

WebSphere Portal Server Express V5.0.2 for iSeries: Collaboration Configuration

by Daniel Hill and Mike Gordon

IBM eServer Solutions Enablement

Updated July 2004

Table of Contents

Why is Collaboration Important to You?	1
Introductory Information	1
Configuration and Requirements.....	2
Step 1: Enabling Domino Servers for Collaboration.....	3
Enabling the DIIOP task	10
Step 2: Configuring Domino LDAP	10
Step 3: Configure Lotus Instant Messaging to use LDAP	15
Editing the Sametime.ini file	16
Step 4: Configure Lotus Team Workplace to use LDAP	18
Adding the QuickPlace servlet	20
Enabling Servlet Support on the Team Workplace server.....	21
Verify the QuickPlace servlet	21
Step 5: Customizing Lotus Team Workplace Log-in	22
Edit the Domino Configuration database (domcfg.nsf).....	22
Map the Team Workplace login form	23
Step 6: Configuring WebSphere Portal through the Wizard.....	24
Step 7: Verify Portal Configuration Properties for Domino (Optional)	27
Step 8: Configuring and Enabling Single Sign-On	31
Step 9: Configuring Portlets.....	40
Summary	53
Appendix	54
Trademarks	58

Why is Collaboration Important to You?

As today's workforce becomes more dispersed and virtual teams become the norm, businesses are looking for ways to quickly connect their workers for collaborative efforts. Most customers initially purchase Lotus® Domino® for the built-in enterprise e-mail, calendaring and scheduling applications, instant messaging, and web conferencing. The majority of customers are exploiting the "more than mail" capabilities that support core business processes. IBM® WebSphere® Portal provides an extensible framework for interacting with enterprise application, content, people, and processes. Self-service features allow end users to:

- Personalize and organize their own view of the portal
- Manage their own profiles
- Publish and share documents with their own view of the portal
- Manage their own profiles
- Publish and share documents with their colleagues.

(For additional information about each of these features, see the Lotus Web site at: www.lotus.com/brand.)

Collaboration consists of these components:

- Lotus Instant Messaging and Web Conferencing Server
- Lotus Team Workplace Server
- Lotus Mail and LDAP Server
- WebSphere Application Server
- WebSphere Portal
- Server Administration tool

This paper will teach the reader more about the collaboration components (listed above) and will help them understand the product's power to transform any work environment.

Introductory Information

Before we get started, there are a few things that need to be disclosed. The following release levels were used on an IBM eServer™ iSeries™ server in this paper: Lotus Domino Release 5.0.12, Lotus Instant Messaging and Web Conferencing (Lotus Sametime®) version 3.1, along with Lotus Team Workplace (Lotus QuickPlace®) version 3.0.1.

In addition, you can configure Lotus collaborative components to use the Domino Directory as the LDAP directory. We then configure our Portal Instance to use Domino as the LDAP directory and Lotus Instant Messaging and Team Workplace.

For Single Sign-On, LTPA tokens provide a means to share authentication information among Lotus, WebSphere, and Tivoli® application Web Servers. A user authenticated by an application server will be authenticated automatically on the other application servers in the same **DNS domain** providing the LTPA keys are shared by all applications.

Configuration and Requirements

Here are the configuration requirements to follow this article and integrate WebSphere Portal and Lotus collaborative technologies:

- Three Domino servers configured with users register with Domino Web Access files, all in the same DNS domain. All three servers need to have to following installed on them:
 - Mail/LDAP Server
 - Instant Messaging and Web Conferencing (Sametime)
 - Team Workplace Server (QuickPlace)
- **wpsadmin** person and the **wpsadmins** group registered within the Domino Directory.
- WebSphere Portal Express v5.0.2 installed and configured
- Sametime 3.1 installed
- QuickPlace 3.0.1 installed

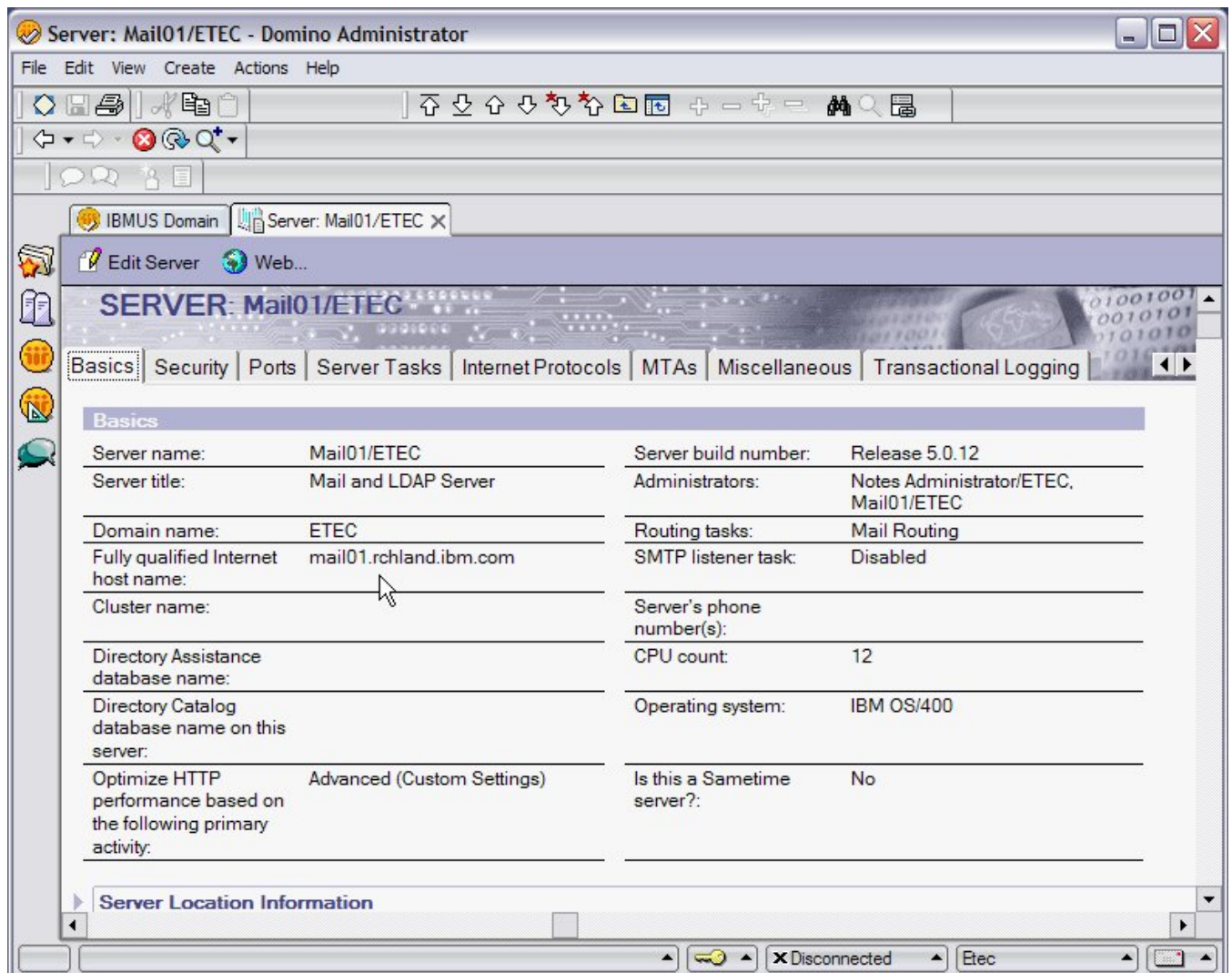
This paper will cover how to configure the Domino servers for collaboration using single sign-on and deploy portlets that use the Collaborative Component APIs. The following steps will be discussed:

- **Step 1:** Enabling Domino Servers for Collaboration
- **Step 2:** Configuring Domino LDAP
- **Step 3:** Configure Lotus Instant Messaging and Web Conferencing to use LDAP
- **Step 4:** Configure Lotus Team Workplace to use LDAP
- **Step 5:** Customizing Lotus Team Workplace Login
- **Step 6:** Configuring WebSphere Portal through the Wizard
- **Step 7:** Verify Portal Configuration Properties for Domino
- **Step 8:** Configuring and Enabling SSO
- **Step 9:** Configuring Portlets

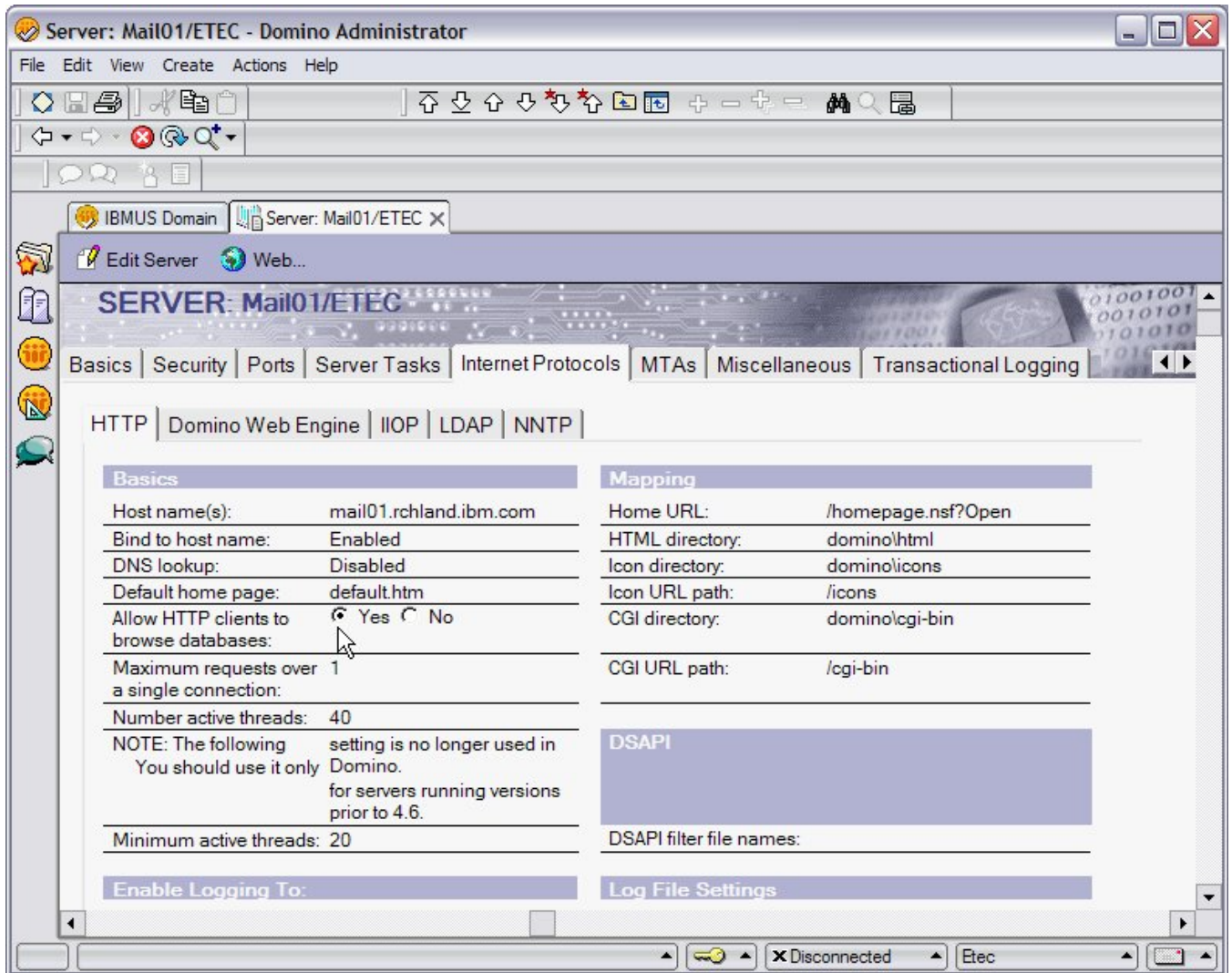
Step 1: Enabling Domino Servers for Collaboration

Edit the properties of each Domino server document to ensure proper configuration for SSO and portlets.

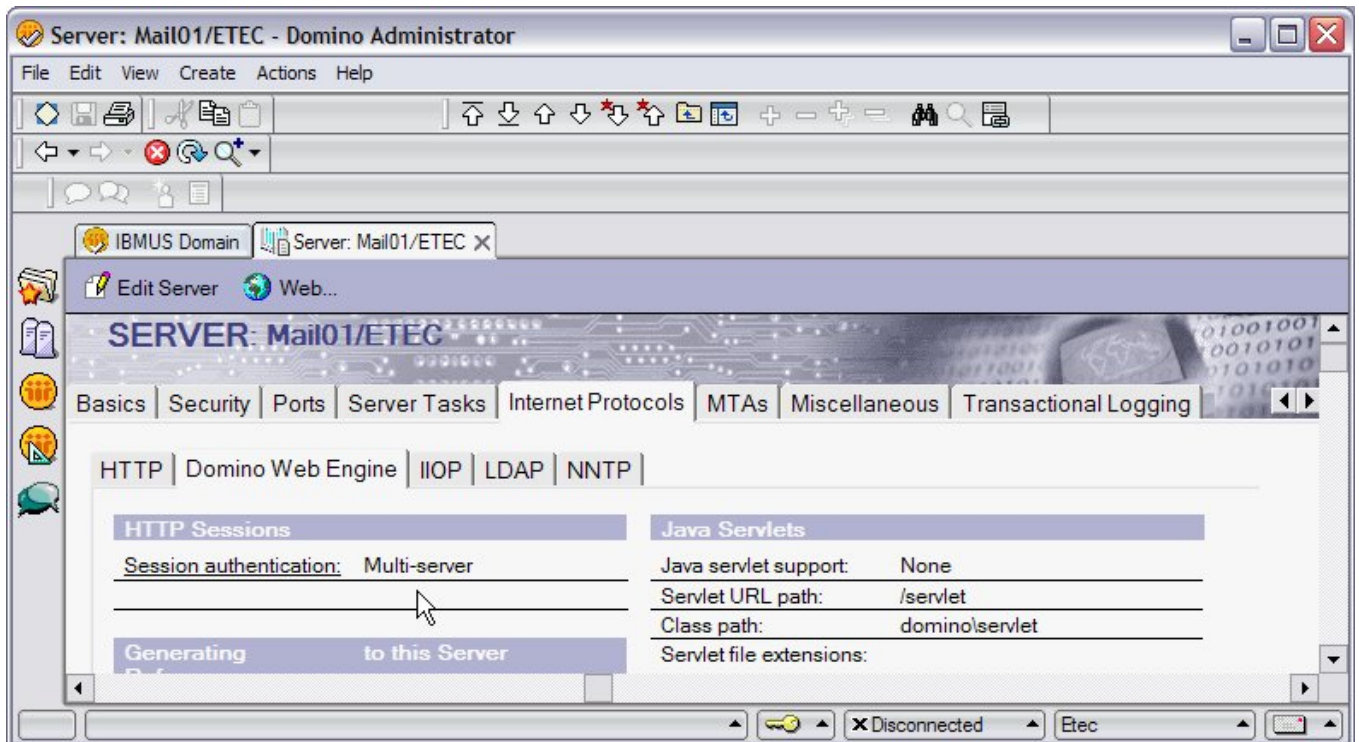
1. Open Domino Admin Client, click **File** → **Open Server** and type the name of the mail/LDAP server – [Mail01/ETEC](#)
2. Click the **Configuration** tab → **Server** → **All Server Documents**. Open the [Mail01/ETEC server](#)
3. Verify the **domain name** and **Fully qualified Internet Host Name** fields are correct, for example — ETEC is the domain name and [mail01.rchland.ibm.com](#) is the fully qualified Internet Host Name in this example.



- Click on the **Internet Protocols** and then the **HTTP** tab, set the Host Name(s) to the fully qualified host name of the server. Click **Enable** in the **Bind to Host Name** field and select **Yes** in the **Allow HTTP clients to browse databases** field.



5. Now select the Domino Web Engine tab (still under the Internet Protocols tab). Set the **Session Authentication** to **Multi-Server**.



6. Select the **Ports** and then the **Notes Network Ports** tab. Ensure a valid network port (TCPIP) and that the **Notes Network** field has a network specified. The servers "**Net Address**" should be the fully qualified host name.

The screenshot shows the Lotus Notes Server configuration window for 'Mail01/ETEC'. The 'Ports' tab is selected, and the 'Notes Network Ports' sub-tab is active. A table lists the configured ports, with the first row (TCPIP) being enabled and the others disabled.

Port	Protocol	Notes Network	Net Address	Enabled
TCPIP	TCP	NETWORK1	Mail01.rchland.ibm.com	ENABLED
			Mail01	DISABLED
			Mail01	DISABLED
			Mail01	DISABLED
			Mail01	DISABLED
			Mail01	DISABLED
			Mail01	DISABLED
			Mail01	DISABLED
			Mail01	DISABLED

- Now select the **Internet Ports** tab (still on the Ports tab) and ensure that the **TCPIP Port Status** is enabled and that the **Authentication Options** for the name and password is set to **Yes**.

1 Edit Server 2 Create Web (R5)... 3 Cancel

Accept SSL site certificates: Yes No

Accept expired SSL certificates: Yes No

Web | Directory | Mail | DIIOP | Remote Debug Manager

Web (HTTP/HTTPS)	
TCP/IP port number:	80
TCP/IP port status:	Enabled
Enforce server access settings:	No
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	443
SSL port status:	Disabled
Authentication options:	
Client certificate:	No
Name & password:	Yes
Anonymous:	Yes

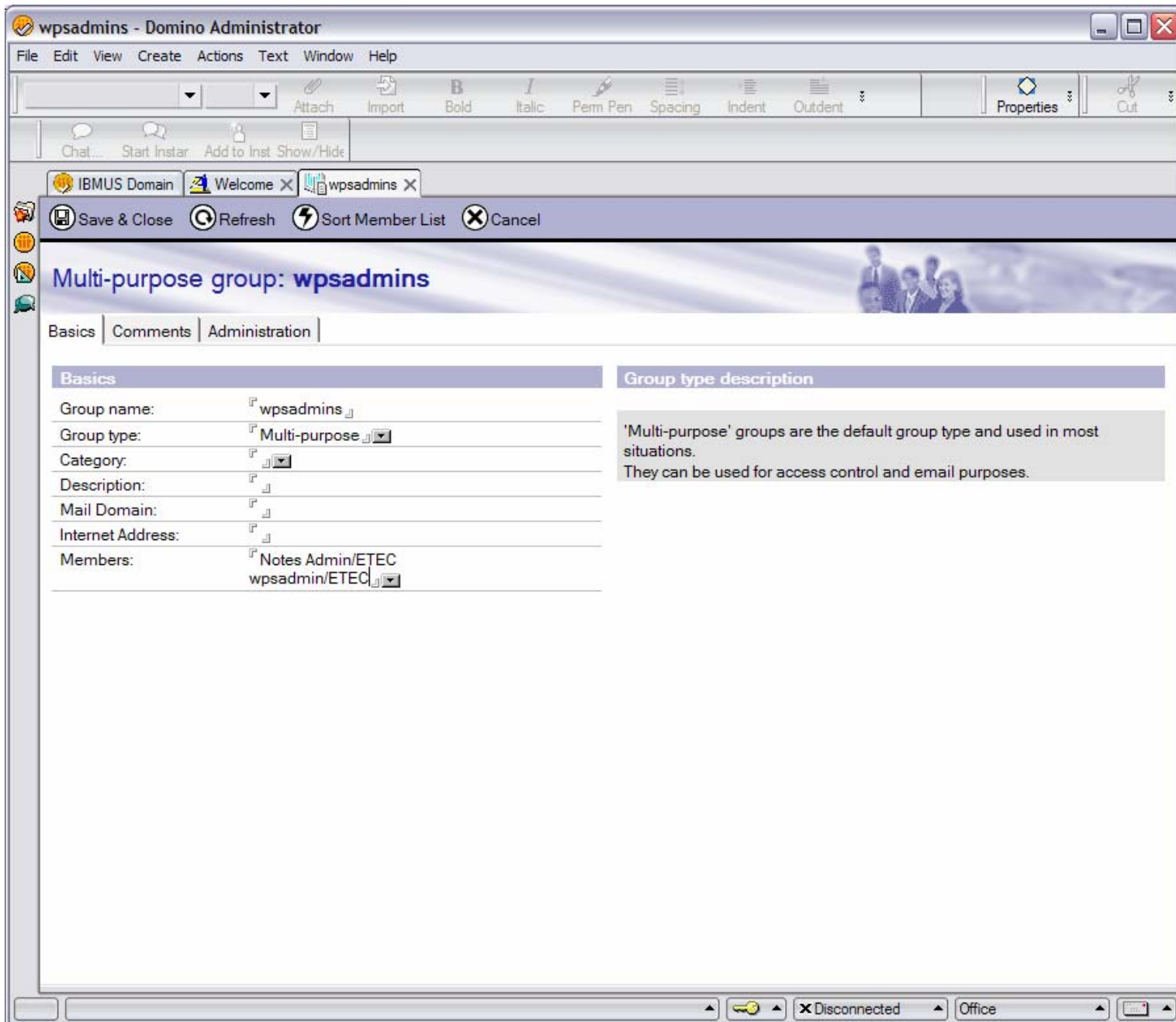
- Repeat Steps 1-7 for the Instant Messaging and Team Workplace servers through their respective server documents.

- Next, click the **People & Groups** tab, click on the **People** link. If the person **wpsadmin** does not exist, then create it using the **Add Person** button.

The screenshot displays the Domino Administrator window for the user **wpsadmin/ETEC**. The interface is divided into several sections:

- Menu and Toolbar:** Includes standard application menus (File, Edit, View, Create, Actions, Window, Help) and navigation tools like 'Prev Main', 'Next Main', 'Next', 'Previous', 'Next Unres', 'Prev Unres', 'Go Up', 'Go to View', 'Expand', 'Collapse', 'Expand All', and 'Collapse All'.
- Navigation:** A breadcrumb trail shows 'IBMUS Domain' > 'wpsadmin/ETEC'. Below it, 'Edit Person' and 'Cancel' buttons are visible.
- Person Information:** The main header identifies the user as 'Person: wpsadmin/ETEC' with the email address 'wpsadmin/ETEC@ETEC'.
- Configuration Tabs:** A row of tabs includes 'Basics', 'Work/Home', 'Other', 'Miscellaneous', 'Certificates', 'Roaming', and 'Administration'. The 'Basics' tab is currently selected.
- Basics Tab Fields:**
 - First name: (empty)
 - Middle name: (empty)
 - Last name: wpsadmin
 - User name: wpsadmin/ETEC, wpsadmin
 - Alternate name: (empty)
 - Short name/UserID: wpsadmin
 - Personal title: (empty)
 - Generational qualifier: (empty)
 - Internet password: (EAE198FC92F337E15652B5CE81652624)
 - Preferred language: (empty)
- Mail Tab Fields:**
 - Mail system: Notes
 - Domain: ETEC
 - Mail server: Mail01/ETEC
 - Mail file: mail/wpsadmin
 - Forwarding address: (empty)
 - Internet address: (empty)
 - Format preference for incoming mail: Keep in senders' format
 - When receiving unencrypted mail, encrypt before storing in your mailfile: No
- Real-Time Collaboration:** A section with a 'Sametime server:' field (empty).
- UserID:** A separate field at the bottom left containing the text 'UserID'.
- Status Bar:** Shows 'Disconnected' and 'Office' status indicators.

10. Click on the **Groups** link. If the group **wpsadmins** does not exist, create it using the **Add Group** button and add the person **wpsadmin** into the group.



In the Access Control List - Basics, ensure that the Portal administrators group **wpsadmins** has either **Author access** or **Editor access** for all available roles.

11. For the wpsadmins group, add and assign the following Role Types:
- GroupCreator
 - GroupModifier
 - UserCreator
 - UserModifier

12. Click **OK** to save the changes to the Access Control List of the Domino Directory.
13. Select EXIT in the Domino Administrator or Notes client.

Enabling the DIOP task

The Lotus Collaborative Components use the Java APIs to communicate with the Domino servers. These APIs use IIOp to connect to and communicate with the Domino servers, so you must enable the diiop task on the Domino LDAP, Instant Messaging, and Team Workplace servers.

Perform the following steps for each of the Domino you are using:

1. Stop the server
2. Once the Domino servers has stopped, edit the server configuration file (notes.ini) and
3. Add diiop to the ServerTasks line
4. Save and close the server configuration file
5. Restart the Domino server.

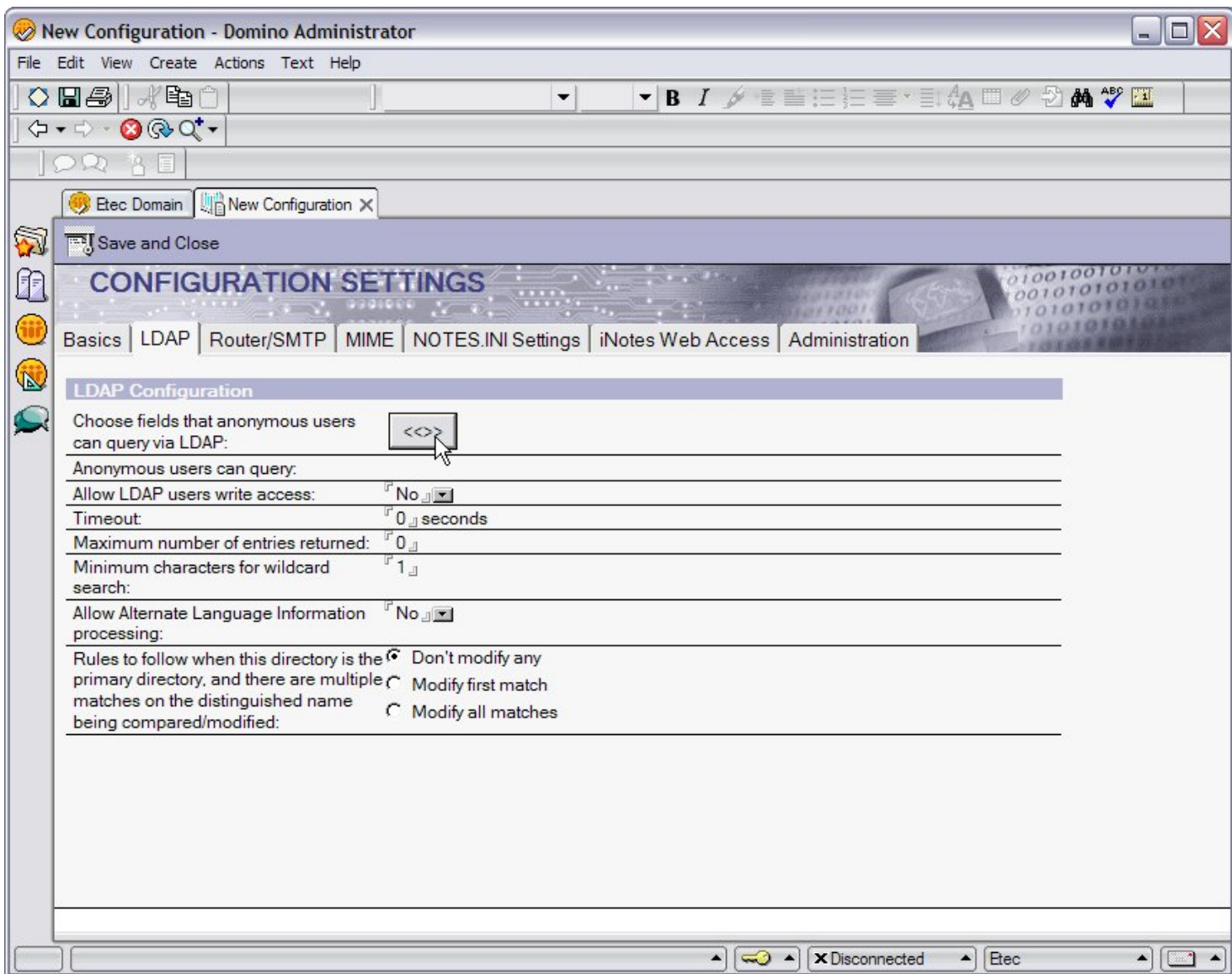
Step 2: Configuring Domino LDAP

The next step is to modify the Domino Mail server configuration so that you can access the same directory using the LDAP server protocol. NOTE: Use careful consideration when choosing a server to use as an LDAP server.

Consider a separate Domino server (a server that is not your Instant Messaging or Team Workplace server) for running LDAP. The Domino LDAP server must be active when running other Lotus Collaborative components.

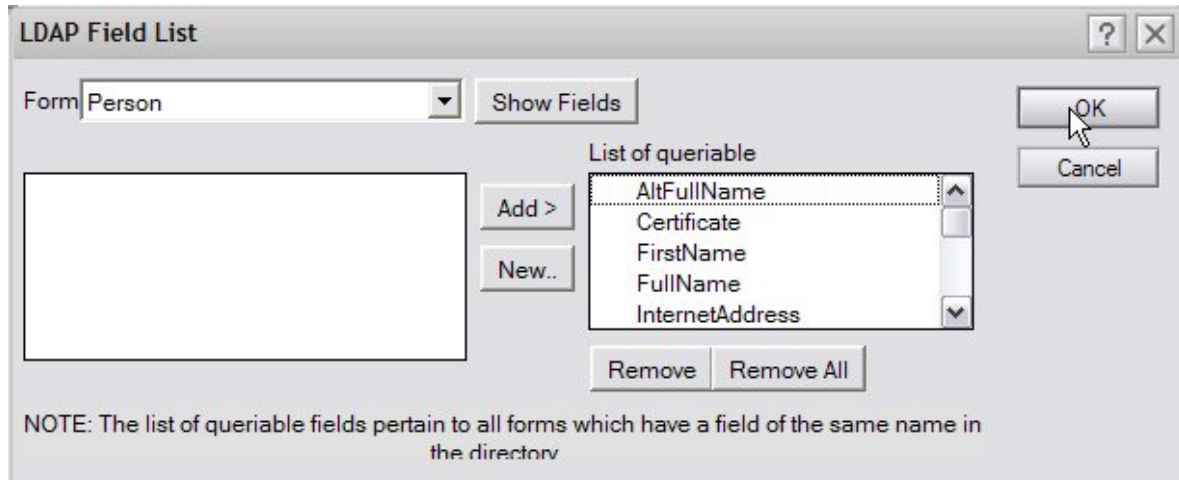
1. From the Domino Admin Client, click **File** —> **Open Server**. Type [Mail01/ETEC](#), choose the **Configuration** tab server and then click **Configurations**. Select the **Add Configuration** button
2. On the **Basics** tab, click the **Use these settings as the default setting for all servers**. This will display the LDAP tab.

3. Click the **LDAP** tab and then click the **Choose fields that anonymous users can query via LDAP** button.



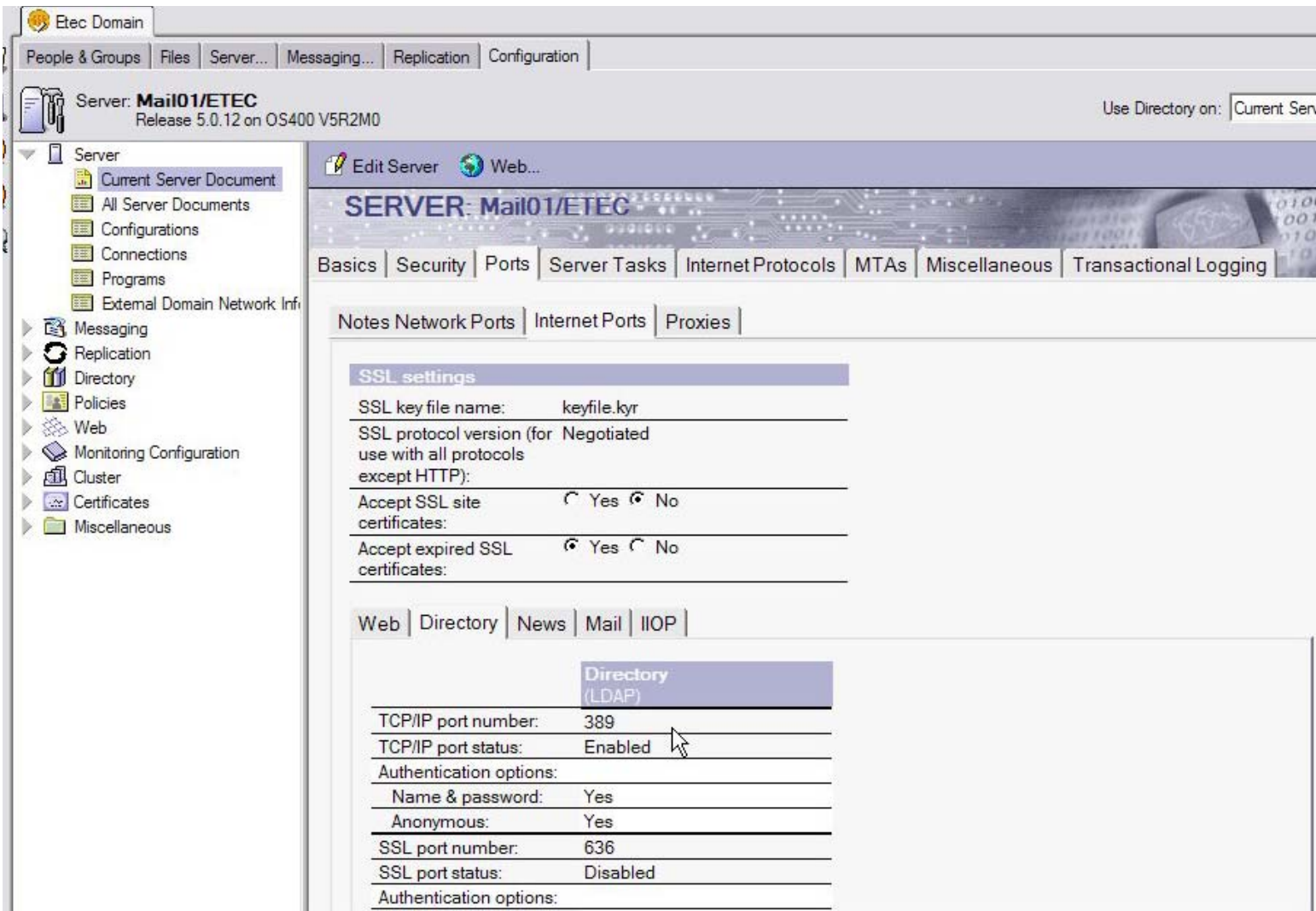
4. This displays the LDAP field list that can be queried. Click **OK** to have all fields be queried. Then click **Save and Close** the configuration document.
5. From the **Form** dropdown list, select **Person** and click **Show Fields**.

- From the **Fields in Form**, select the following fields to add them to the **Person** form:
 - MailFile
 - Mail Server
 - SametimeServer



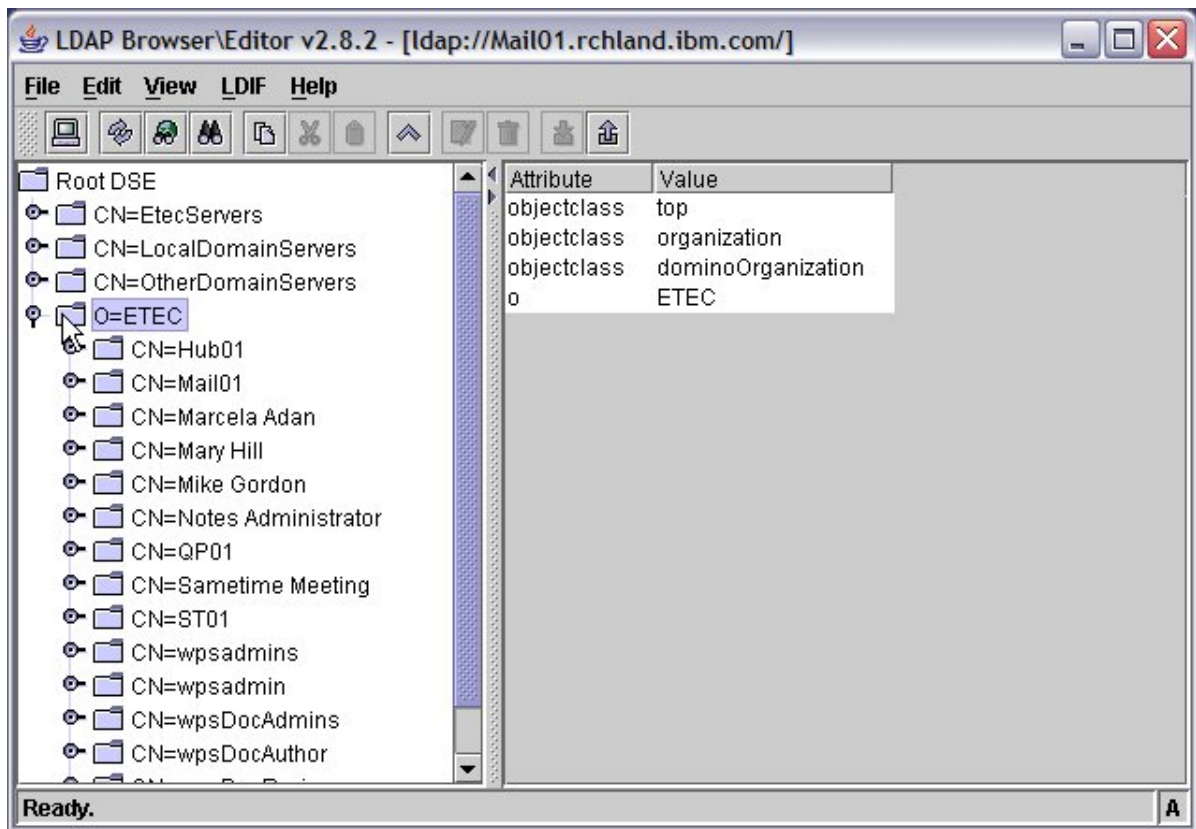
- From the **Form** drop-down list, select **Server\Server** and click **Show Fields**.
- From the **Fields in Form**, select the following fields to add them to the Server form:
 - HTTP_HostName
 - NetAddresses
- Click **OK** to close the LDAP Field List dialog box and return to the Configuration Settings document, the LDAP tab
- Ensure that the Anonymous users can query field displays the following attributes:
 - AltFullName
 - Certificate
 - FirstName
 - FullName
 - HTTP_HostName
 - InternetAddress
 - LastName
 - ListName
 - Location
 - MailAddress
 - MailDomain
 - MailFile
 - MailServer
 - Members
 - NetAddresses
 - PublicKey
 - SametimeServer
 - ShortName
 - userCertificate
- For the option, Allow LDAP users write access, click Yes. This setting ensures that Portal users can use the self care and self-registration features of WebSphere Portal.
- Keep all other default LDAP settings in configuration settings the same.

13. Click **Save and Close** to close the configuration settings.
14. Proceed to the **Current Server Configuration Document** view from the same section of the **Domino Admin Client, Configuration Tab-Server-Current Server Configuration** document.
15. On the server document, click **Ports** → **Internet Ports** → **Directory**. Ensure the LDAP Port is correct (usually 389) and the LDAP TCPIP Status is enable.



16. Edit the Notes.ini file to ensure that the LDAP server task is added and starts on server startup. From the Domino console, you can also issue a "load LDAP" to start the task.

17. (Optional) Utilize a free LDAP browser to view the schema for future WebSphere Portal configuration and test connection.



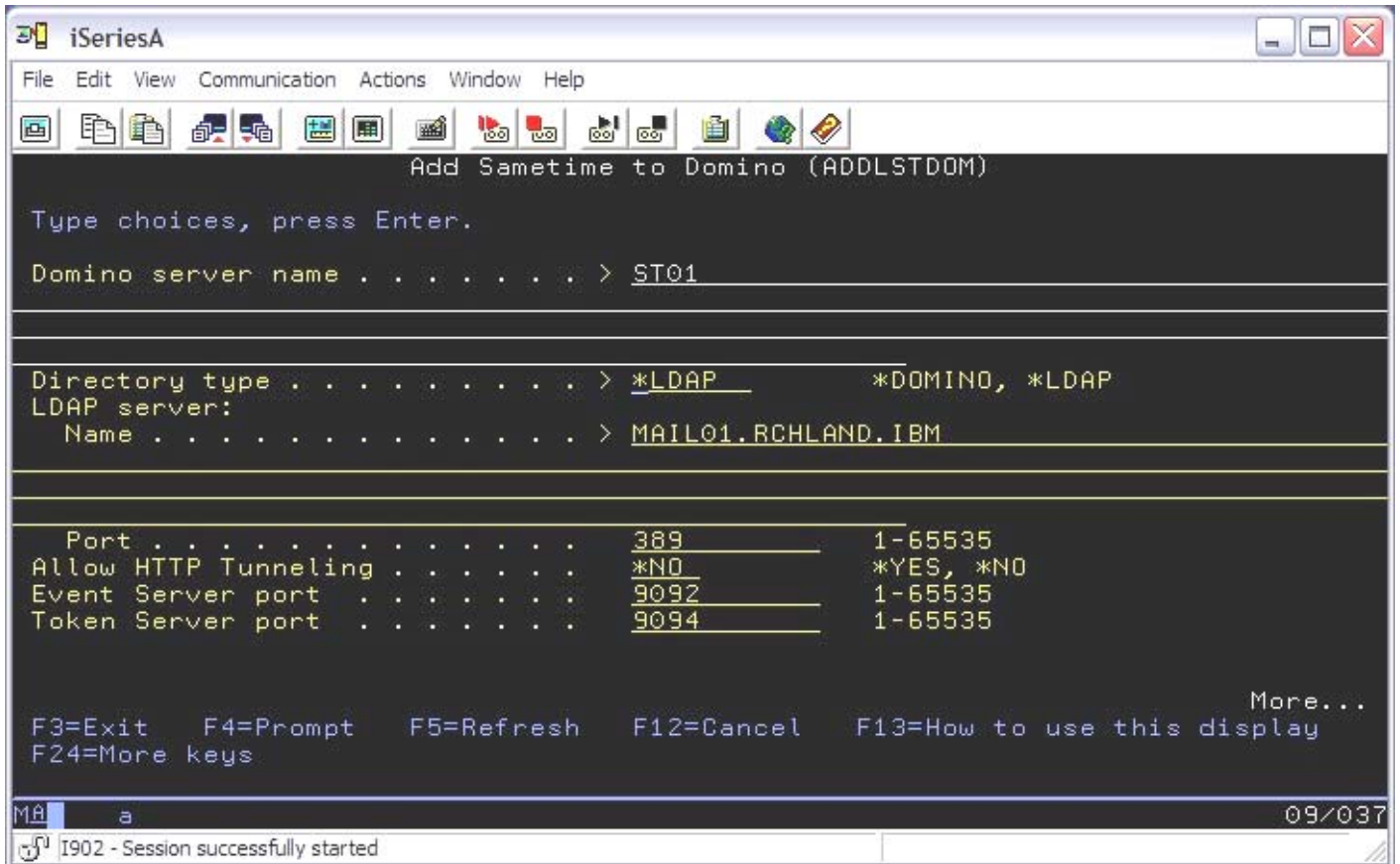
18. Replicate the Domino directory to the Instant Messaging and Team Workplace servers.

Step 3: Configure Lotus Instant Messaging to use LDAP

From the Personal Communications screen, sign in with your iSeries user profile:

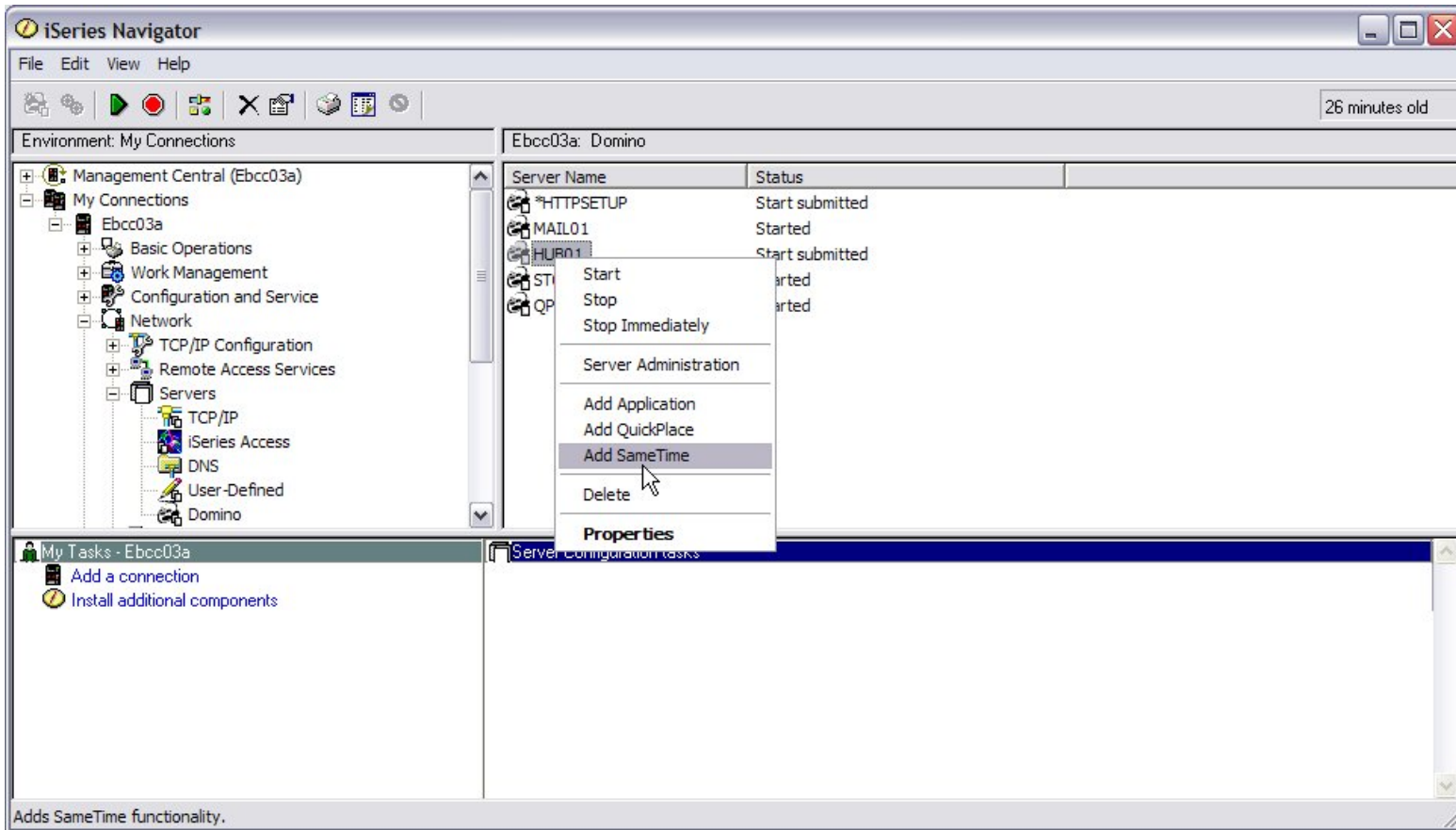
1. Issue the command **ADDLSTDOM** and then Prompt with **F4**

When prompted, enter the name of your Instant Messaging Server, Directory Type of ***LDAP**, and the name of the LDAP server which is the fully qualified Internet host name (mail01.rchland.ibm.com). Make sure to specify the correct port for LDAP, the default is 389.



```
iSeriesA
File Edit View Communication Actions Window Help
Add Sametime to Domino (ADDLSTDOM)
Type choices, press Enter.
Domino server name . . . . . > ST01
Directory type . . . . . > *LDAP      *DOMINO, *LDAP
LDAP server:
  Name . . . . . > MAIL01.RCHLAND.IBM
Port . . . . . 389      1-65535
Allow HTTP Tunneling . . . . . *NO      *YES, *NO
Event Server port . . . . . 9092      1-65535
Token Server port . . . . . 9094      1-65535
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display   More...
F24=More keys
MA a 09/037
I902 - Session successfully started
```

- (Optional Method) Using iSeries Navigator, Instant Messaging can be added to the configured Domino Server by selecting your iSeries server, signing in. Under **Network** → **Servers** → **Domino**, right-click on the server, and choose **Add Sametime**. Follow Step 1 for parameters.



Editing the Sametime.ini file

WebSphere Portal uses a Lotus Instant Messaging server application to enable connectivity for People Awareness. To allow this connectivity to work, you must set a security level by editing the Sametime.ini file.

Use a text editor to open the Sametime.ini file located in the Lotus Instant Messaging server data directory.

- Do one of the following to set a security level:

In a test or development environment, you can configure Lotus Instant Messaging to accept all IP addresses as trusted. To do this, add the following line to the Debug section:

```
[Debug]
VPS_BYPASS_TRUSTED_IPS=1
```

In a production environment, you can add the IP address of the portal server machine to the list of IP addresses of trusted servers. To do this, add the following line to the Configuration section:

```
[Config]
```

```
VPS_TRUSTED_IPS=trusted IP address1, trusted IP address2
```

For example

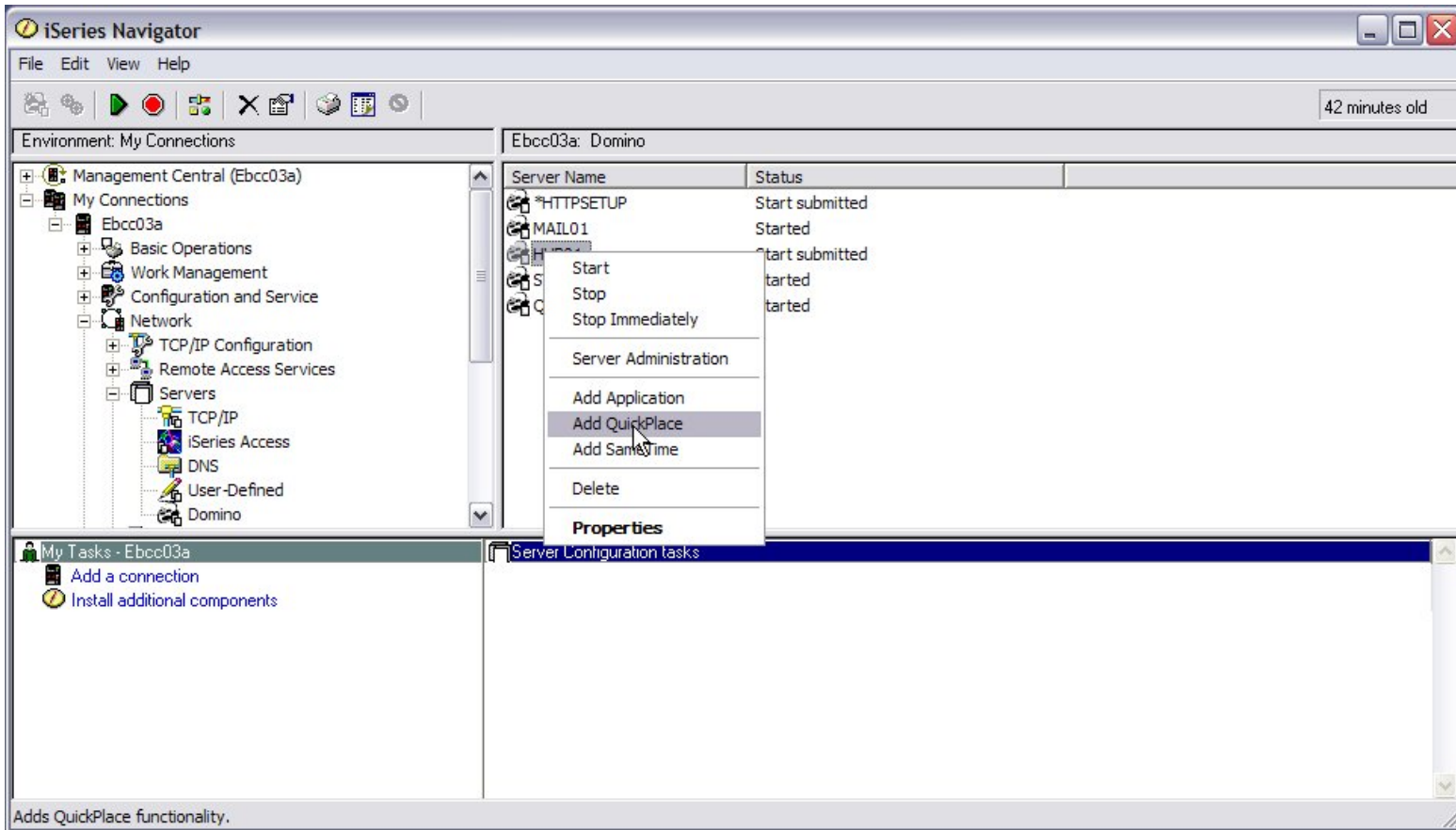
```
VPS_TRUSTED_IPS=168.0.0.1,168.0.0.2
```

2. Save and close the Sametime.ini file.
3. Restart the Lotus Instant Messaging server.

Step 4: Configure Lotus Team Workplace to use LDAP

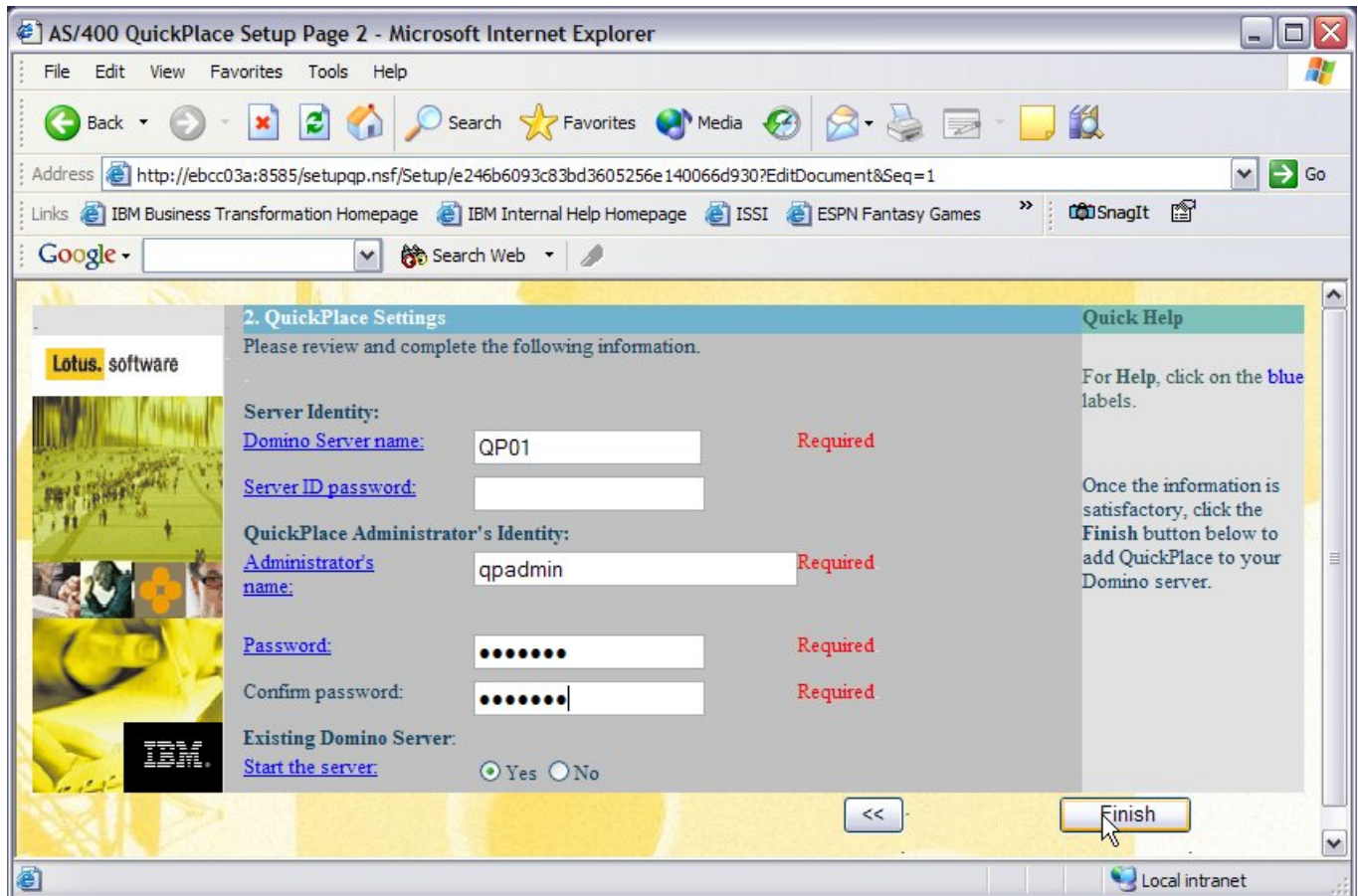
To configure Lotus Team Workplace to use LDAP, follow these steps:

1. Using iSeries Navigator, choose **Network** → **Servers** → **Domino**, right-click on the server that will be used as the Team Workplace server. Choose **Add QuickPlace** and sign-on to the iSeries server again.



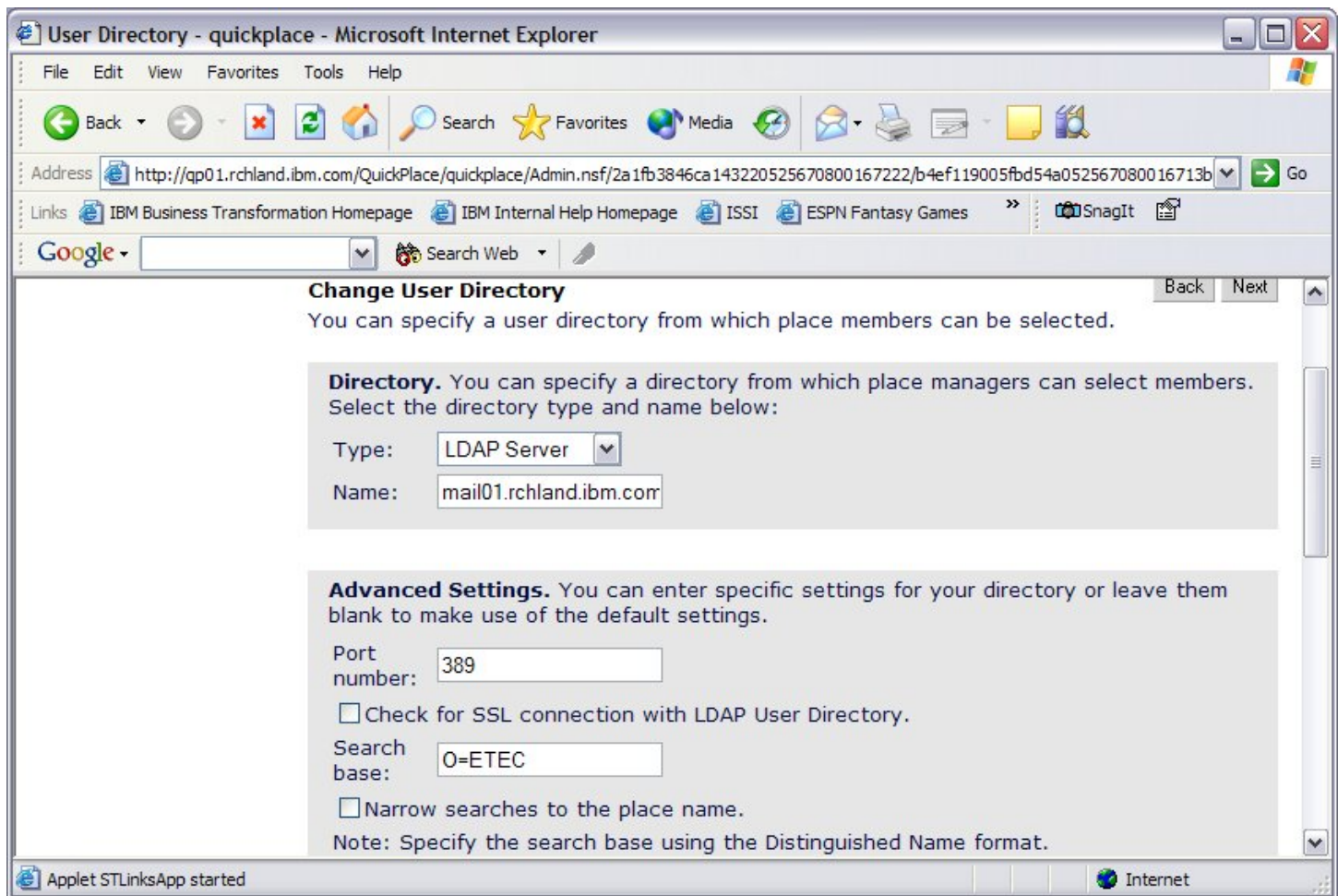
2. Enter the Domino Server name, for example, **QP01**.

3. Enter an Administrator username and password that is not a user within the Notes domain. This is strictly an administrator for this application, for example, **QPADMIN**
 - Confirm the password and click **Finish**. This will run the agent to configure the Team Workplace.



4. When successful completion is listed, click **Close**
5. Sign in to the Team Workplace administrative interface with the user ID created in step 3. In this example, we would go to <http://qp01.rchland.ibm.com/QuickPlace/> and log in as qpadmin
6. Select **Server Settings** → **User Directory, Change Directory** button. Select LDAP as the server type and enter the fully qualified host name of the directory server (mail01.rchland.ibm.com).

7. Under Advanced Settings, choose the LDAP Port and set **Search Base** to the Organizational Unit of the Notes domain; for example, **O=ETEC**. This is used for lookups. Click **Next**.



Adding the QuickPlace servlet

We need to configure the Team Workplace server to load the QuickPlace servlet on startup.

1. Stop the Team Workplace server.
2. Find the `servlets.properties` file in the Team Workplace server's data directory.
3. If the file does not exist, create it with a text editor.
4. Open the `servlets.properties` file in a text editor and add this line:
`servlet.QPServlet.code=com.lotus.cs.util.QPServlet`
5. Save and close the `servlets.properties` file.
6. Find the `cs.ear` file on the server in the directory:
`/qibm/ProdData/portalserver5/installableApps/cs.ear`
7. Extract the Collaborative Services Web archive file (`cs.war`) from the Collaborative Services Enterprise Application file (`cs.ear`).
8. Extract the Collaborative Services Java archive file (`cs.jar`) from `cs.war`.

9. Follow these steps to copy the cs.jar file to a directory on your iSeries server:
 - Enter the following on an OS/400 command line to create a new directory called WPS1.:
MKDIR '/WPS1'
 - Enter the following command to change the owner of the new directory to QNOTES:
CHGOWN OBJ('/WPS1') NEWOWN(QNOTES)
 - Copy cs.jar to the WPS1 directory.
 - Enter the following command:
CHGOWN OBJ('/WPS1/cs.jar') NEWOWN(QNOTES)
10. Edit the notes.ini file for the Team Workplace server making the following changes:
 - Add the following line:
WPS1=/WPS1/cs.jar
 - Append WPS1 to the JavaUserClassesExt line.
11. Verify that the following entries are listed in the notes.ini file; if they are not listed, then add:
 - NoWebFileSystemACLs=1
 - h_ScopeUrlInQP=1
12. Save and Close the notes.ini file.

Enabling Servlet Support on the Team Workplace server

Follow these steps to ensure that the Domino Servlet Manager is set for Java servlet support

1. Create a directory under *<serverdatadir>/Domino* called *Servlet*, if it does not already exist
2. Start Domino Administrator client.
3. Edit the Team Workplace server document on the Hub server:
4. Go to the **Internet Protocols** tab and click **Domino Web Engine**.
5. Set the Java Servlet Support to Domino Servlet Manager.
6. Save and close the document.
7. Start the Team Workplace server
8. Ensure that the changes to the server document are replicated to the Team Workplace server.

Verify the QuickPlace servlet

We can now verify that the QuickPlace servlet is working correctly.

1. Verify that the QuickPlace servlet is working by opening the following URL:
http://<domino_quickPlace_server>/servlet/QPServlet?actionType=69
where *domino_quickPlace_server* is the fully-qualified host name.

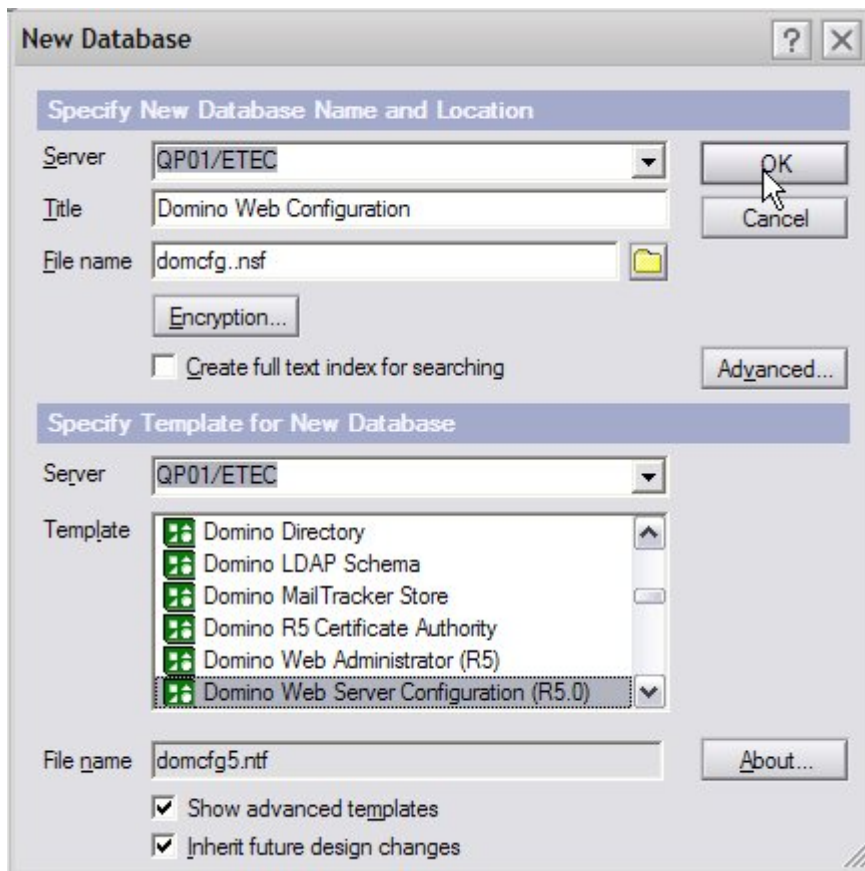
Step 5: Customizing Lotus Team Workplace Log-in

The Lotus Team Workplace server needs to be enabled to make single sign-on work because the login form contains JavaScript.

Edit the Domino Configuration database (domcfg.nsf)

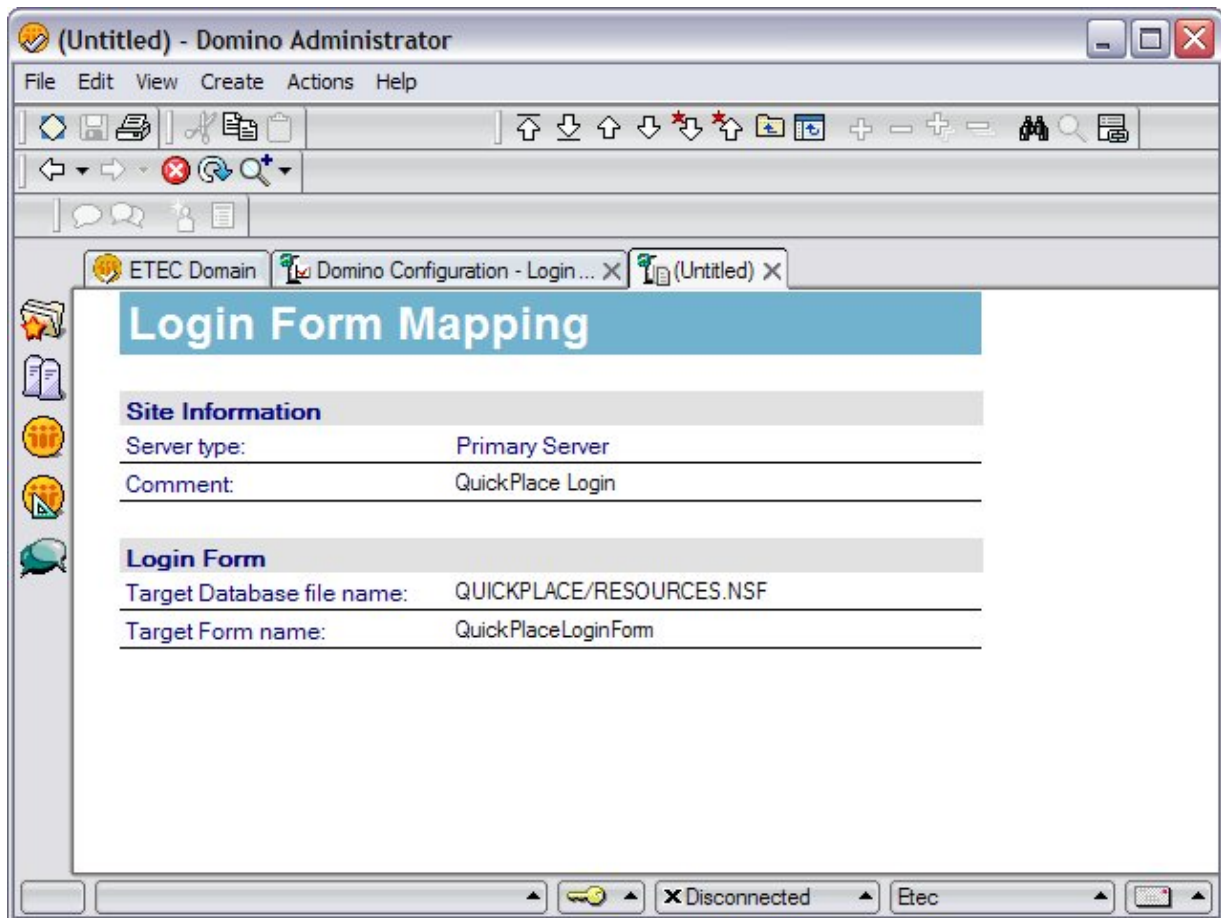
If the Domcfg.nsf does not exist, follow these steps:

1. Start the Domino Server and login to the Domino Administrator.
2. Select File → Database New.
Type the name of the Team Workplace server in the Server field. For the Filename, type **domcfg.nsf**. Make sure that the file name is typed exactly as shown.
3. Click the template Server button and select your server and show advanced templates checkbox.
4. Select the Domino Web Server Configuration (R5.0) template and then click **OK**.
(domcfg.ntf)



Map the Team Workplace login form

1. Open the domcfg.nsf database. (Select **File** → **Database** → **Open** or **Cntrl-O**)
2. Click **Create** → **Mapping Login Form**
3. Type **quickplace/resources.nsf** in the Target Database file name field
4. Type **QuickPlaceLoginForm** for the Target form name field.
5. Click **File** → **Save** to close the form



Step 6: Configuring WebSphere Portal through the Wizard

Note: If you want to configure Domino as the LDAP server of an existing Portal instance, see the appendix of this course.

Next, create the WebSphere Portal instance and add Lotus Collaboration Options while configuring the WebSphere Portal instance to use the Domino LDAP server. The wpconfig.properties file will be updated with corresponding information entered for the Domino servers.

Follow these steps for the configuration of a WebSphere Portal Instance:

IMPORTANT: Make sure the wpsadmin person and the wpsadmins group are registered within the Domino Directory.

1. Through an emulator session, start the HTTPADMIN server using the command:
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
2. Through a browser, sign into the Admin server with your user ID and password:
<http://iSeries.domain.com:2001/HTTPAdmin>
3. Select **Create WebSphere Portal** and follow the Summary Configuration listed below for the entire configuration of a WebSphere Portal Instance.

Property	Value
Application server Name=	wps1team
Server Description=	Portal Server instance
HTTP Server Name=	wps1team
HTTP Server Description=	HTTP server for Portal wps1team
IP Addresses=	10.10.10.1
Port=	20180
First Port in Range	20100
Collection, Schema, or Library name	<iSeries DB2 Schema Name> e.g. PortalDB1
UserName	<iSeries UseraName> e.g. wpsdbuser
Password	password
Default URL path http://bvilla.rchland.ibm.com:10000/ wps/portal	wps
Default home path http://bvilla.rchland.ibm.com:10000/wps/ portal	portal
Personalized path: http://bvilla.rchland.ibm.com:10000/ wps/myportal	myportal
LDAP server host name:	Mail01.rchland.ibm.com
LDAP port:	389
LDAP administrator DN:	cn=Notes Admin
LDAP administrator password:	password
Information describing user entries Parent DN:	o=ETEC
Information describing the administrative group entry Parent DN:	*ROOT
Portal administrative group and administrator information: Administrative group name: wpsadmins Administrator name: wpsadmin Password: Confirm Password:	wpsadmin wpsadmin

Deploy Portlets	Administrative portlets Themes and Skins Business portlets Lotus Collaborative portlets
Choose the collaborative components to configure: Lotus Sametime Hostname: Port:	ST01.rchland.ibm.com 1533
Lotus QuickPlace Hostname: Port	QP01.rchland.ibm.com 80
Lotus Domino Directory	

4. Click finish to create the Portal instance.

Step 7: Verify Portal Configuration Properties for Domino (Optional)

NOTE: If you used the Portal Configuration wizard, this configuration will have been completed for you.

If you are adding the Collaboration functionality to an existing Portal instance or the configuration wizard failed to run correctly, you must run the following steps to enable the Collaborative Components.

- Lotus QuickPlace Properties
 - Lotus Sametime Properties
 - Lotus Domino Directory
 - LDAP Properties
 - WebSphere Portal Security
1. From Windows Explorer, locate the wpconfig.properties file in the **/QBIM/Userdata/Webas5/Base/<portalinstance>/PortalServer5/config** directory on the mapped drive on the iSeries server. Make a backup copy of this file before changing any values.
 2. Use a Text Editor (Microsoft Word) to open the wpconfig.properties file and make sure of the values below for QuickPlace in your organization.
 - # Description: Lotus Collaborative Components required properties
 - # to enable Lotus QuickPlace
 - # LCC.QuickPlace.Enabled: Is Lotus QuickPlace enabled in the environment?
 - # { true | false }
 - LCC.QuickPlace.Enabled=true
 -
 - # LCC.QuickPlace.Server: The Lotus QuickPlace server name.
 - # { hostname | ip address }
 - LCC.QuickPlace.Server=qp01.rchland.ibm.com
 -
 - # LCC.QuickPlace.Protocol: The protocol used to connect to the Lotus QuickPlace server.
 - # { http | https }
 - LCC.QuickPlace.Protocol=http
 -
 - # LCC.QuickPlace.Port: The port number for the Lotus QuickPlace server.
 - # { port number }
 - LCC.QuickPlace.Port=80

3. Ensure the values for Sametime in your organization.

- # Description: Lotus Collaborative Components required properties
- # to enable Lotus Sametime
- # LCC.Sametime.Enabled: Is Lotus Sametime enabled in the environment?
- # { true | false }
- LCC.Sametime.Enabled=true
- # LCC.Sametime.Server: The Lotus Sametime server name.
- # { hostname | ip address }
- LCC.Sametime.Server=st01.rchland.ibm.com
- # LCC.Sametime.Protocol: The protocol used to connect to the Lotus Sametime server.
- # { http | https }
- LCC.Sametime.Protocol=http
- # LCC.Sametime.Port: The port number for the Lotus Sametime server.
- # { port number }
- LCC.Sametime.Port=1533

4. Ensure the values for the Domino Directory (used for Server Lookups for mail files).

- # Description: Lotus Collaborative Components required properties
- # to enable Lotus Domino Directory
- # LCC.DominoDirectory.Enabled: Is Lotus Domino Directory enabled in the environment?
- # { true | false }
- LCC.DominoDirectory.Enabled=true
- # LCC.DominoDirectory.Server: The Lotus Domino Directory server name.
- # { hostname | ip address }
- LCC.DominoDirectory.Server=mail01.rchland.ibm.com
- # LCC.DominoDirectory.Port: The port number for the Lotus Domino Directory server.
- # { port number }
- LCC.DominoDirectory.Port=389
- # LCC.DominoDirectory.SSL: Is SSL used to connect to the Lotus Domino Directory Server?
- # { true | false }
- LCC.DominoDirectory.SSL=false

5. Update values for WebSphere Portal Security and a desired password (these are the LTPA settings).

- # WebSphere Portal Security LTPA and SSO configuration
- #####
- # LTPAPassword: Specifies the password to encrypt and decrypt the LTPA keys.
- LTPAPassword=wpsadmin
- # LTPATimeout: Specifies the time period in minutes at which an LTPA token will expire.
- LTPATimeout=120
- # SSOEnabled: Specifies that the Single Sign-on function is enabled.
- SSOEnabled=true
- # SSORequiresSSL: Specifies that Single Sign-On function is enabled
- # only when requests are over HTTPS Secure Socket Layer (SSL) connections.
- SSORequiresSSL=false
- # SSODomainName: Specifies the domain name (.ibm.com, for example) for all Single Sign-on hosts.
- SSODomainName=rchland.ibm.com

6. Ensure the values and desired passwords for the LDAP Properties Section for your organization.

- # LookAside: To configure LDAP with an additional LookAside Database
- # true - LDAP + Lookaside database
- # false - only LDAP
- LookAside=false
- # LDAPHostName: The LDAP server hostname
- LDAPHostName=mail01.rchland.ibm.com
- # LDAPPport: The LDAP server port number
- # For example, 389 for non-SSL or 636 for SSL
- LDAPPport=389
- # LDAPAdminUIId: The LDAP administrator ID
- LDAPAdminUIId=cn=administrator
- # LDAPAdminPwd: The LDAP administrator password
- LDAPAdminPwd=password
- # LDAPServerType: The type of LDAP server to be used for WebSphere Portal
- # IBM Directory Server: { IBM_DIRECTORY_SERVER }
- # Domino: { DOMINO502 }
- # Active Directory: { ACTIVE_DIRECTORY }

- # SunOne: { IPLANET }
- # Novell eDirectory: { NDS }
- # Note: use IPLANET for SunONE
- LDAPServerType=DOMINO502
- #LDAPBindID: The user ID for LDAP Bind authentication
- # See LDAP examples below:
- # IBM Directory Server: { uid=wpsbind,cn=users,dc=yourco,dc=com }
- # Domino: { cn=wpsbind,o=yourco.com }
- # Active Directory: { cn=wpsbind,cn=users,dc=yourco,dc=com }
- # SunOne: { uid=wpsbind,ou=people,o=yourco.com }
- # Novell eDirectory { uid=wpsbind,ou=people,o=yourco.com }
- LDAPBindID=CN=wpsadmin,O=ETEC
- #LDAPBindPassword: The password for LDAP Bind authentication
- LDAPBindPassword=wpsadmin

7. Stop the WebSphere Portal Instance using the command line or the GUI:

- **Strqsh – cd /QIBM /ProdData/Webas5/Base/bin**
- **stopServer –instance wps1 –username wpsadmin –password wpsadmin**

8. Through an emulator session, at the command line, type **run STRQSH**

9. Change to the directory to:

```
cd /QIBM/Userdata/Webas5/Base/<wps_instance>/PortalServer5/config
```

10. Type the following command to run the appropriate configuration task:

```
WPSconfig.sh lcc-configure-dominodirectory
```

11. Check the output for any error messages. If you encounter an error, check the appropriate logs file for more information.

Note: The preceding task, lcc-configure-dominodirectory, is specific for configuring Lotus Collaborative Components to use a Domino Directory only. It is possible to change and save other Lotus Collaborative Components values in wpsconfig.properties, and then run the configuration task WPSconfig.sh lcc-configure-all to configure multiple components.

12. Type the following command to run the appropriate configuration task:

```
WPSconfig.sh lcc-configure-quickplace
```

13. Check the output for any error messages.

14. Type the following command to run the appropriate configuration task:

```
WPSconfig.sh lcc-configure-sametime
```

15. Check the output for any error messages.

Step 8: Configuring and Enabling Single Sign-On

LTPA keys need to be shared across all Web servers for Domino and WebSphere. This is accomplished through WebSphere Application Server Administration and Domino Admin Client.

1. Start the WebSphere Administration Console through a browser:
http://<servername>:admin Port/>admin. Login using the user ID “wpsadmin” and the password “wpsadmin”.
2. Select Security → Authentication Mechanism → LTPA

WebSphere Administrative Console - Microsoft Internet Explorer

Address: <https://portal3.rchland.ibm.com:20211/admin/secure/securelogin.do?action=secure>

WebSphere Application Server Administrative Console Version 5

User ID: wpsadmin

PORTAL3_wps2

- Servers
- Applications
- Resources
- Security
 - Global Security
 - SSL
 - Authentication Mechanisms
 - LTPA**
 - User Registries
 - JAAS Configuration
 - Authentication Protocol
- Environment
- System Administration
- Troubleshooting

WebSphere Application Server on IBM.com

The place for support; including WebSphere Flashes, FAQs, Hints and Tips, and Technotes. You will also find Downloads, Library, News, and other useful information.

About your WebSphere Application Server

IBM WebSphere Application Server, 5.0.2
Build Number: ptf2M0325.01
Build Date: 06/23/2003

IBM WebSphere Application Server Enterprise, 5.0.2

WebSphere Developer Domain

Get the latest technical articles, best practices, tutorials and much more in the [WebSphere Application Server Zone](#). Influence the evolution of WebSphere Application Server and [request new product features](#).

InfoCenter

The complete source for product documentation, including tasks, reference, and conceptual information on product features and functions.

WebSphere Status January 13, 2004 5:05:06 PM UTC

WebSphere Configuration Problems

Total Configuration Problems :0	0 total	0 total	0 total
---------------------------------	---------	---------	---------

Preferences

<https://portal3.rchland.ibm.com:20211/admin/navigatorCmd.do?forwardName=LTPA.config.view>

3. Type and confirm the password (wpsadmin). Then click **Generate Keys**. **DO NOT CLICK THE APPLY OR OK BUTTONS!**

The screenshot displays the WebSphere Administrative Console interface in Microsoft Internet Explorer. The main content area is titled "LTPA" (Lightweight Third Party Authentication) and contains a "Configuration" section. Within this section, there are three buttons: "Generate Keys", "Import Keys", and "Export Keys". The "Generate Keys" button is currently selected, with a mouse cursor hovering over it. Below the buttons is a table of configuration properties:

General Properties		
Password	*	The password to encrypt and decrypt the LTPA keys. This password should be used when importing these keys into other WebSphere Application Server administrative domain configurations (if any) and when configuring SSO for Domino Server. If the password is changed and OK or Apply is pressed, a new set of keys are automatically generated. This new set of keys will be used after saved.
Confirm Password	*	Confirm the password to encrypt and decrypt the LTPA keys.
Timeout	* 120	The time period in minutes at which an LTPA token will expire. This time period should be longer than cache timeout configured in the Global Security panel.
Key File Name		The name of the file used when importing or exporting keys. Enter file name and then click either Import Keys or Export Keys. The imported keys will be used after saved.

Below the table are buttons for "Apply", "OK", "Reset", and "Cancel". Underneath is an "Additional Properties" section with two entries:

- Trust Association**: Enable Trust Association. Trust Association is used to connect reversed proxies to Websphere.
- Single Signon (SSO)**: Specifies the configuration values for single sign-on.

At the bottom of the console, the "WebSphere Status" bar shows the date and time as "January 14, 2004 5:49:07 PM UTC". Below this, the "WebSphere Configuration Problems" section indicates "Total Configuration Problems : 1" with a red error icon and "1 total". There are also indicators for warnings (0 total) and information (0 total).

4. Click the **Save** button to saving to the master configuration once the screen refreshes.

The screenshot displays the WebSphere Administrative Console in a Microsoft Internet Explorer browser window. The browser title is "WebSphere Administrative Console - Microsoft Internet Explorer". The console interface includes a navigation bar with "Home", "Save", "Preferences", "Logout", and "Help" buttons. On the left, a navigation tree shows the user ID "wpsadmin" and various configuration categories like "Servers", "Applications", "Resources", "Security", "Authentication Mechanisms", "LTPA", "User Registries", "JAAS Configuration", "Authentication Protocol", "Environment", "System Administration", and "Troubleshooting". The "LTPA" section is selected, showing "Lightweight Third Party Authentication configuration settings". A message box at the top states: "Changes have been made to your local configuration. Click **Save** to apply changes to the master configuration. The server may need to be restarted for these changes to take effect." Below this, the "Configuration" section has three buttons: "Generate Keys", "Import Keys", and "Export Keys". The "General Properties" section features a "Password" field with a masked input (dots) and a help icon. The help text explains that the password is used to encrypt and decrypt LTPA keys and should be used when importing keys into other WebSphere configurations. At the bottom, the "WebSphere Status" section shows the date and time "January 14, 2004 5:56:48 PM UTC" and a "WebSphere Runtime Messages" table with a "Clear All" button. The table shows: "Total All Messages:493", "1 new, 1 total" (with a red error icon), "25 new, 25 total" (with a yellow warning icon), and "467 new, 467 total" (with a green info icon). The browser address bar shows the URL "https://tcebiz1.rchland.ibm.com:20111/admin/syncworkspace.do?syncaction=list".

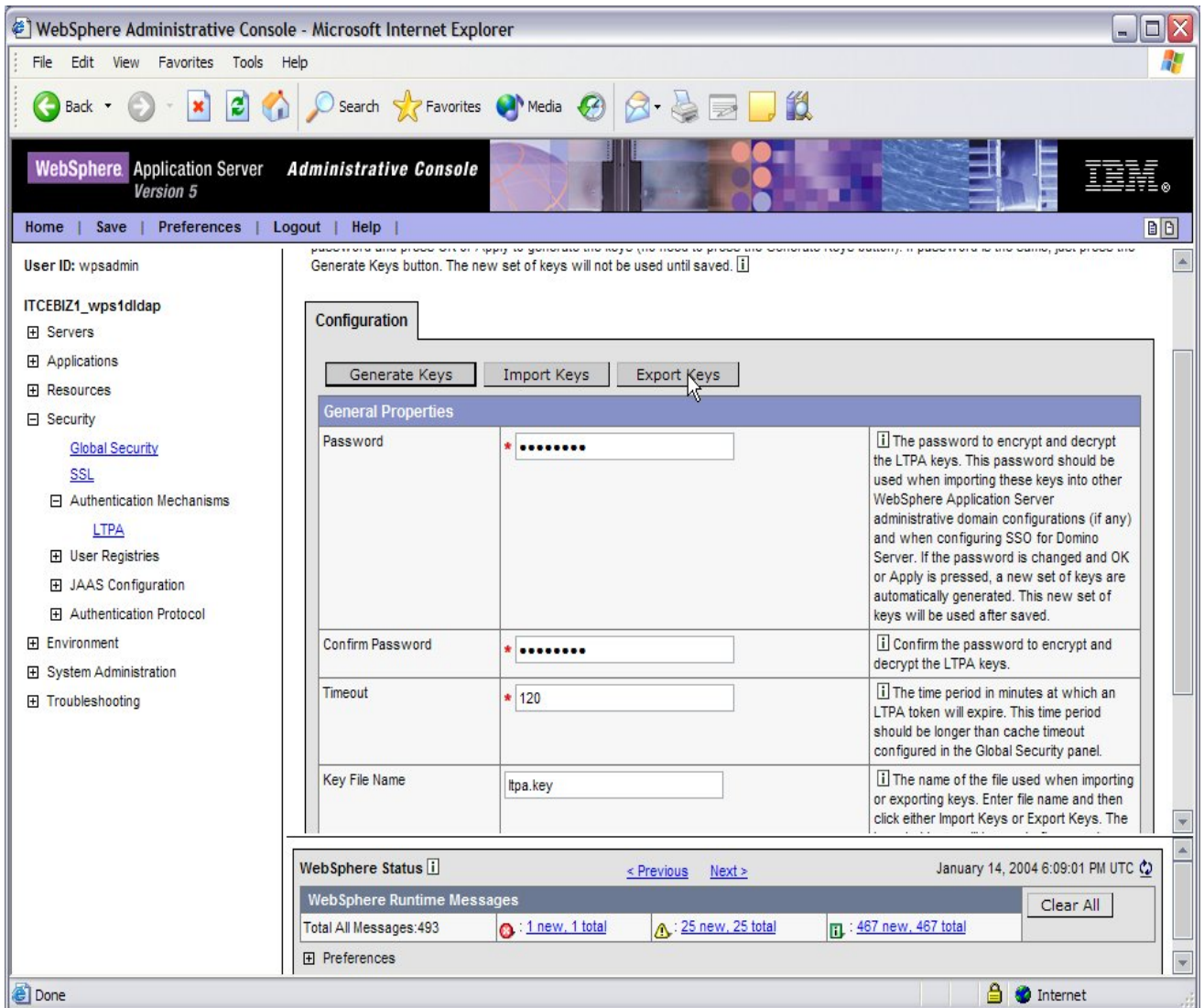
5. When the screen refreshes, click **Save** to finish saving the changes.

The screenshot displays the WebSphere Administrative Console interface within a Microsoft Internet Explorer browser window. The browser's address bar shows the URL for the console. The page header includes the WebSphere logo and the text 'Application Server Administrative Console Version 5'. A navigation bar contains links for 'Home', 'Save', 'Preferences', 'Logout', and 'Help'. On the left side, a tree view shows the navigation structure, with 'LTPA' selected under 'Authentication Mechanisms'. The main content area features a 'Message(s)' box with a warning icon and text: 'Changes have been made to your local configuration. Click Save to apply changes to the master configuration. The server may need to be restarted for these changes to take effect.' Below this is a link for 'LTPA >' and a large 'Save' button. The 'Save' button is highlighted, and a mouse cursor is positioned over it. Below the 'Save' button are 'Discard' and 'Cancel' buttons. At the bottom of the page, a 'WebSphere Status' section shows the date and time as 'January 14, 2004 5:56:48 PM UTC'. Below this is a 'WebSphere Runtime Messages' table with a 'Clear All' button. The table contains the following data:

WebSphere Runtime Messages			
Total All Messages:493	: 1 new, 1 total	: 25 new, 25 total	: 467 new, 467 total

The status bar at the bottom of the browser shows 'Done' on the left and 'Internet' on the right.

- Go back into Authentication Mechanisms folder and select LTPA , In the **Key File Name**, enter a name for the file (ltpa.key) and choose **Export Keys**.



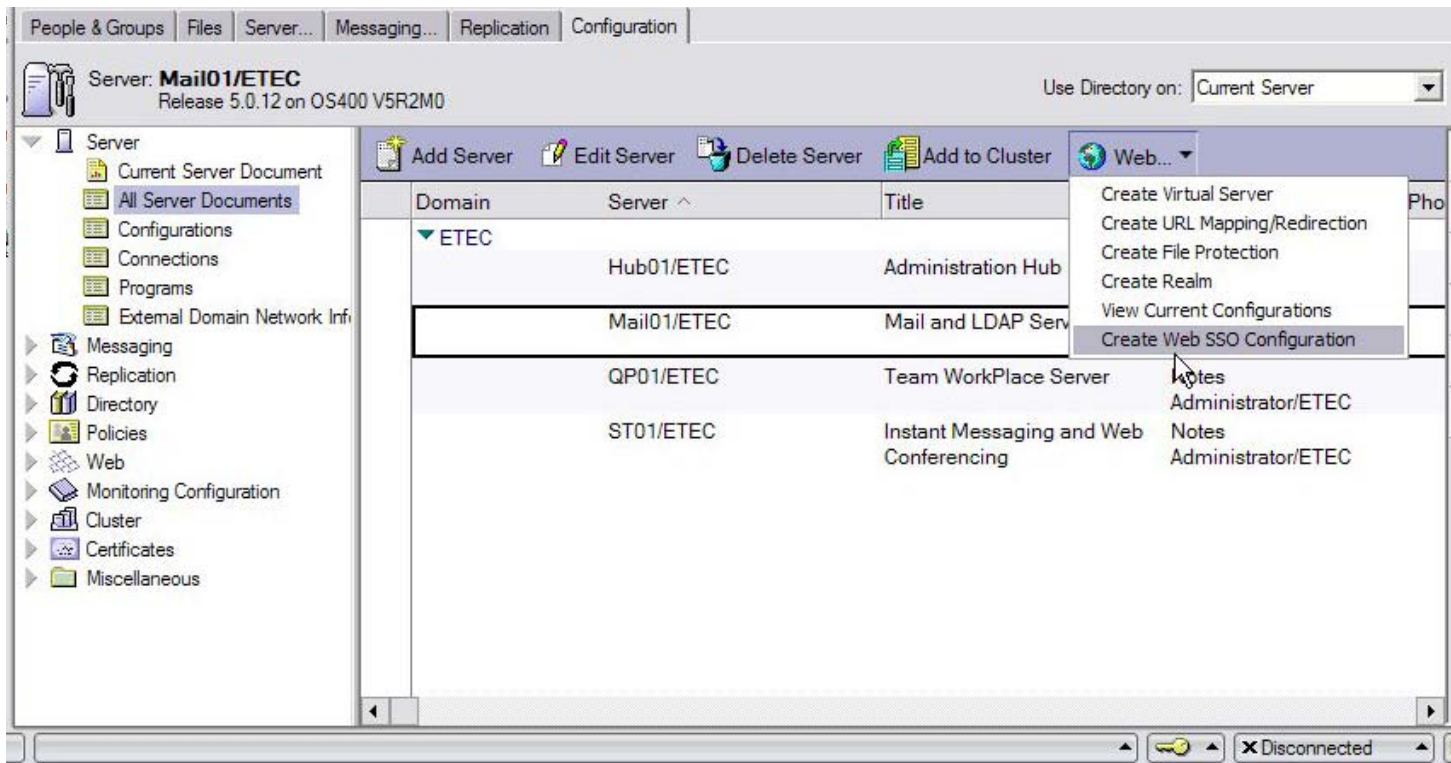
- Click **Save** and then **Save** again for the Master Configuration. This is similar to steps 4 and 5.
- Stop the WebSphere Portal Instance using the command line or the GUI:
 - Strqsh – cd /QIBM /ProdData/Webas5/Base/bin**
 - stopServer –instance wps1 –username wpsadmin –password wpsadmin**

9. From a DOS prompt, FTP the **LTPA.key** file to your local PC for importing the keys to Domino.
 - **Cd /QIBM/UserData/WebAS5/Base/<Instance Name>**
 - **Get ltpa.key**

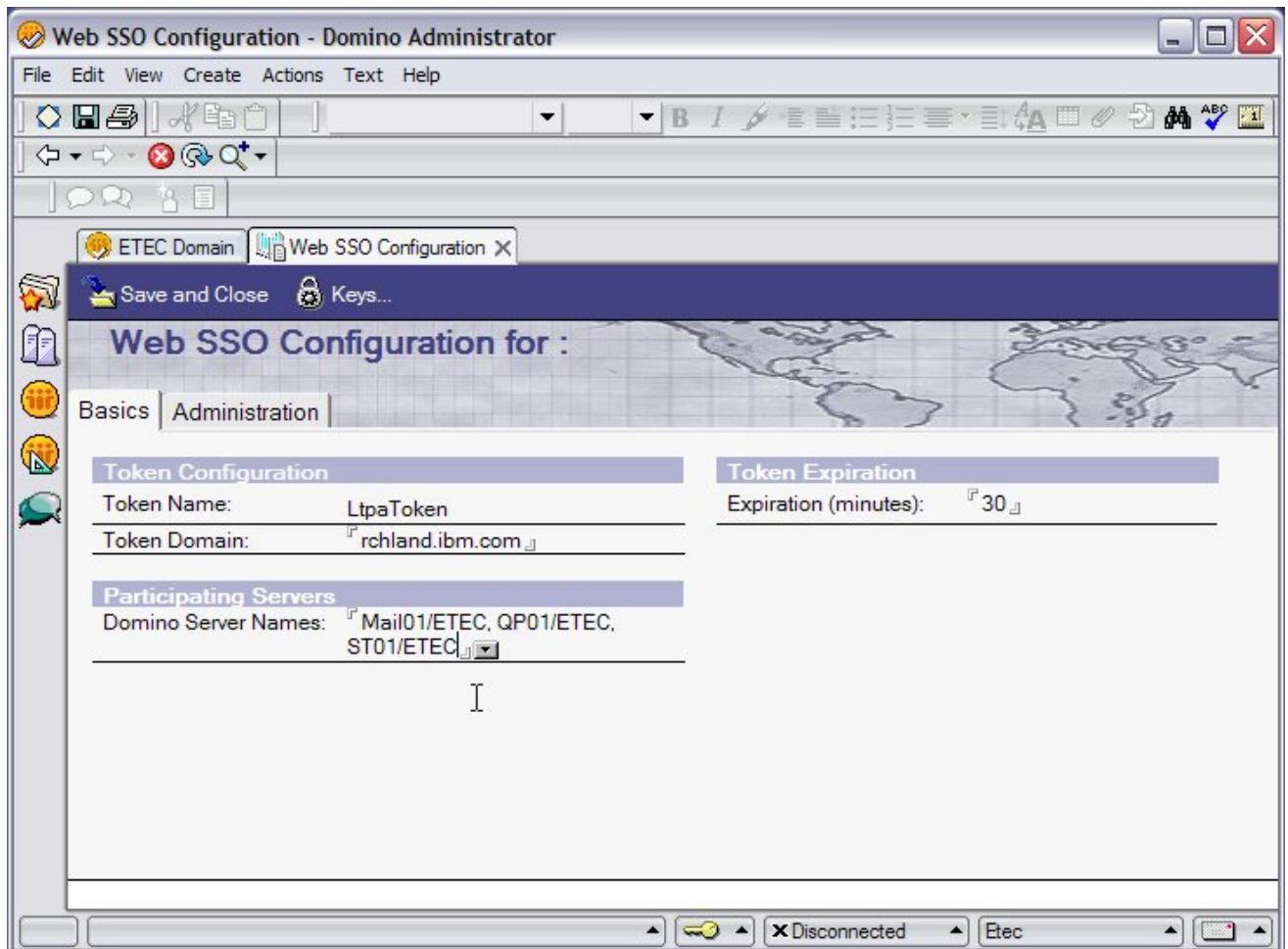
```

C:\> Command Prom... - ftp itcebiz1
220-QTCP at ITCEBIZ1.
220 Connection will close if idle more than 5 minutes.
User <itcebiz1.rchland.ibm.com:<none>>: mgordo
331 Enter password.
Password:
230 MGORDO logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> cd /QIBM/Userdata/WebAS5/Base/wps1ddap
250-NAMEFMT set to 1.
250 "/QIBM/Userdata/WebAS5/Base/wps1ddap" is current directory.
ftp> get ltpa.key
200 PORT subcommand request successful.
150 Retrieving file /QIBM/Userdata/WebAS5/Base/wps1ddap/ltpa.key
250 File transfer completed successfully.
ftp: 970 bytes received in 0.03Seconds 32.33Kbytes/sec.
ftp>
  
```

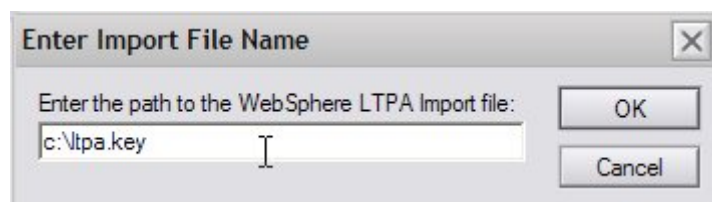
10. If a Web SSO document does not exist under **Web -> InterNet Sites**, you must create one and import the WebSphere LTPA keys. From the Domino Admin Client, open the Mail or LDAP server. Click **Configuration -> Server -> All Server Documents**. On the **Web** button, choose **Create Web SSO Configuration**.



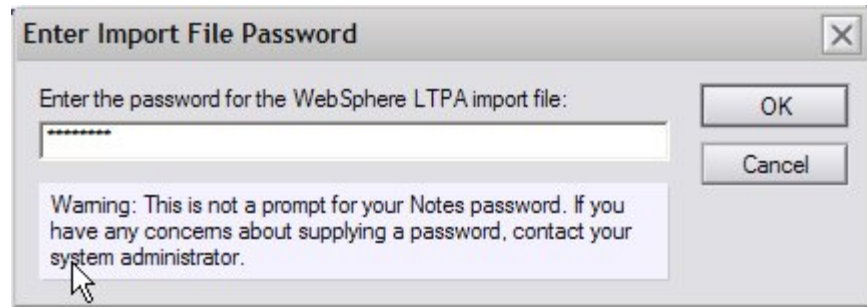
11. In the Web SSO document, enter the Token domain (domain.ibm.com). **Note: it will automatically add a dot (.) at the beginning of the parameter.** Add the Participating servers which will be the Mail, Instant Messaging, and Team Workplace servers.



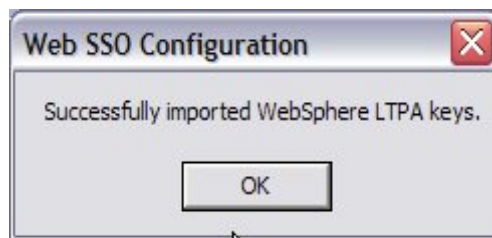
12. Click the **Keys** button and **Import WebSphere LTPA keys**. Enter the path on your local PC to the ltpa.key file (c:\ltpa.key) then click OK.



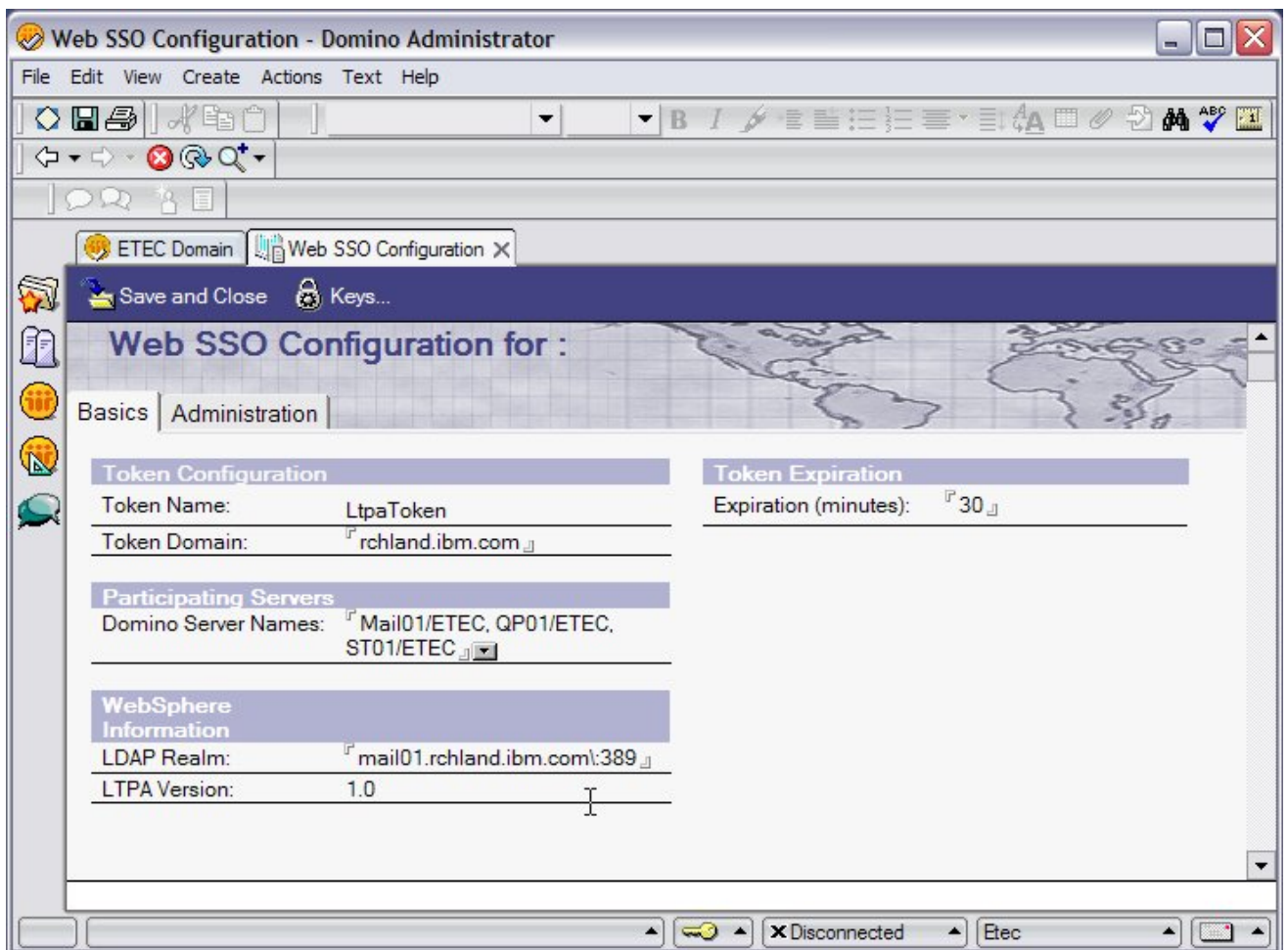
13. Enter the password to the Key file (wpsadmin) and click OK.



14. A successful import Window will appear; click OK.



15. Once this is imported successfully, the **WebSphere Information** section will appear. A modification needs to be made to the **LDAP Realm** — it requires a “\” so that it reads **yourhostname\389**.

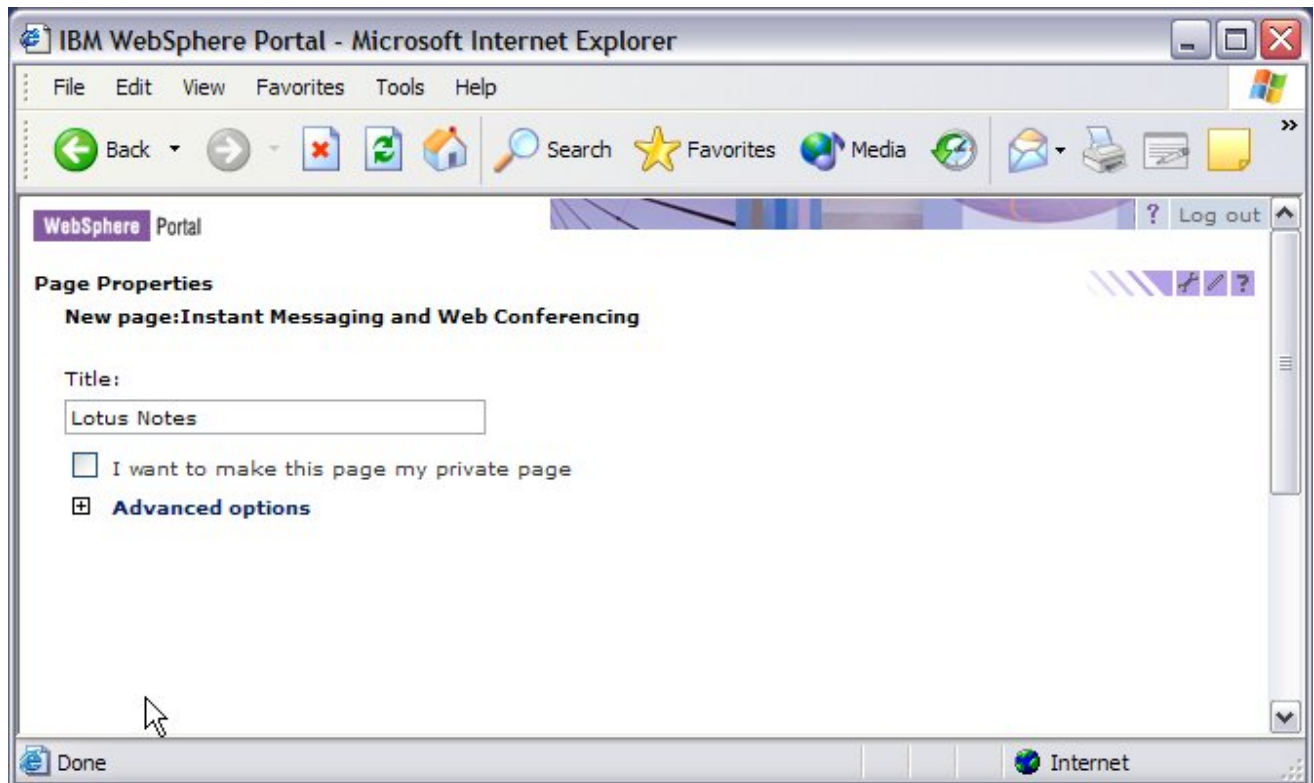


16. Save and close the Web SSO document and replicate the Domino Directory to the Instant Messaging and Team Workplace servers so they can also use the LTPA Token.
17. Restart HTTP for all Domino servers and start the WebSphere Portal Server
- From the console, type **Tell HTTP Restart –**
 - A message will appear that says: **Successfully loaded Web SSO Configuration.**
 - From QSH, issue the command, **StartServer –instance InstanceName**

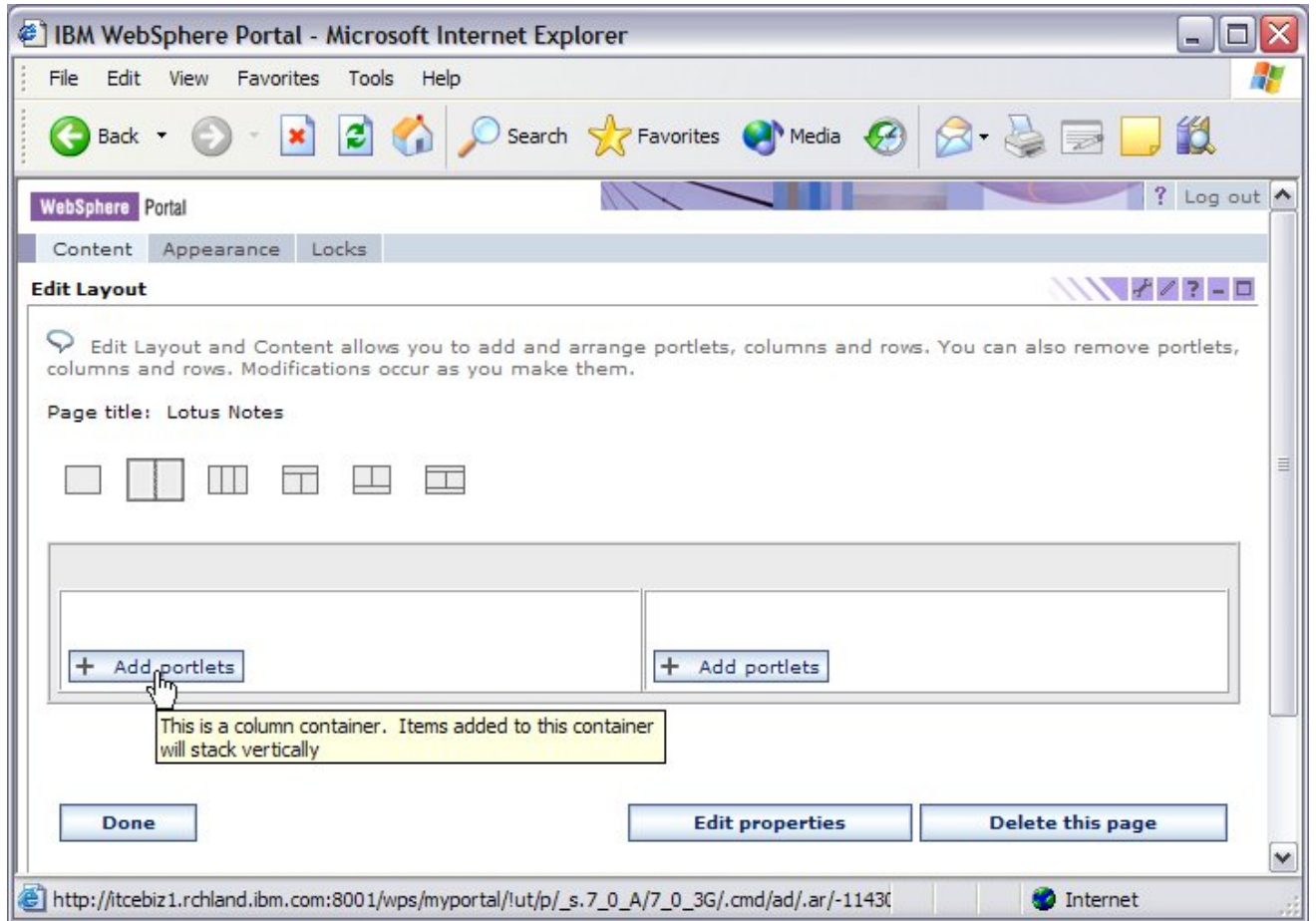
Step 9: Configuring Portlets

Now we are ready to deploy the Base Domino Portlets. This section will explain how to deploy Domino Web Access, Sametime, and QuickPlace portlets.

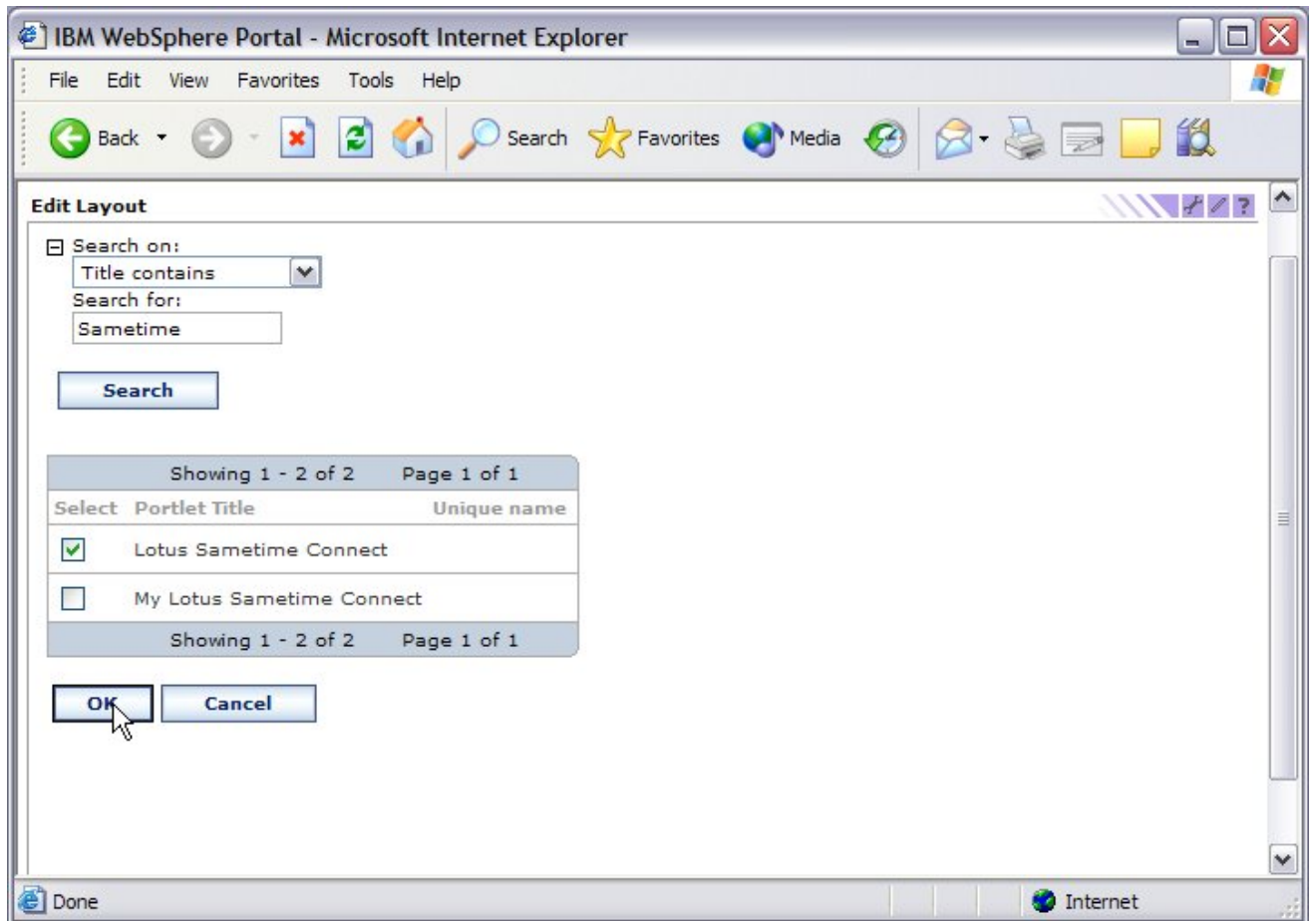
1. Open a browser and navigate to your Portal instance URL:
http://<system name>:<portal server port>/wps/portal
2. Sign in as **wpsadmin** and click **New Page**.
3. Type a title name for the page and click **OK**.



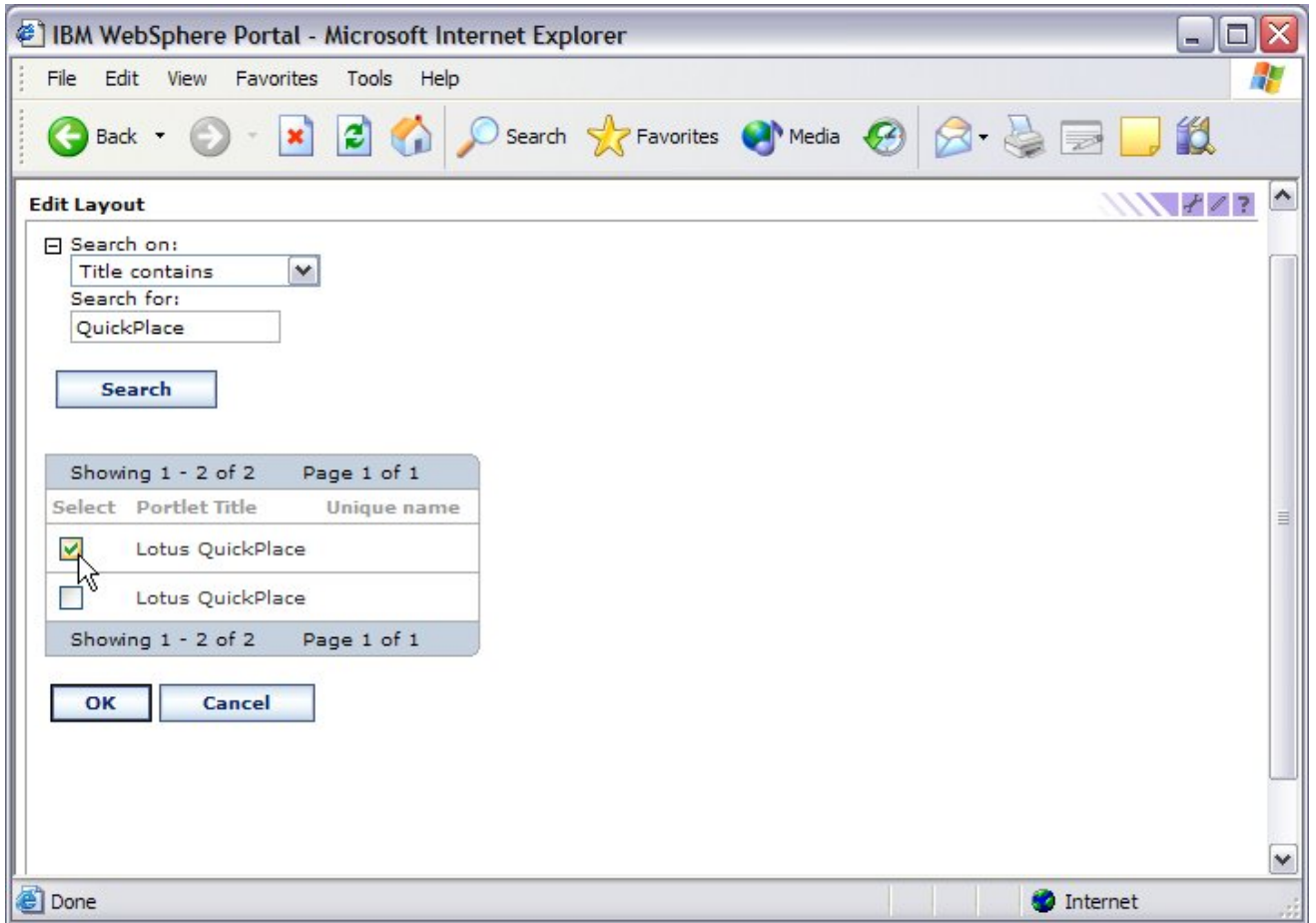
4. Choose **Add Portlets** to add a specific Domino Portlet.



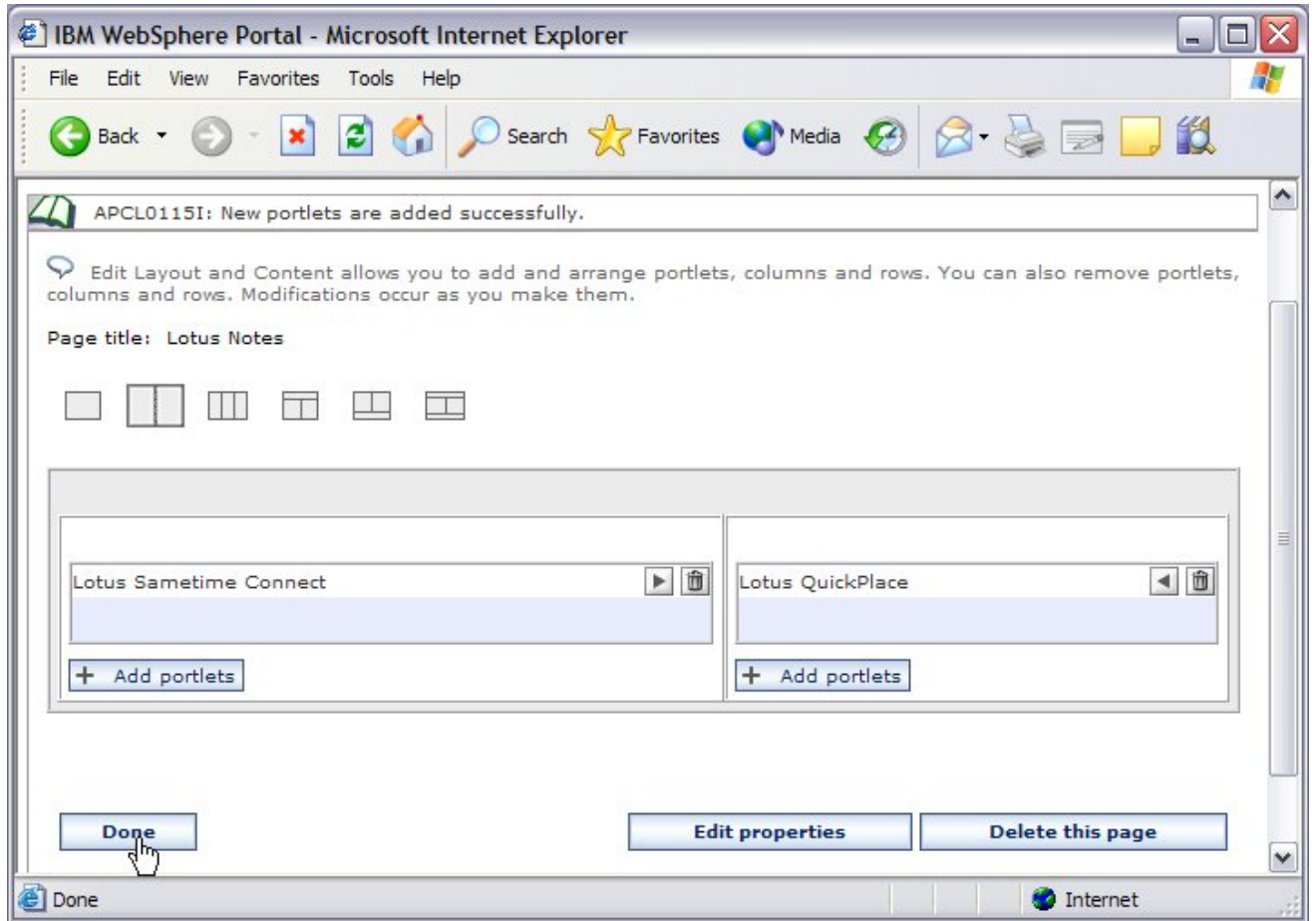
5. Search for the Sametime Portlet and select the box of the Portlet that you are looking for (Lotus Sametime Connect in this example). Click **OK**.



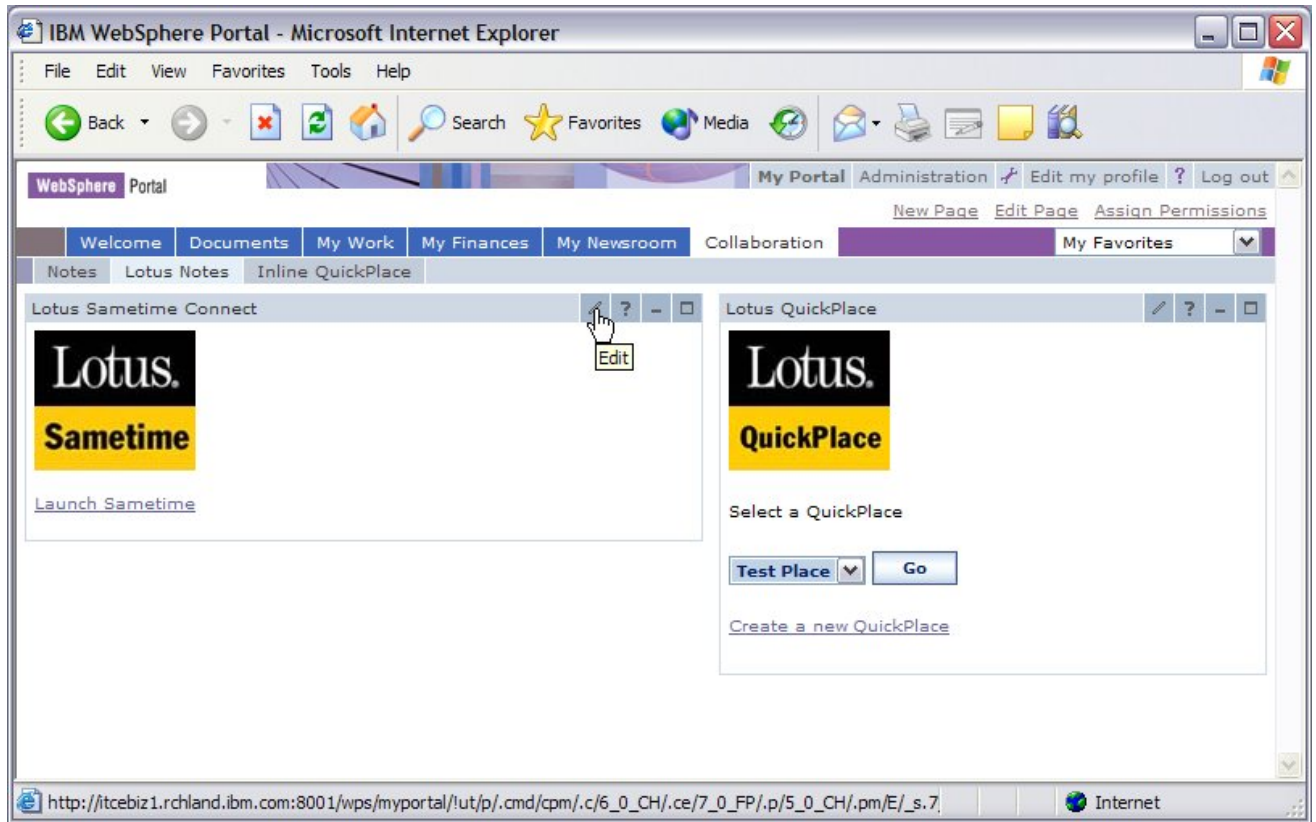
6. Click **Add Portlet** on the right side of the page and search for Lotus QuickPlace; click **OK**.



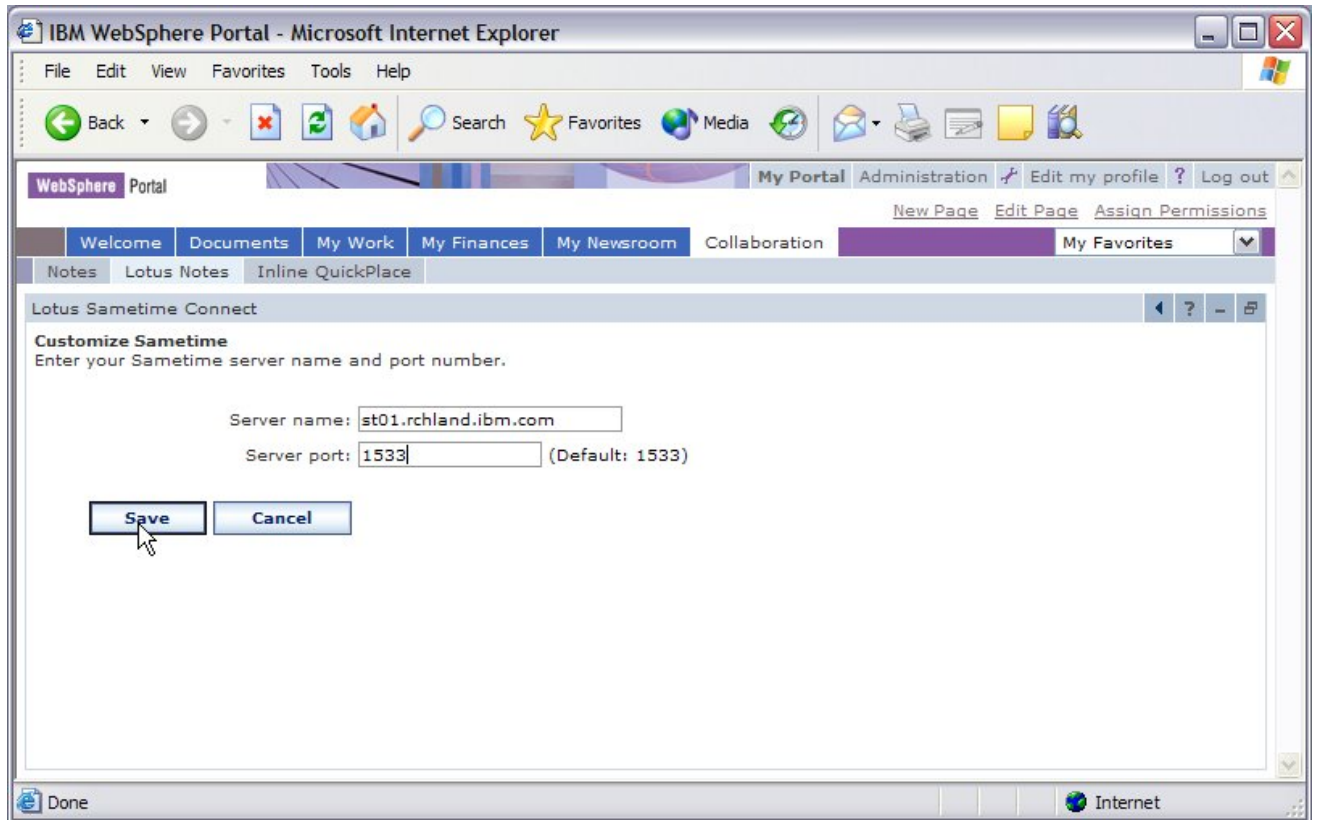
7. Once the portlets have been added, click **Done**.



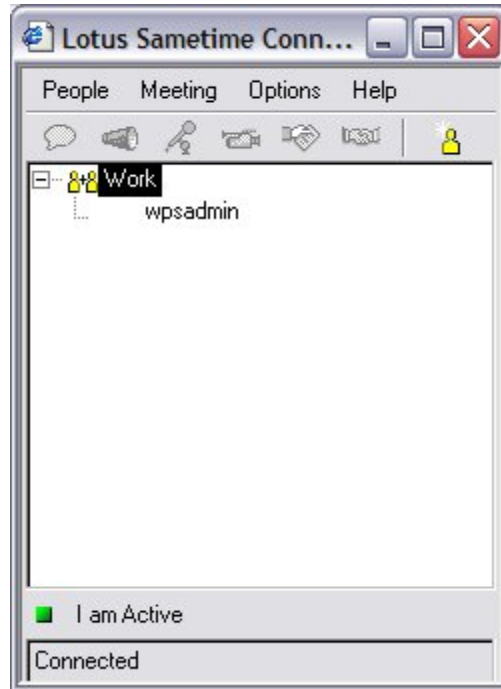
8. Edit the Sametime Portlet by clicking on the **Pencil Icon**.



9. Type in the Instant Messaging server name and the port number (1533) and click **Save**.

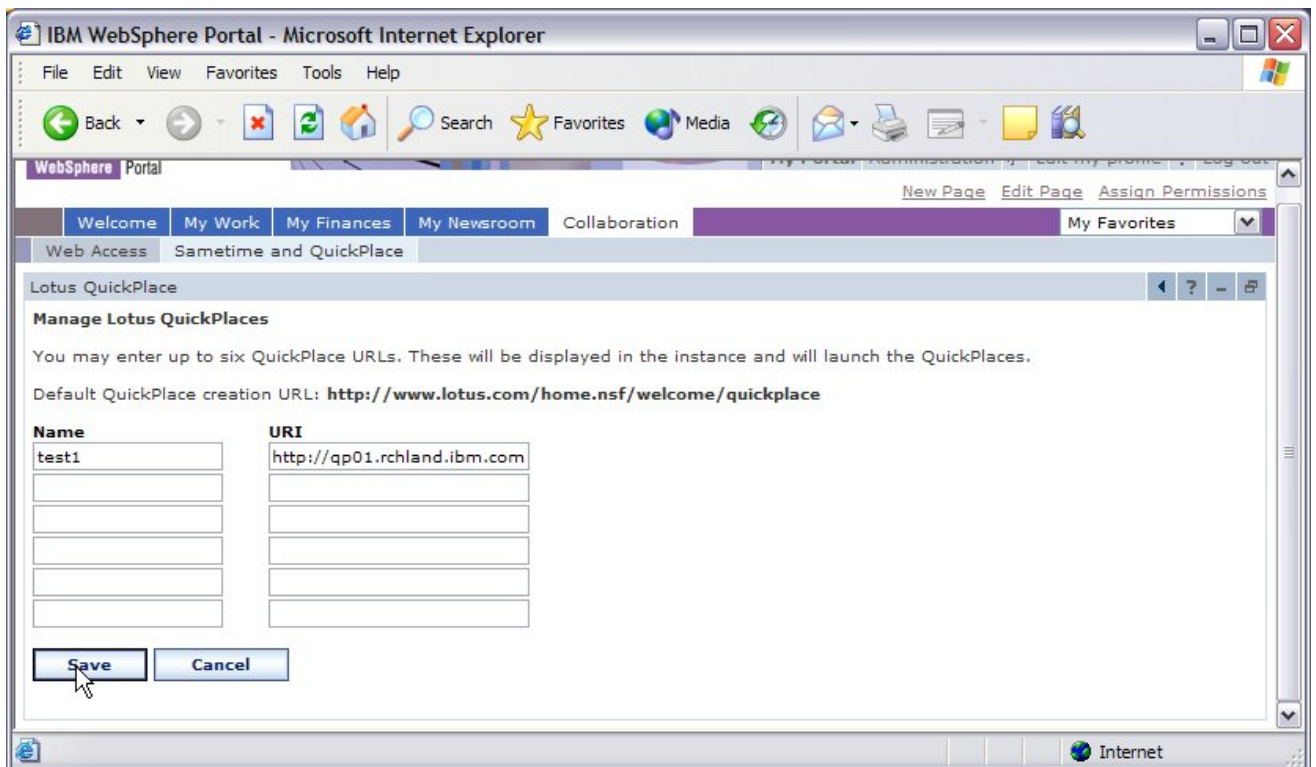


10. Launch the Sametime Client. You should not have to login with SSO working.

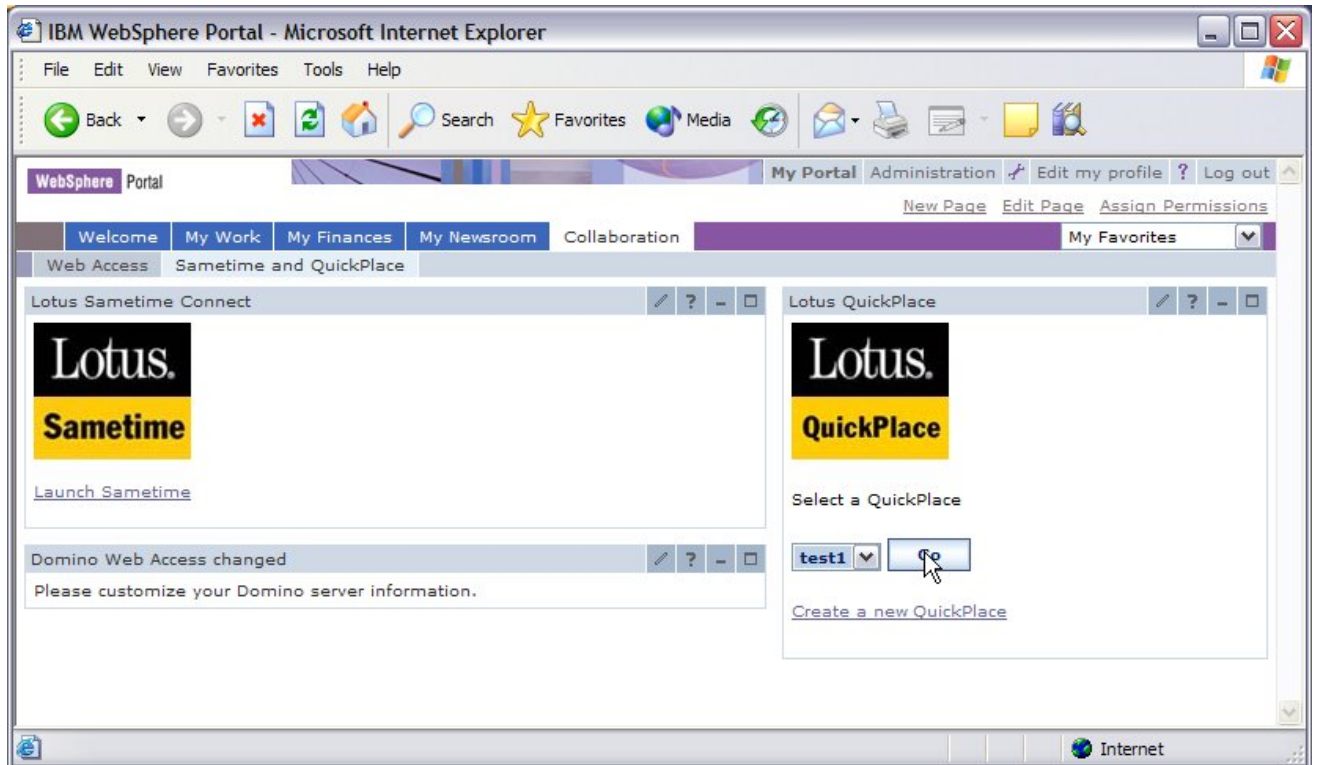


11. Edit the QuickPlace Portlet by clicking on the **Pencil Icon**

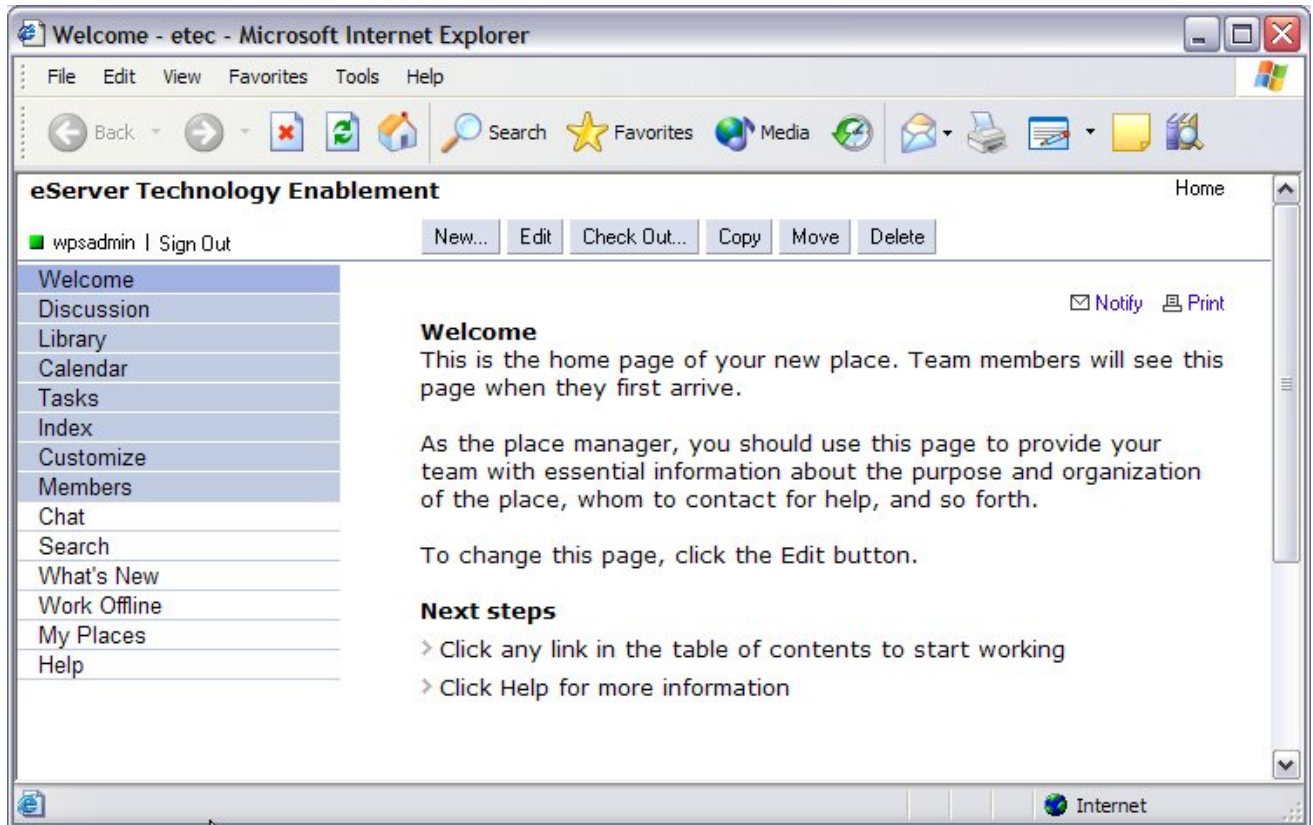
12. Enter the name of the Team Workplace and the URL of the Team Workplace server and click **Save**.



13. Click on the **Go** button to launch a Team Workplace.

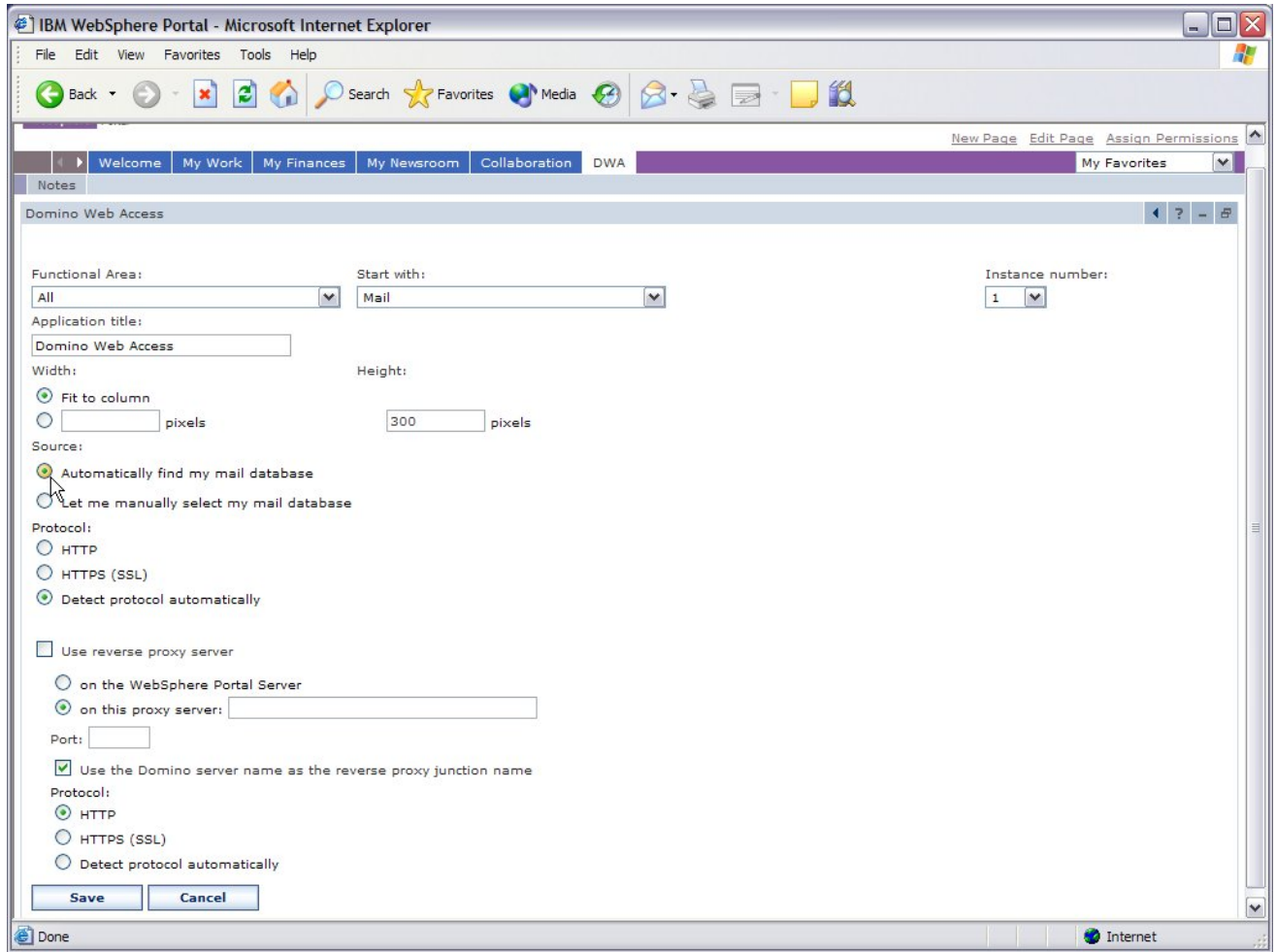


14. Another browser will open and launch into the Team Workplace. **Note:** The integration with online awareness within Team Workplace for chat purposes.

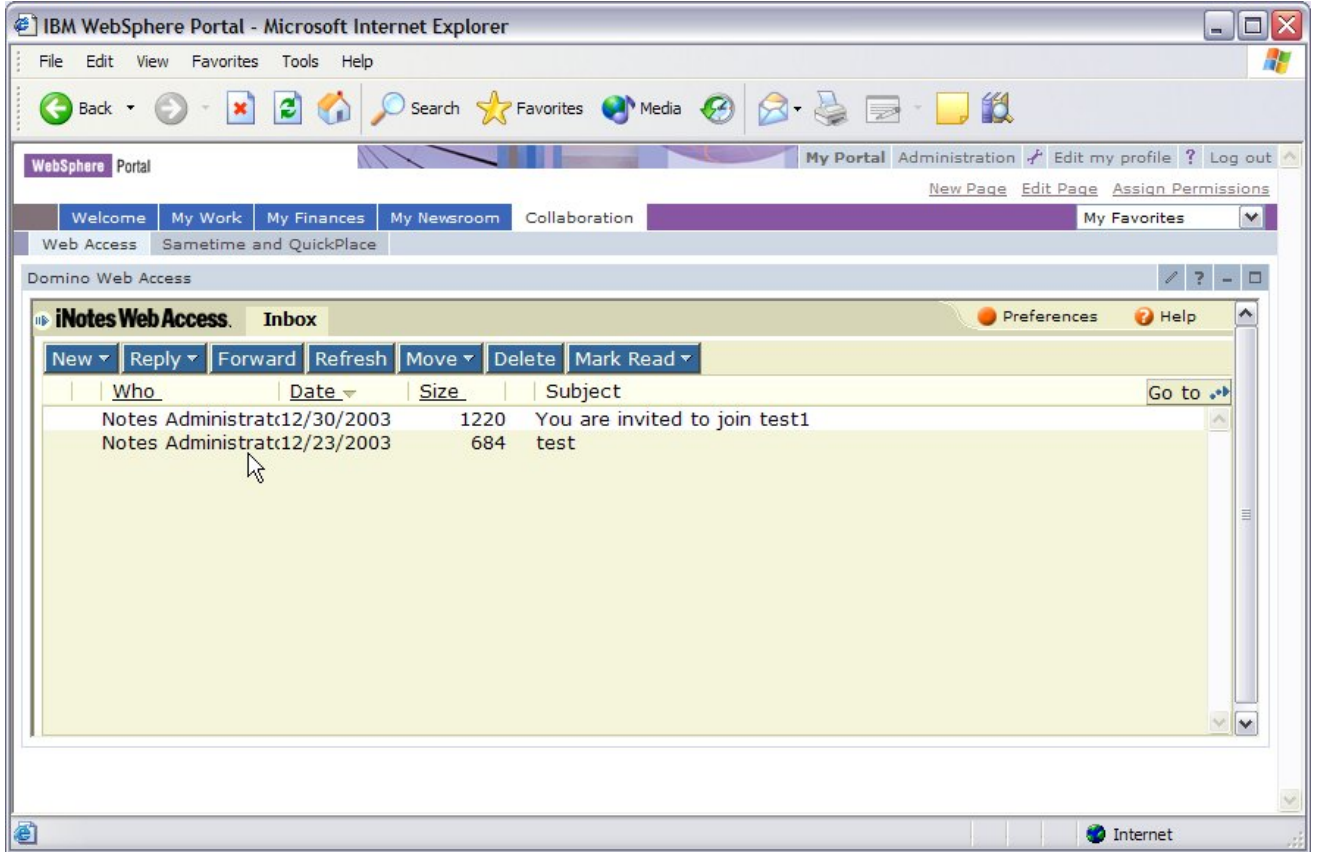


15. Domino Web Access Portlet can be added by editing the page and searching for the Domino Web Mail Portlet.

16. Choose to automatically lookup the mail database to allow users to login and be redirected to their e-mail.



17. Click back on the Domino Web Access page and notice your mail file being displayed.



Summary

This paper walked you through the steps needed to integrate the Domino servers for collaboration into WebSphere Portal and how to configure single sign-on. The deployment of portlets that use the Collaborative Component APIs was also covered. By using these instructions, you should now be able to configure a WebSphere Portal instance and add these same collaborative functionalities to it.

Appendix

Adding Domino as LDAP to existing Portal Instance.

These steps will configure WebSphere Application Server global security to use a Domino server in the LDAP configuration that will then be used for authentication requests.

1. **IMPORTANT!!** Make sure that there is a backup copy of the wpconfig.properties in the \QIBM\UserData\WebAS5\Base\- 2. Rather than edit the wpconfig.properties file directly, a configuration template will be used to make interaction with the wpconfig.properties file more convenient. WebSphere Portal includes configuration templates, which are condensed, special-purpose properties files. These templates provide only the properties needed for a given task and can also be tailored to a particular type of resource. The security_domino.properties template will be used to configure WebSphere Portal to use WebSphere Application Server security with Domino as its LDAP directory.
 - a. Using a text editor (i.e., WordPad), open the security_domino.properties file located in the \QIBM\UserData\WebAS5\Base\
- 3. The values in this file should be updated to the values for the environment. The following values in bold have been changed from the original security_domino.properties file as shipped with Portal.

```
#####  
# WebSphere Application Server Properties – BEGIN  
#####  
WasUserId=cn=wpsadmin,o=EETC  
WasPassword=wpsadmin  
WpsHostName=rchland.ibm.com  
#####  
# Portal Config Properties - BEGIN  
#####  
PortalAdminId=cn=wpsadmin,o=EETC  
PortalAdminPwd=wpsadmin  
#####  
#WebSphere Portal Security LTPA and SSO configuration  
#####  
LTPAPassword=wpsadmin  
SSODomainName=rchland.ibm.com  
#####  
# LDAP Properties Configuration - BEGIN  
#####  
LDAPHostName=Mail01.rchland.ibm.com
```



```
LDAPAdminUid=Notes Admin
LDAPAdminPwd=password
LDAPBindID=cn=wpsadmin,o=EETEC
LDAPBindPassword=wpsadmin
```

```
#####
# Advanced LDAP Configuration – BEGIN
#####
```

```
LDAPUserSuffix=o=EETEC
```

4. Save the security_domino.properties file and close WordPad.
5. Stop your Portal application server.

General rule of thumb: By default, the administration server and portal server are running in the same application server. To execute WPSConfig.sh scripts, the administration server must be running; therefore, the developer would not want to execute the stopServer command. But if the configuration changes apply, stop and restart the Portal server after executing the WPSConfig.sh script. The tasks should take care of this for you but there may be some cases in which you will need to explicitly stop and restart the Portal server. For this particular task, the application server does not need to be running initially.

6. Import the contents of security_domino.properties into wpconfig.properties
 - a. From QShell, change the directory to:
/QIBM/UserData/WebAS5/Base/<instancename>/PortalServer5/config
 - b. Enter the command:
WPSconfig.sh -DparentProperties=
/QIBM/UserData/WebAS5/Base/<instancename>/PortalServer5/config/helpers/security_d
omino.properties -DSaveParentProperties=true
Note: there should not be any spaces between the equal (=) sign and /QIBM.
 - c. Ensure that the “Successfully copied properties to...” message before proceeding.
 - d. If a “Successfully copied properties to...” message is not received, look for an exception message displayed earlier on the QShell console and verify that the command was entered correctly. “Page up” to view previously displayed messages.
7. Test the connections to the directory:
 - a. Enter the command: wpsconfig.sh validate-ldap

b. Messages similar to the following should be displayed:

```

Session A - [24 x 80]
File Edit View Communication Actions Window Help
[Icons]
Display Spooled File
File . . . . . : QSYSPRT                               Page/Line  11/30
Control . . . . . : _____                           Columns   1 - 78
Find . . . . . : _____
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
[ldapcheck] ldapPassword      : *
[ldapcheck] ldapSslEnabled    : false
[ldapcheck] objectDn         : cn=wpsadmins
[ldapcheck] #####
[ldapcheck] Checking for 'cn=wpsadmins'
[ldapcheck] #####
action-validate-ldap-bind-user:
[ldapcheck] #####
[ldapcheck] ldapURL              : port1.rchland.ibm.com:389
[ldapcheck] ldapUser         : cn=wpsadmin,o=IBM
[ldapcheck] ldapPassword     : *
[ldapcheck] ldapSslEnabled    : false
[ldapcheck] #####
BUILD SUCCESSFUL
Total time: 20 seconds
$
F3=Exit  F12=Cancel  F19=Left  F20=Right  F24=More keys
M@ a MW 03/022
Connected to remote server/host port2 using port 23

```

8. Make sure that the “BUILD SUCCESSFUL” message is at the end.
9. Run the WebSphere Portal configuration tool against the newly edited wpconfig.properties file.
 - a. From QShell, ensure the current directory is:
/QIBM/UserData/WebAS5/Base/<instancename>/PortalServer5/config
 - b. Enter the command: wpsconfig.sh enable-security-ldap –DDbPassword=<password for user who owns portal db schema>
i.e. wpsconfig.sh enable-security-ldap –DDbPassword=password
 - c. This process will run for a few minutes. At the end, the programmer should get a BUILD SUCCESSFUL message, indicating that the procedure has succeeded.
10. Configuring WebSphere Portal to work with an LDAP directory automatically enables WebSphere Application Server Global Security. In particular, with the Single Sign-On functionality, the user must type the fully qualified host name when accessing WebSphere Portal.

Note: Once security has been established with the LDAP directory, the programmer needs to provide the user ID and password required for security authentication on WebSphere Application Server when certain administrative tasks are performed with WebSphere Application Server. For example, to stop the WebSphere Portal application server, issue the following command:

```
stopServer -instance <instancename> -user admin_userid -password admin_password
```

11. Continue on with configuration by following Step 7: Verify Portal Configuration Properties for Domino (Optional) within this paper.

Trademarks

© IBM Corporation 1994-2004. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both: IBM, eServer, iSeries, Lotus, Domino, Notes, Sametime, QuickPlace, WebSphere, Tivoli

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.