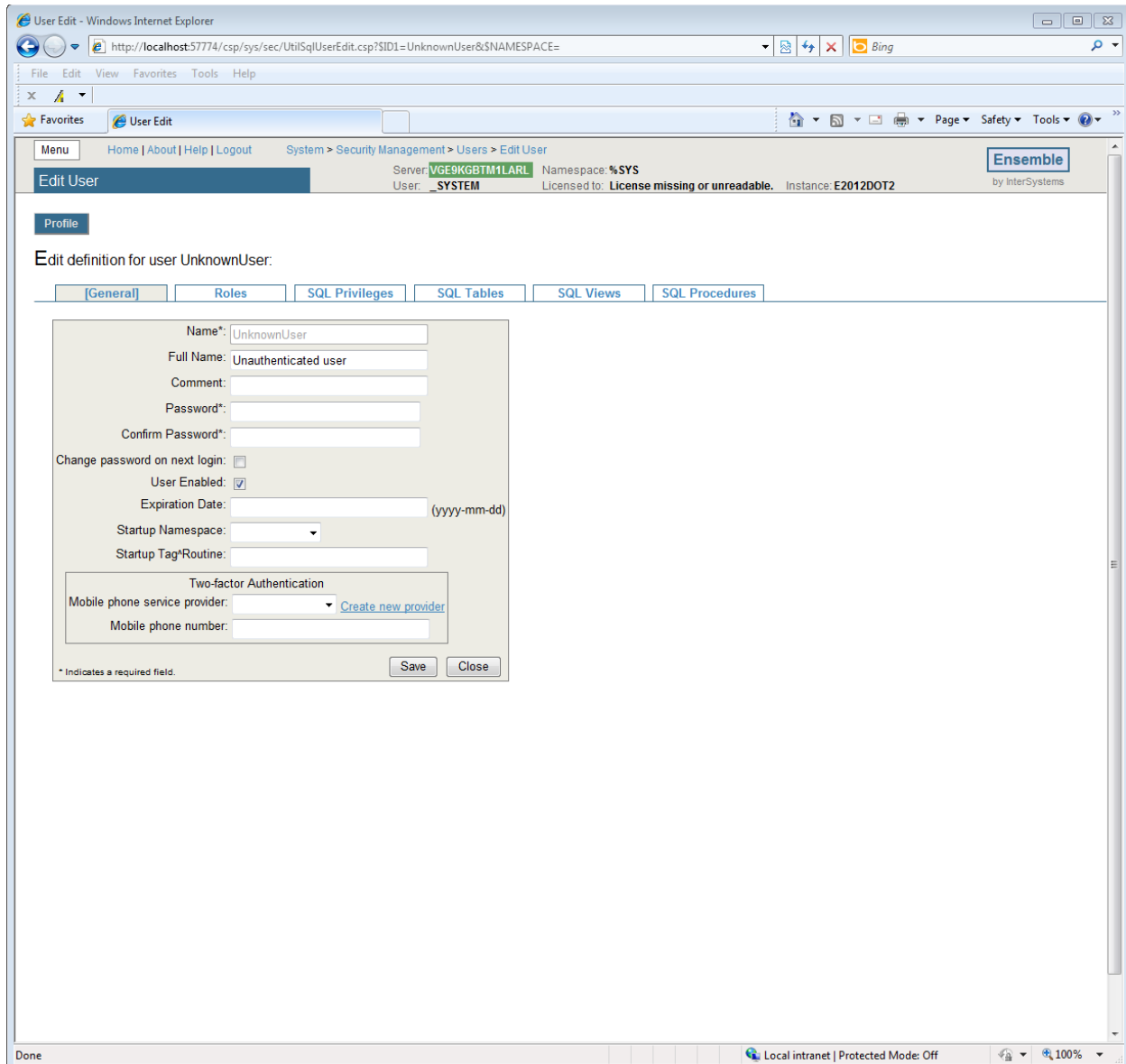


Figure 5-4: User Management screen

2. Locate the user called **UnknownUser** on this screen. Once found, click on the **Edit** link. A screen similar to Figure 5-5 will display.

Figure 5-5: **Edit User** screen

- Click on the word **Roles** immediately under **Edit definition for user UnknownUser** and the **Edit User** screen similar to Figure 5-6 will display:

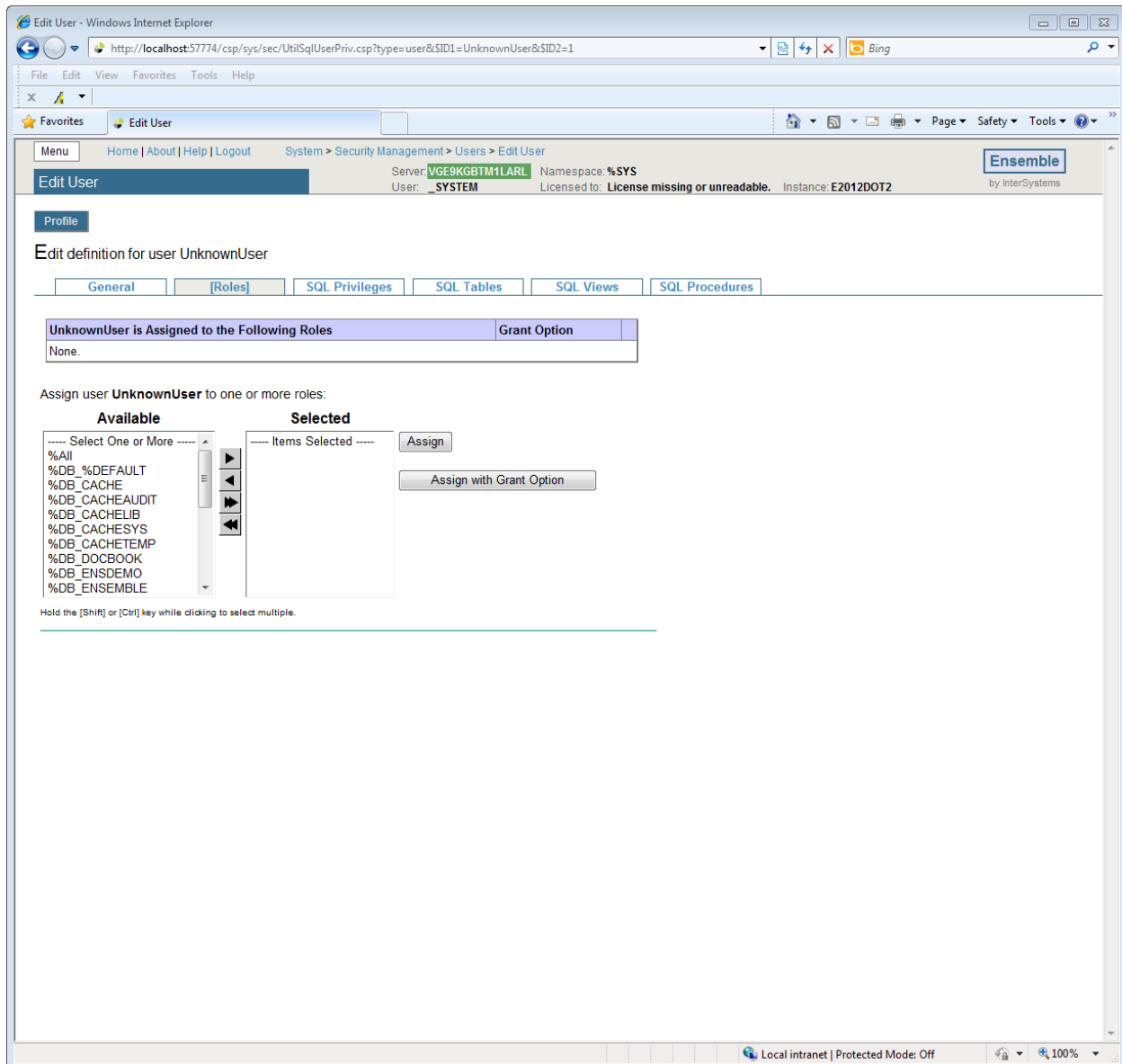


Figure 5-6: Edit User

4. If the list of roles which appears at the top of the page immediately under **UnknownUser is Assigned to the Following Roles** includes **%All**, then no further action in this section is required. If not, then select **%All** in the list of **Available** roles on the left hand side of the page, and click the top arrow located between the **Available** and **Selected** columns.
5. Once **%All** appears in the **Selected** column, click on the Assign button and **%All** will appear under **UnknownUser is Assigned to the Following Roles** indicated in Figure 5-7:

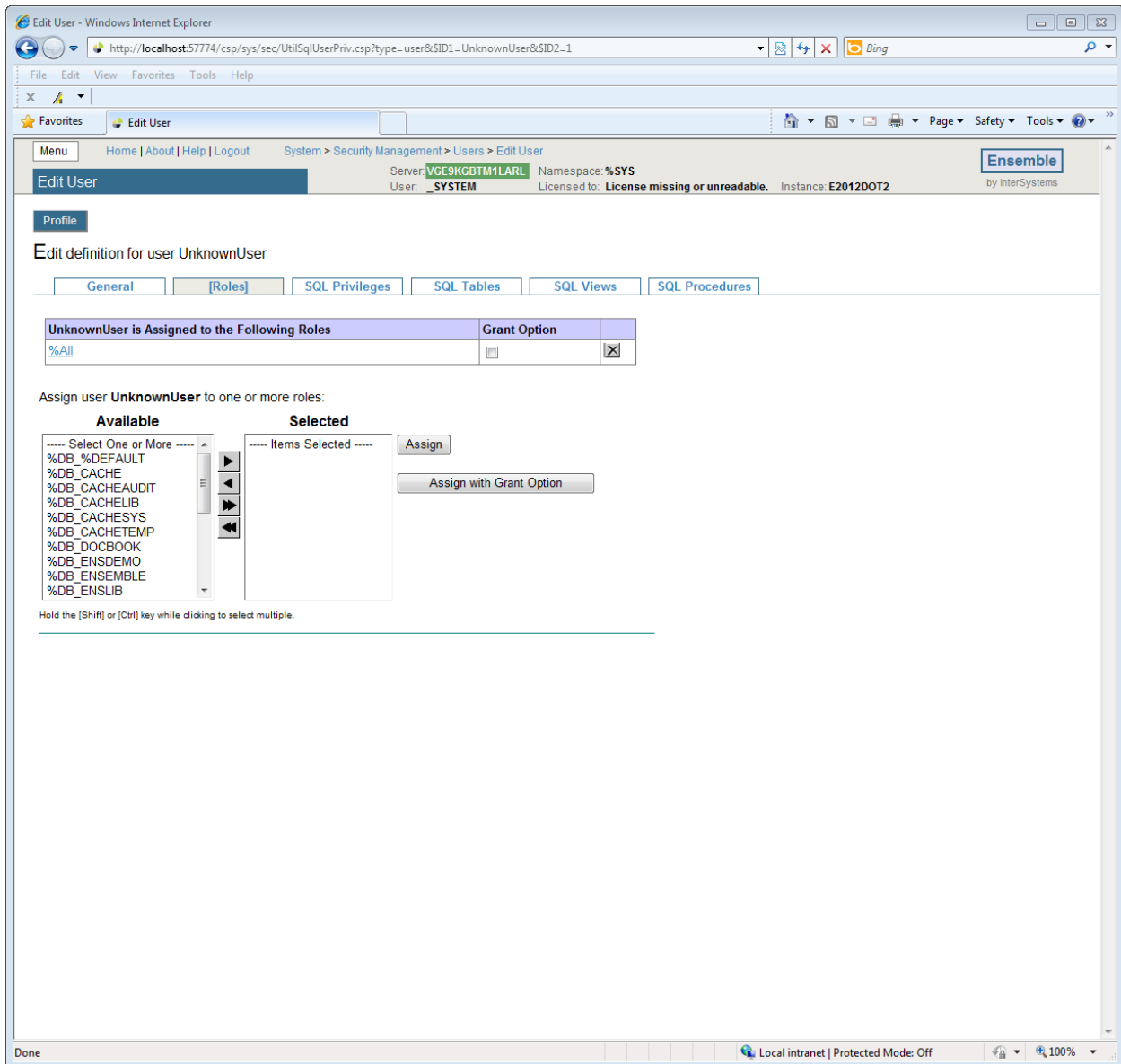


Figure 5-7: Edit User - Roles tab

6. The Web application portion and security setup is complete.

6.0 Cache Server Page (CSP) Web Gateway Installation

The CSP Web Gateway provides the communications layer between the hosting Web server and Ensemble when you call a Caché® Server Page (CSP) or Caché® Zen application. The purpose of using the Web Gateway is to offload the access to the BUSA application to a dedicated web server, as well as use Secure Socket Layer (SSL) communication to encrypt the data between the user and the server.

Note: The instructions in this section assume the site is running Microsoft Internet Information Server (version 7 or higher) with a valid installed SSL certificate. Installation of IIS and SSL certificates are outside the scope of this document.

6.1 Install Cache Shell

1. Start by launching the Ensemble executable appropriate for your version of Windows and checking **I accept the terms in the license agreement** and click **Next** as indicated in Figure 6-1.

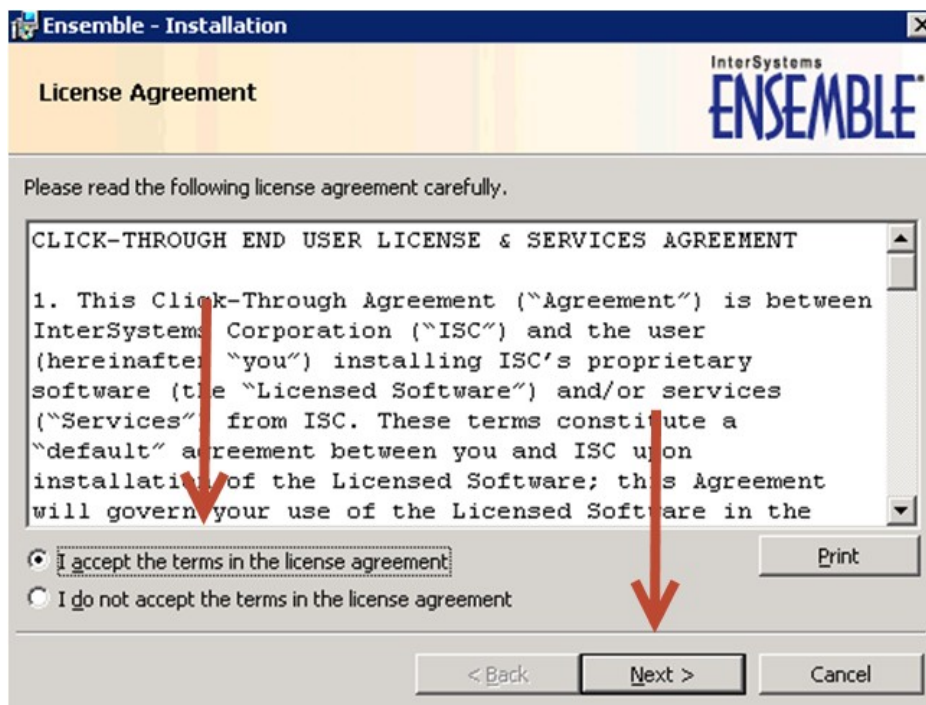


Figure 6-1: Ensemble Installation – License Agreement

2. Enter a unique Ensemble Instance Name for this physical machine and click **Next** as indicated in Figure 6-2.

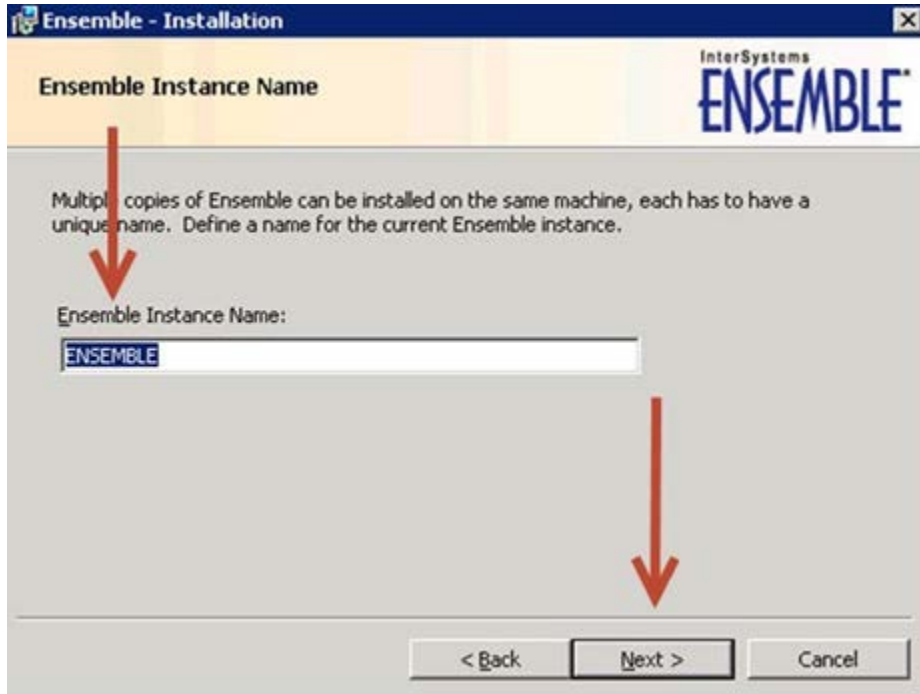


Figure 6-2: Ensemble Installation - Ensemble Instance Name

3. On the next screen, enter the path where the Ensemble shell will be located by clicking **Change** as in Figure 6-3.

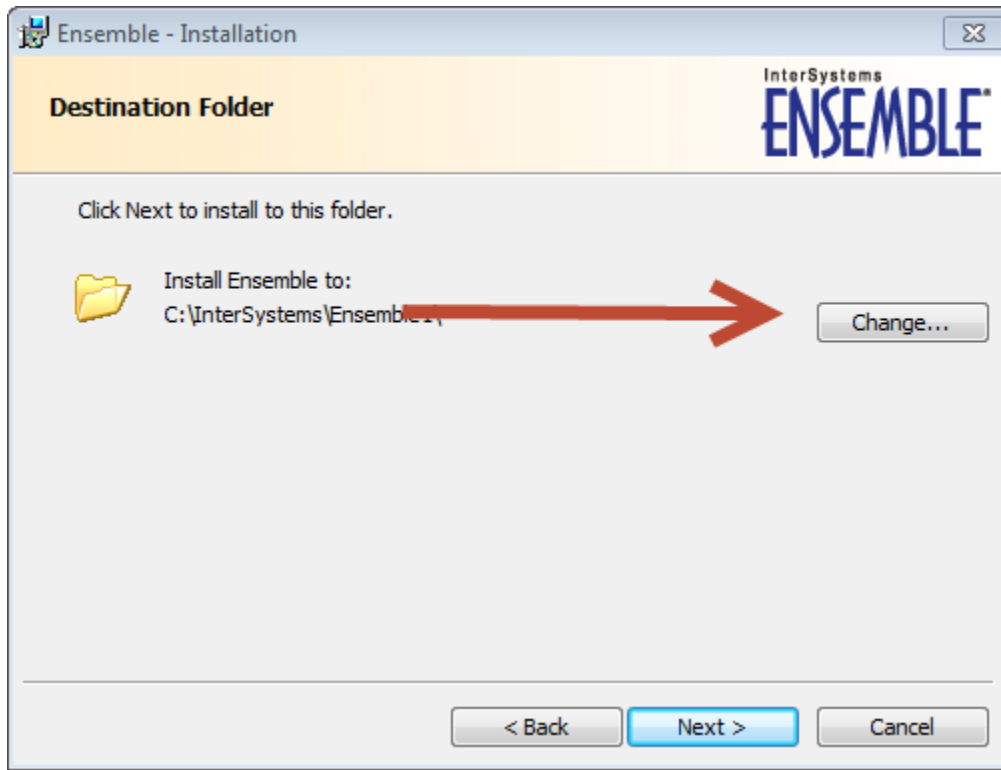


Figure 6-3: Ensemble Installation – Destination Folder

- 4. Install into the directory C:\InterSystems\EnsembleCSP and click **OK** as indicated in Figure 6-4.

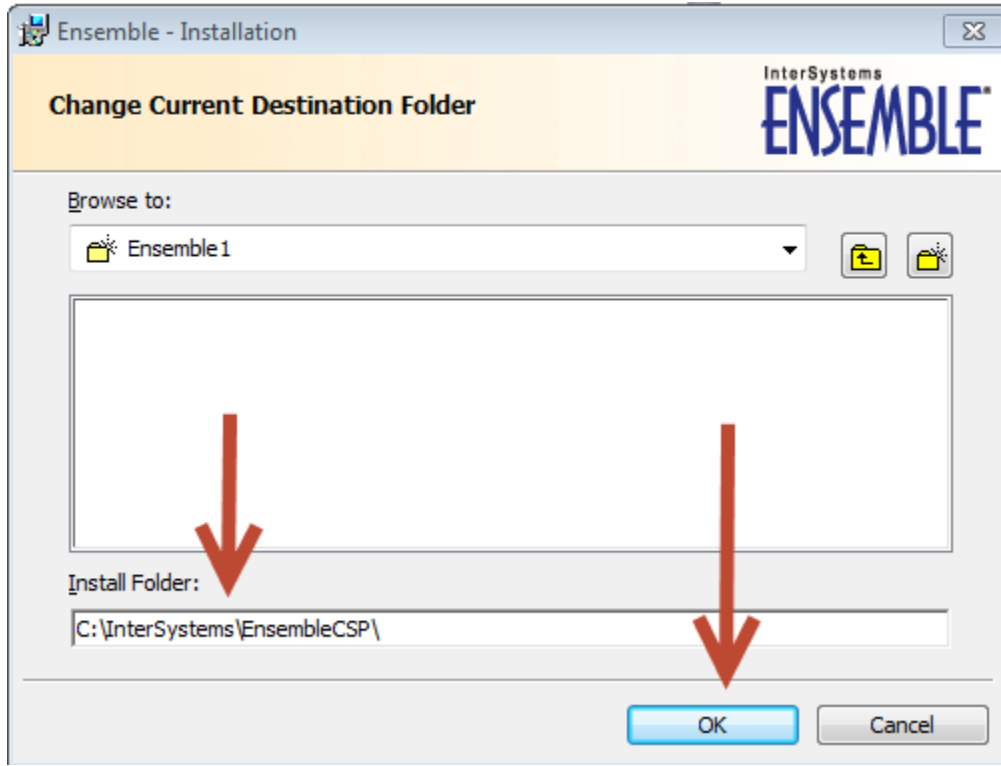


Figure 6-4: Ensemble Installation – Change Current Destination Folder

5. Select **Web Server** on the next screen and click **Next** as indicated in Figure 6-5.

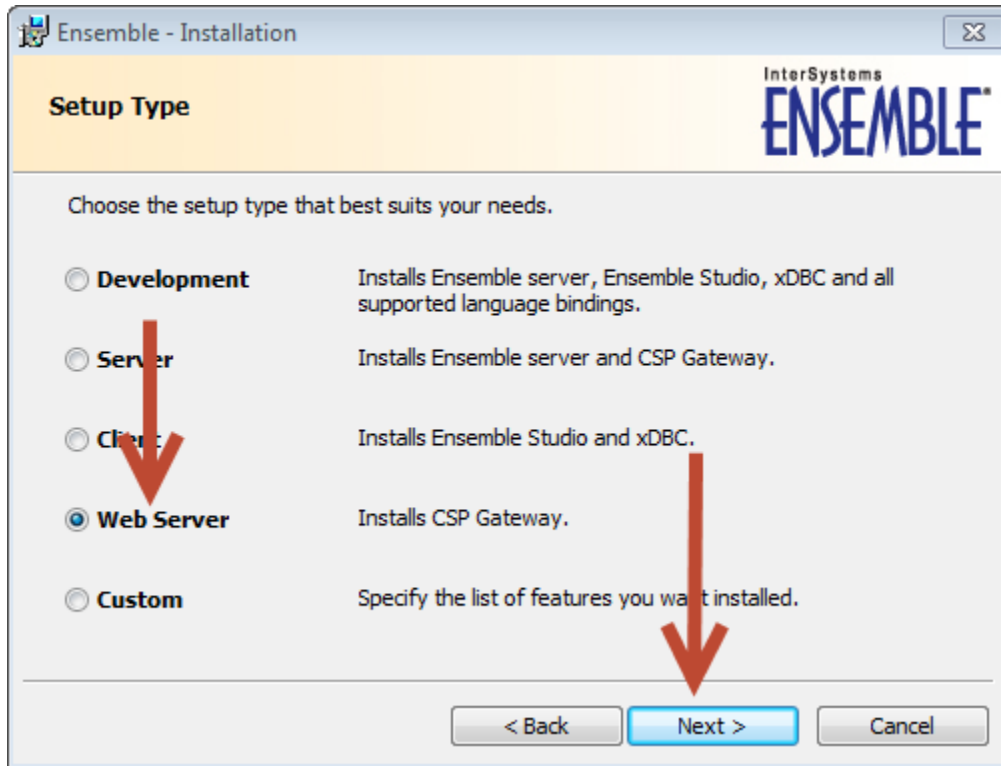


Figure 6-5: Ensemble Installation – Setup Type

6. A screen will appear as in Figure 6-6 allowing a review of the options. Review and click **Install**.

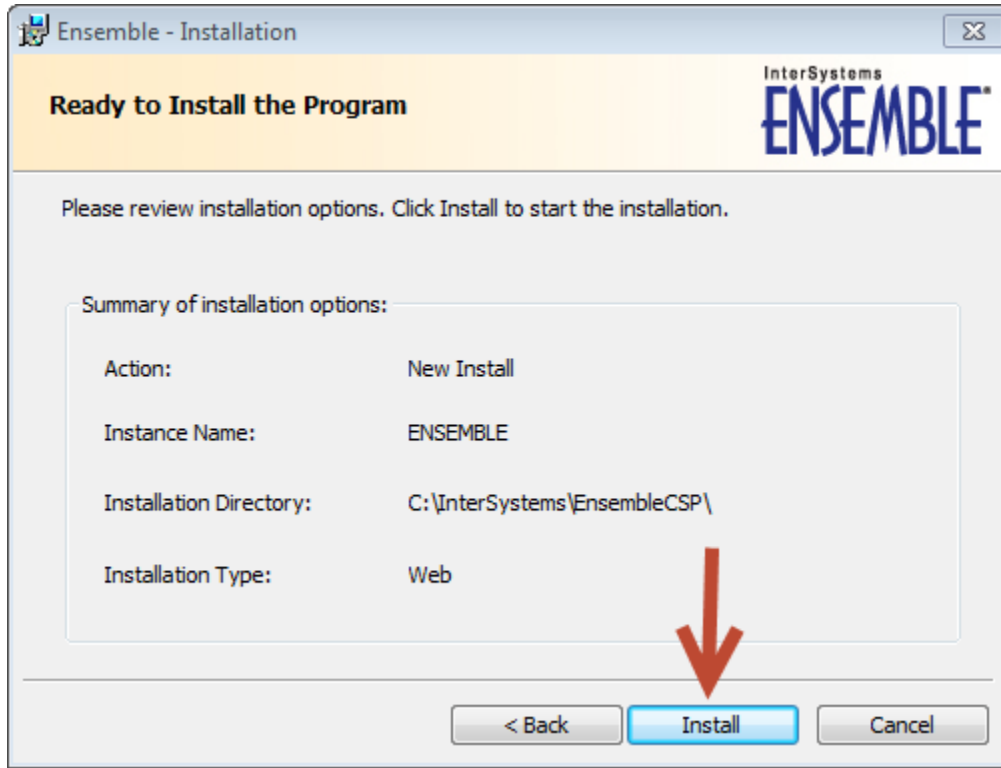


Figure 6-6: Ensemble Installation – Ready to Install the Program

7. If IIS is running you will receive a warning message asking you to stop the IIS WebServer as seen in Figure 6-7. Click **Yes** and it will stop IIS and continue the installation process.

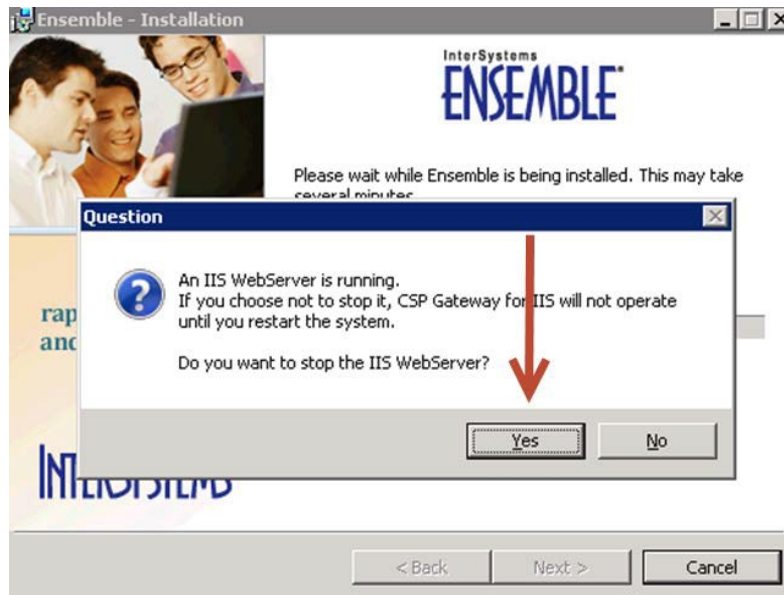


Figure 6-7: **Ensemble Installation** – Stop IIS webserver

8. Click **Finish** on the screen to complete the installation as indicated in Figure 6-8.

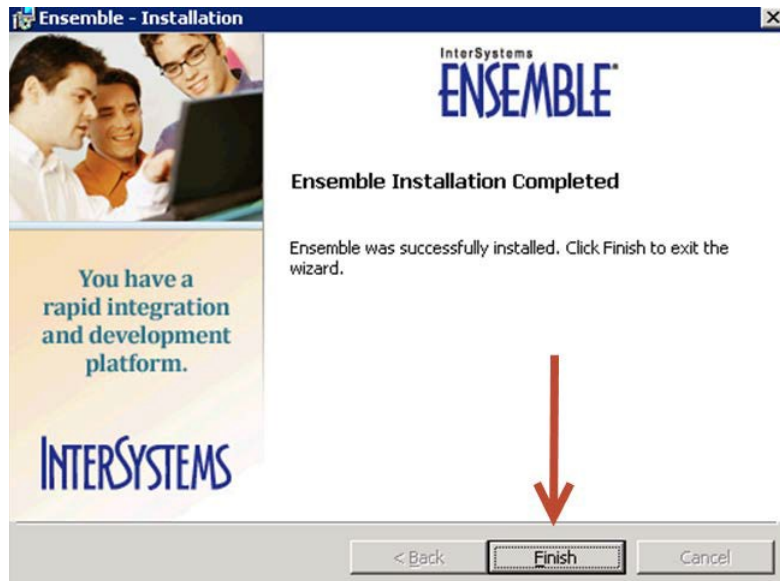


Figure 6-8: **Ensemble Installation** - Finish

6.2 Configure IIS

1. On the webserver that the CSP gateway was just installed, navigate to **Administrative Tools -> Internet Information Services (IIS) Manager** as indicated in Figure 6-9.

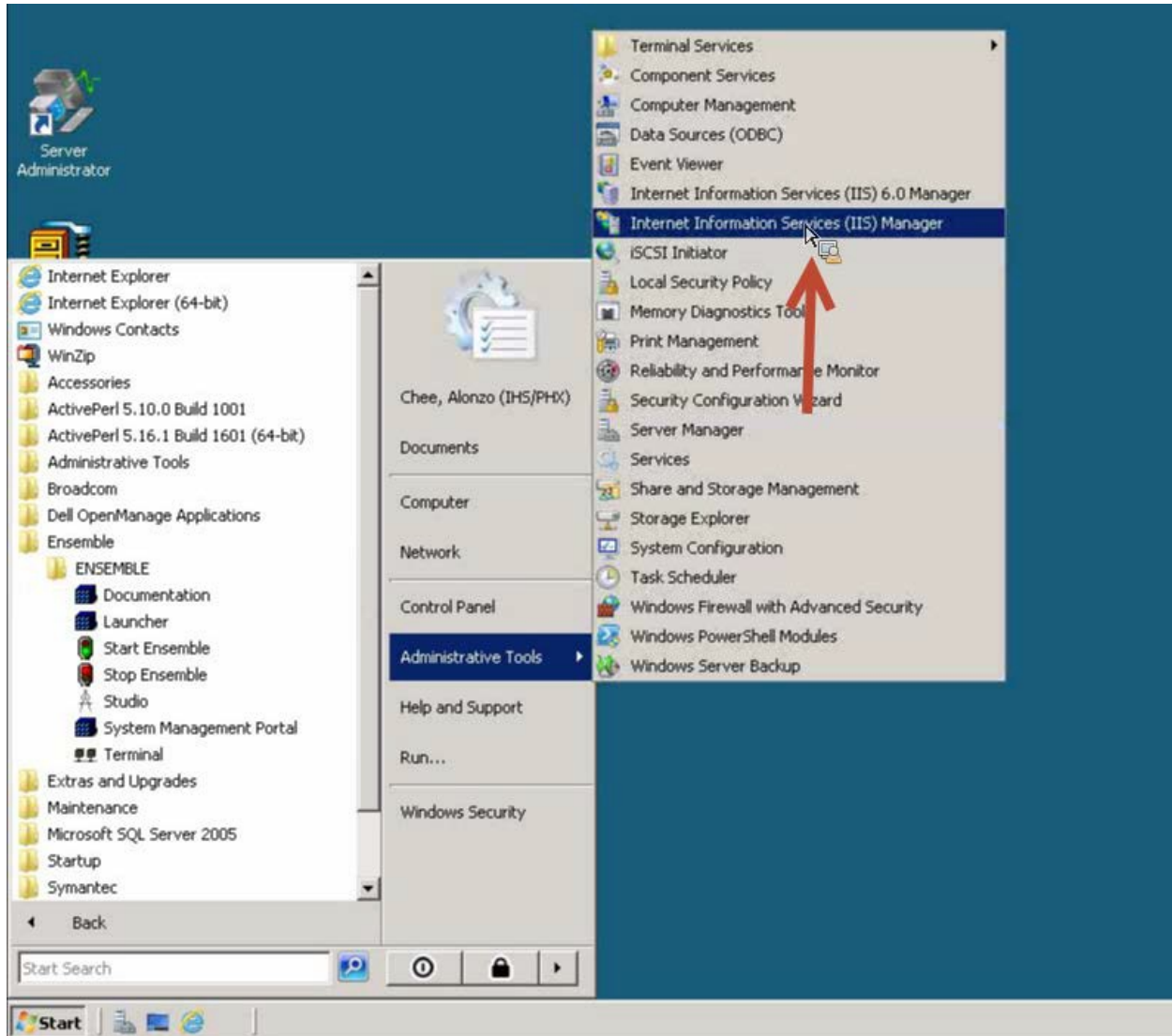


Figure 6-9: Ensemble Installation cont'd

2. Select **Default Web Site**, click on **csp**, then **Handler Mappings** as indicated in Figure 6-10.

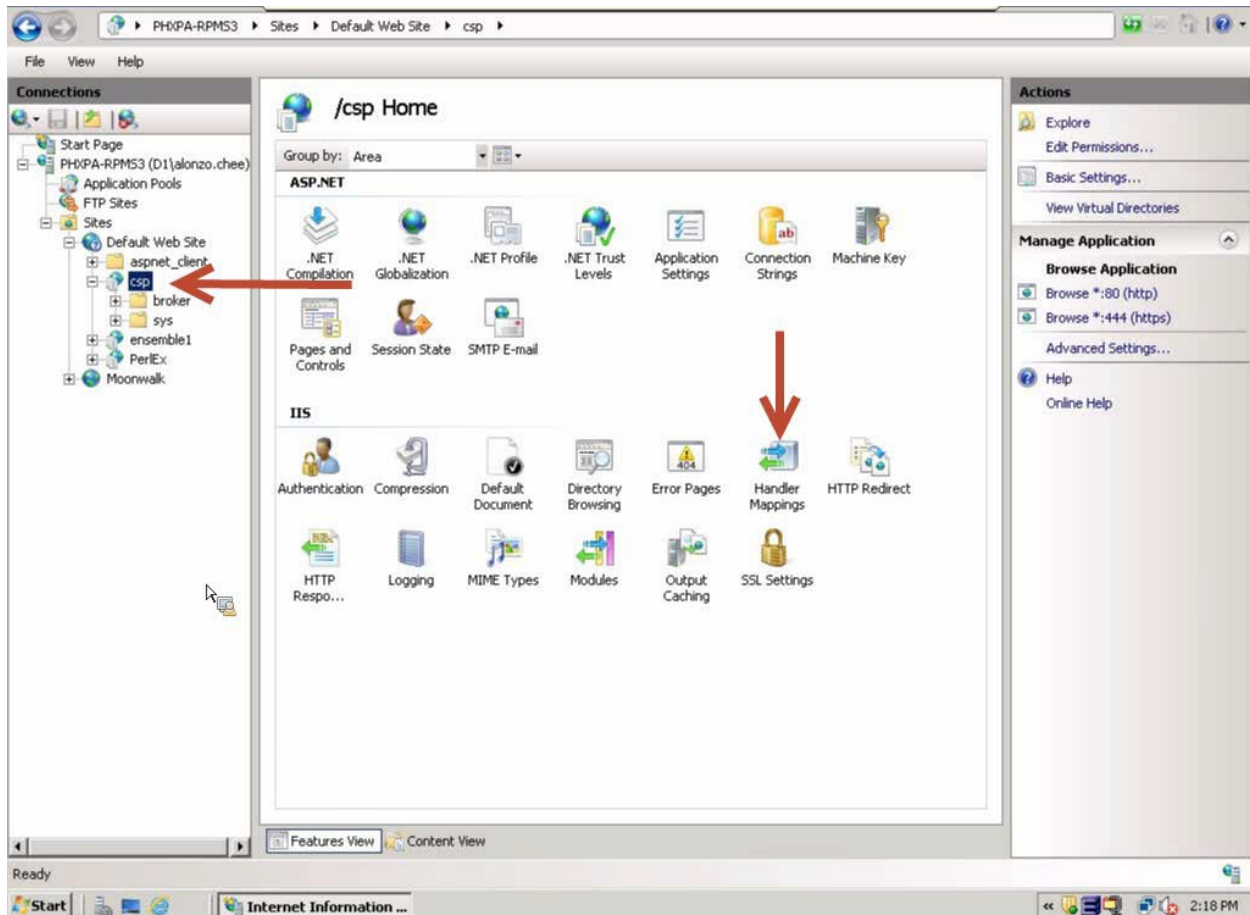


Figure 6-10: IIS Handler Mappings

3. Validate that the **CSPGateway_*** mappings are present for ***.cls**, ***.csp**, ***.cxw** and ***.zen**, and that they are listed as **Enabled** as indicated in Figure 6-11.

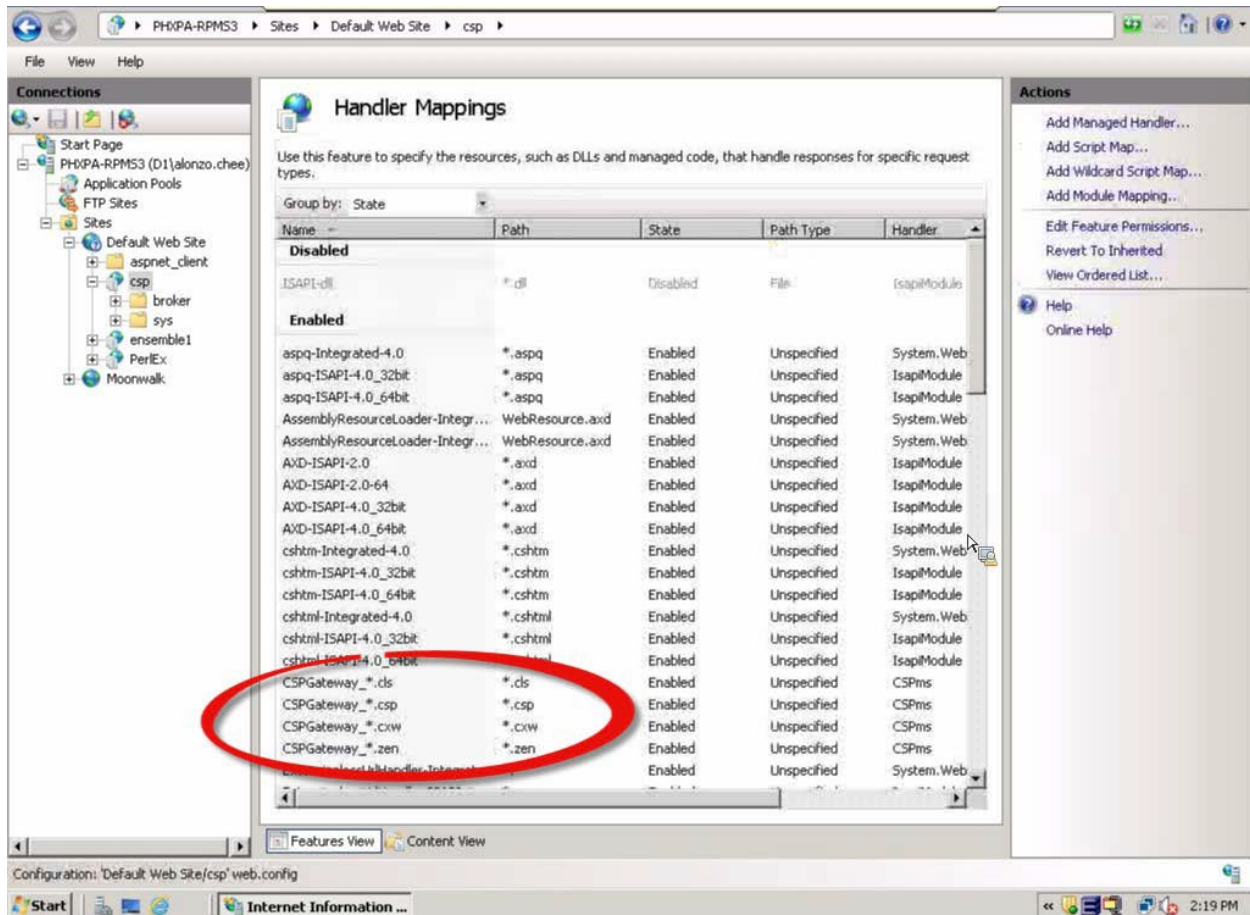


Figure 6-11: IIS Handler Mappings cont'd

4. In order to have IIS handle CSP applications like BUSA via IIS, click **Add Module Mapping** and enter values as indicated in Figure 6-12.

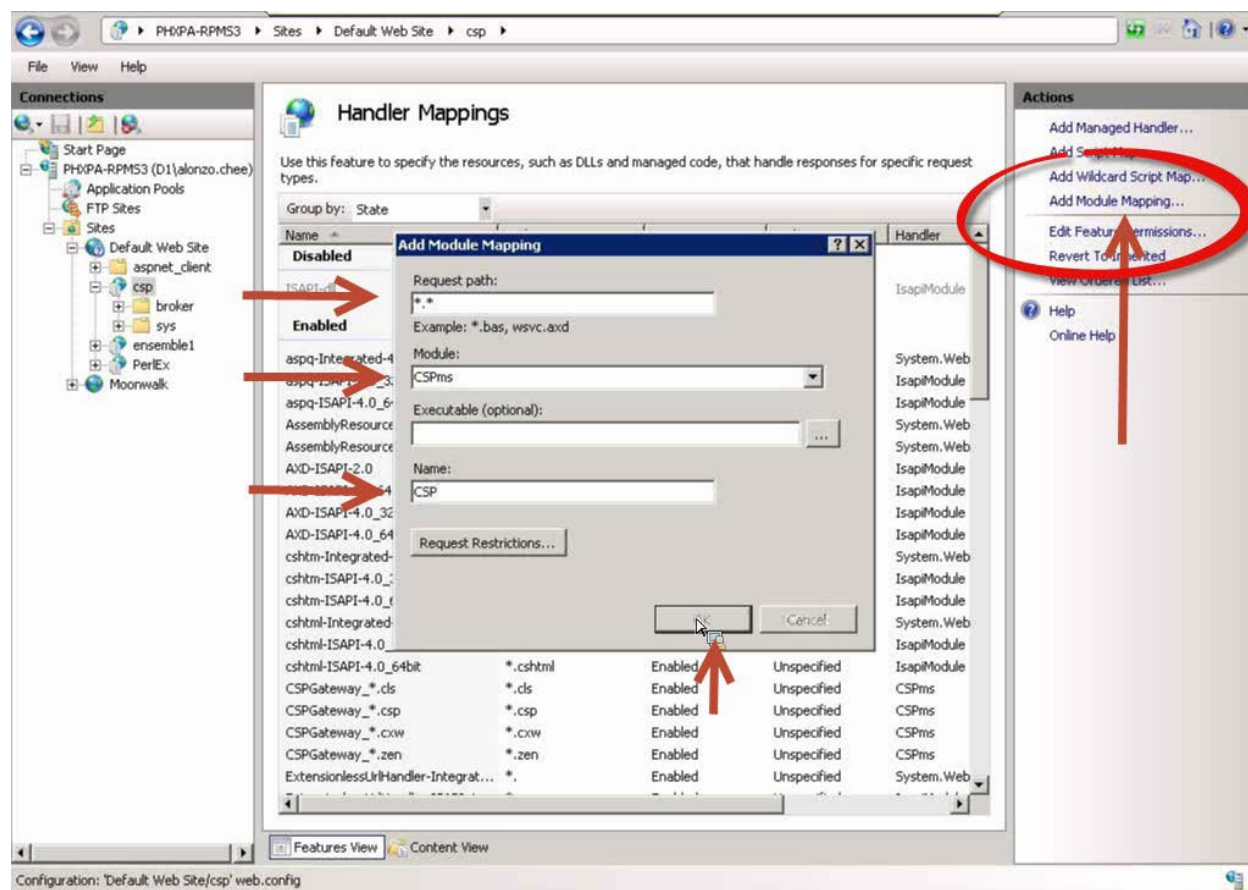


Figure 6-12: IIS Handler Mappings – Add Module Mapping

6.3 Configure CSP Web Gateway

1. While connected to the server where the CSP Web Gateway was installed, enter the following link in a web browser:
<http://localhost:PORT/csp/bin/Systems/Module.cwx>

Where PORT should be set to the appropriate assigned port number.

Providing the correct link is entered, the following screen shown in Figure 6-13 will appear.

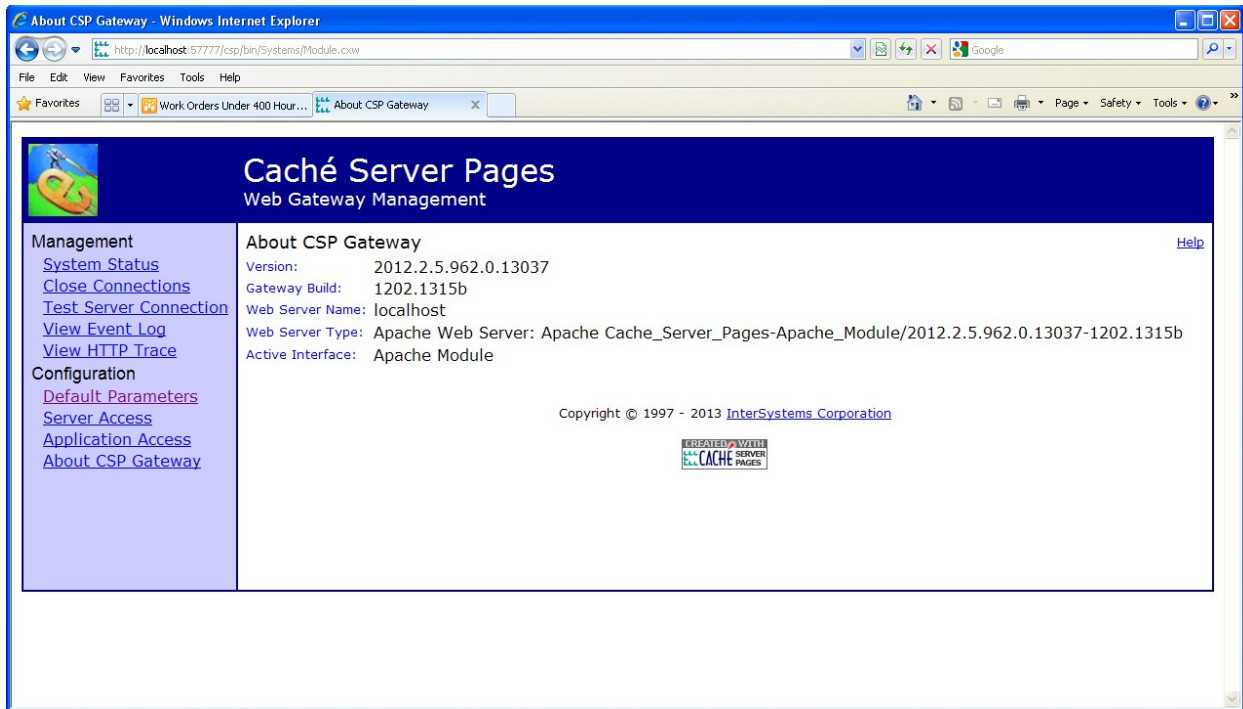


Figure 6-13: CSP Web Gateway configuration

2. Click on **Default Parameters** as indicated in Figure 6-14.

Figure 6-14: Navigate to the **Default Parameters**

- Located the Connections to Cache parameters section

- In the **Server Response Timeout** and **Queued Request Timeout** fields, adjust each value so that the reporting tool can handle searches which will be sifting through large amounts of data and which might return a large number of results. The values entered in these fields depend largely on the system processing capabilities and the typical load on the system. If, when performing searches, users are frequently encountering gateway timeout errors, then these values should be increased. An initial setting of 180 (3 minutes) should be a good starting value to place into these fields. See Figure 6-15 for locations of these parameters. Click **Save Configuration**.

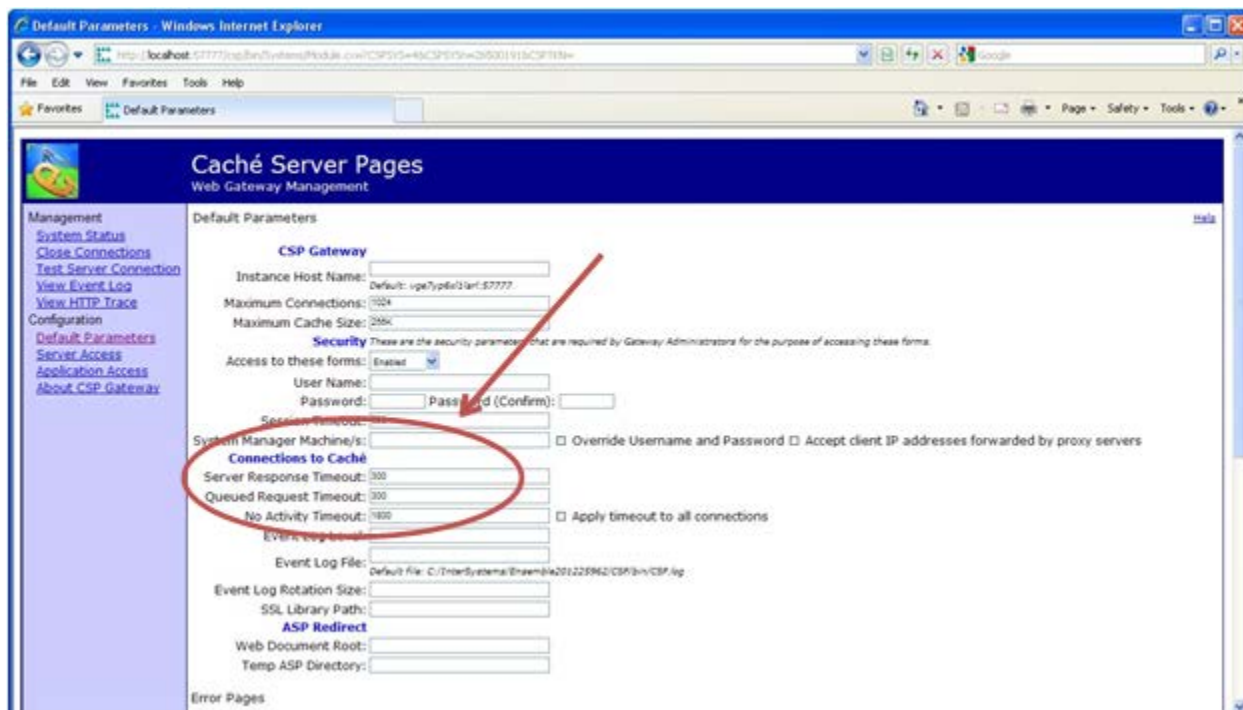


Figure 6-15: Adjusting the gateway timeout settings

3. Click on **Server Access** and **Add Server** as indicated in Figure 6-16.

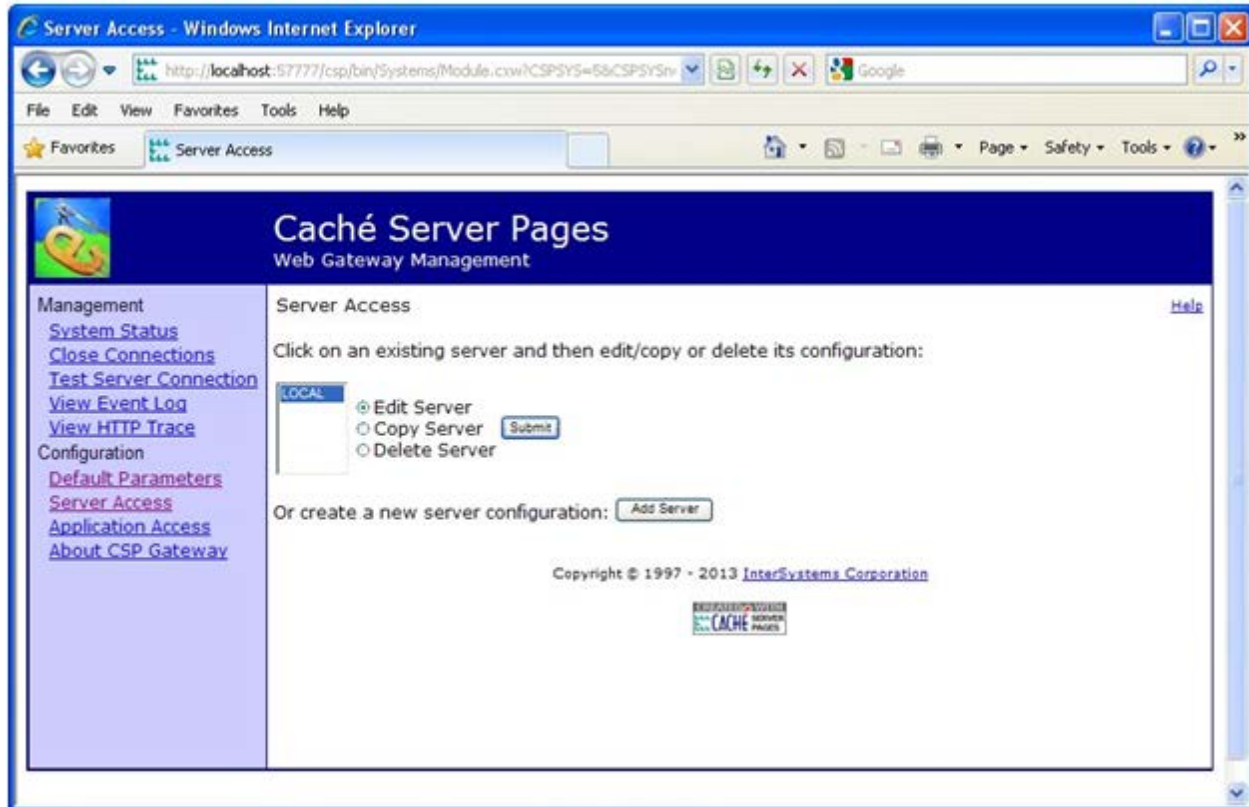


Figure 6-16: CSP Gateway configuration - Server Access and Add Server

4. Insert the appropriate site information in the highlighted areas on the following screen as indicated in Figure 6-17, and click **Save Configuration** at the bottom when complete.

The screenshot displays the 'Caché Server Pages' Web Gateway Management interface. The browser address bar shows 'http://localhost:57772/csp/bin/Systems/Module.cxx'. The page title is 'Caché Server Pages' and the subtitle is 'Web Gateway Management'. A navigation menu on the left includes 'Management' (System Status, Close Connections, Test Server Connection, View Event Log, View HTTP Trace) and 'Configuration' (Default Parameters, Server Access, Application Access, About CSP Gateway). The main content area is titled 'Server Access' and contains the following configuration fields:

- Server Name:** RPMS
- Service Status:** Enabled
- IP Address:** 10.0.1.120
- TCP Port:** 1972
- State-Less Parameters:**
 - Minimum Server Connections: 3
 - Maximum Server Connections: [empty]
 - Maximum Connections per Session: 3
- Connection Security:** *These are the security settings that are required by the Gateway for the purpose of accessing this server.*
 - Connection Security Level: Password
 - User Name: CSPSystem
 - Password: [masked] Password (Confirm): [masked]
 - Product: Cache
 - Service Principal Name: [empty]
 - Key Table: [empty]
 - SSL Protocol: SSLv2 SSLv3 TLSv1
 - SSL Key Type: RSA
 - Require peer certificate verification
 - SSL Certificate File: [empty]
 - SSL Certificate Key File: [empty]
 - SSL CA Certificate File: [empty]
 - SSL Private Key Password: [empty]
- Optional Parameters:** *These parameters will be inherited from the CSP Gateway 'Default Parameters' if not specified here.*
 - Server Response Timeout: [empty] *Inherited Value: 60*
 - No Activity Timeout: [empty] *Inherited Value: 1800* Apply timeout to all connections
 - Event Log Level: [empty] *No Value to Inherit*
- Error Pages:** *Enter the filename of the html page to display or a URL to redirect the browser to if this error occurs. These values will be inherited from the CSP Gateway.*

Figure 6-17: CSP Web Gateway configuration – Site Information

- Click on **Application Access** and **Add Application** as indicated in Figure 6-18.



Figure 6-18: Web Gateway configuration cont'd

6. On the following screen, for **Application Path:** set to `/csp/busa` and for **Default Server:** select your previously configured server name from the dropdown, then click **Save** as indicated in Figure 6-19.

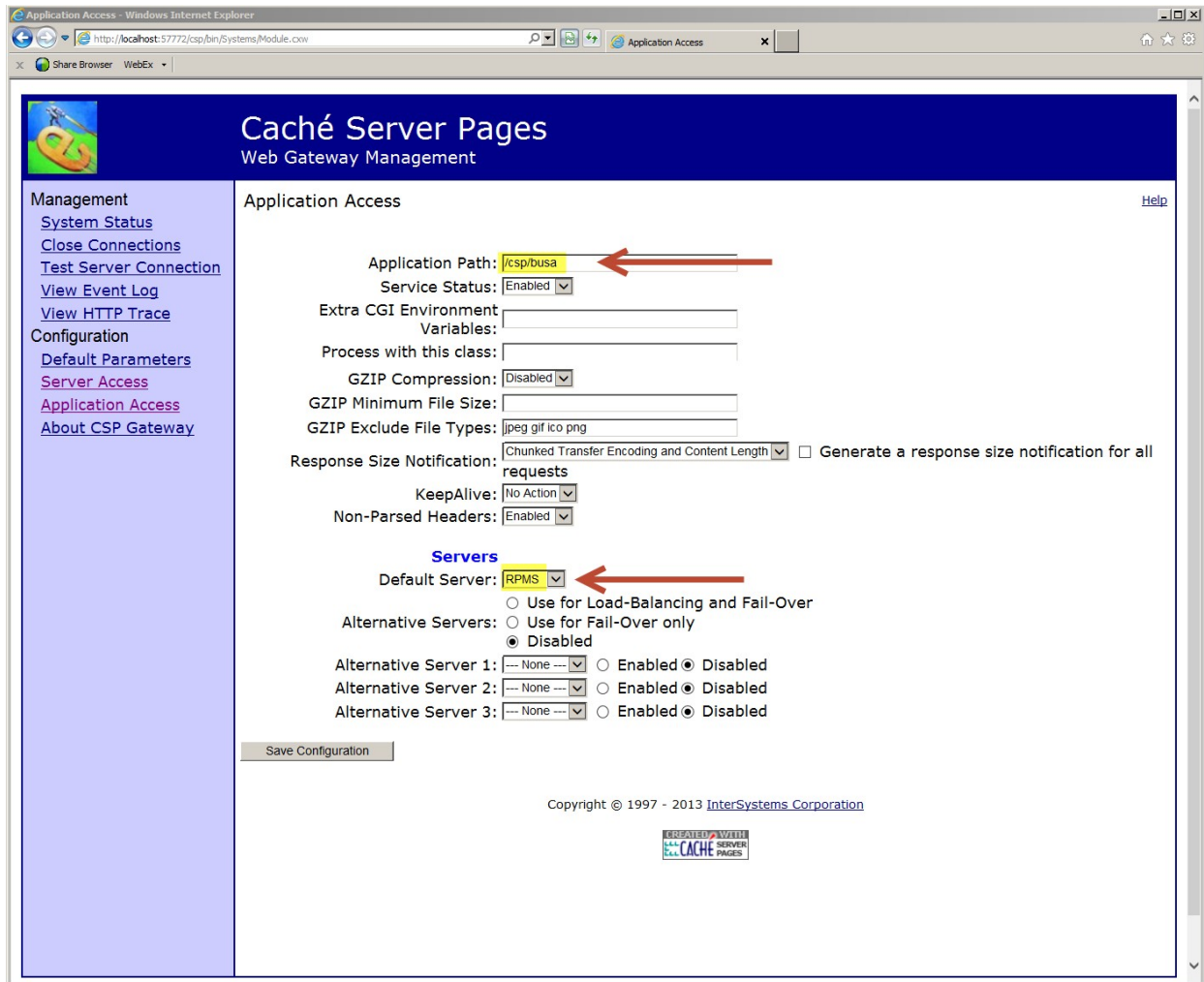


Figure 6-19: CSP Web Gateway configuration – **Application Access**

7. Click on **Test Server Connection**. If successful the following screen will appear similar to Figure 6-20.

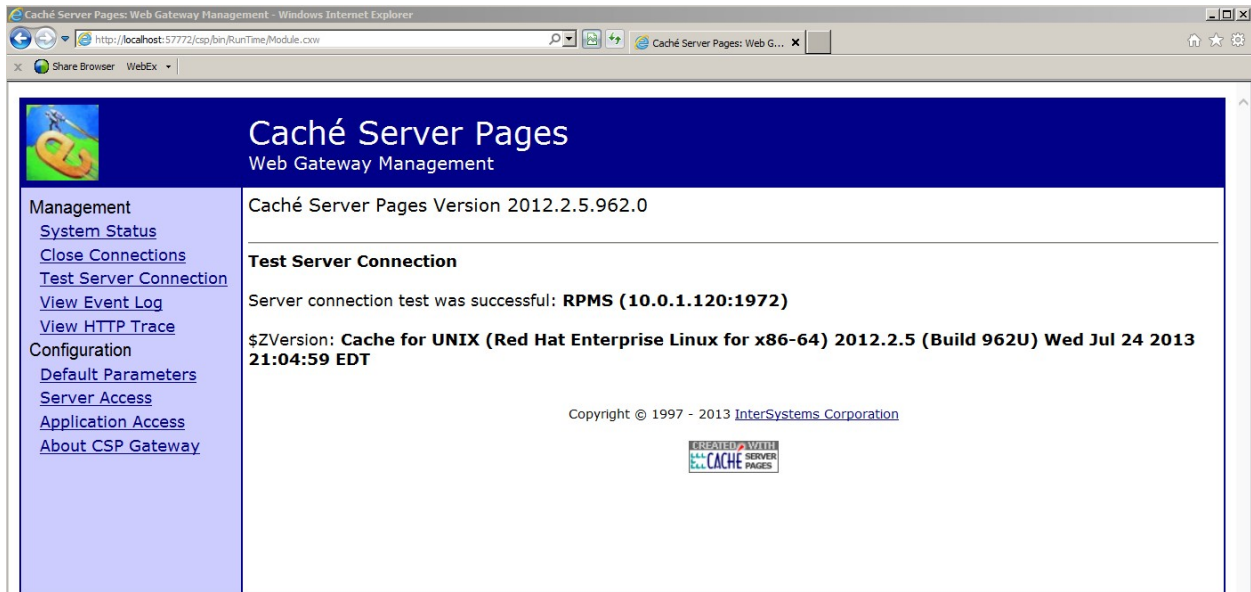


Figure 6-20: CSP Web Gateway configuration – Test Server Connection

8. Enter the website link for the ED Dashboard from a workstation browser, for example: <http://10.24.196.43:57777/csp/busa/BUSA.MainReportPage.cls> and the page as shown in Figure 6-21 will appear.



Figure 6-21: Sample BUSA Reporting page

Acronym List

API	Application Programming Interface
BUSA	IHS USER SECURITY AUDIT
CPU	Central Processing Unit
IHS	Indian Health Service
KIDS	Kernel Installation and Distribution System
MU	Meaningful Uss
RPMS	Resource and Patient Management System

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (888) 830-7280 (toll free)

Web: <http://www.ihs.gov/helpdesk/>

Email: support@ihs.gov