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

by Daniel Hill and Mike Gordon

IBM eServer Solutions Enablement

Updated July 2004

© Copyright IBM Corporation, 2004. All Rights Reserved. All trademarks or registered trademarks mentioned herein are the property of their respective holders.

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: <u>www.lotus.com/brand</u>.)

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.

- Open Domino Admin Client, click File -> Open Server and type the name of the mail/LDAP server - Mail01/ETEC
- Click the Configuration tab —> Server —> All Server Documents. Open the Mail01/ETEC server
- 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.

Server: Mail01/ETEC - Dom	nino Administrator		
File Edit View Create Actions	Help		
] 중 🕹 승 🏷 🏷	🗈 💽 + - +	M () 🗟 📄
(+ + -) - (2) (?) (* - (+ -)			
]			
18MUS Domain	ver: Mail01/ETEC X		
T Edit Server			
			1001001
SERVER: Mail	UI/EIEG * ** ·		0010101
Basics Security Ports	Server Tasks Internet Protoco		
	Derver rasks internet rotoco	is [WITAS] Wiscellaneo	
Basics			
Server name:	Mail01/ETEC	Server build number:	Release 5.0.12
Server title:	Mail and LDAP Server	Administrators:	Notes Administrator/ETEC, Mail01/ETEC
Domain name:	ETEC	Routing tasks:	Mail Routing
Fully qualified Internet host name:	mail01.rchland.ibm.com	SMTP listener task:	Disabled
Cluster name:	W.	Server's phone number(s):	
Directory Assistance database name:		CPU count:	12
Directory Catalog database name on this server:		Operating system:	IBM OS/400
Optimize HTTP performance based on the following primary activity:	Advanced (Custom Settings)	Is this a Sametime server?:	No
Server Location Info	rmation		
		A Solaria A	nnected

4. 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.

Server: Mail01/ETEC - Domino Administrator			X				
File Edit View Create Actions Help							
◇							
BMUS Domain 🛄 Server: Mail01/ETEC 🗙							
🙀 🕜 Edit Server 🥥 Web							
SERVER: Mail01/ETEC		0100100 0010101 0010101	1				
Basics Security Ports Server Tasks Internet Proto							
			-				
HTTP Domino Web Engine IIOP LDAP NNTP	1						
Basics	Mapping						
Host name(s): mail01.rchland.ibm.com	Home URL:	/homepage.nsf?Open					
Bind to host name: Enabled	HTML directory:	domino\html					
DNS lookup: Disabled	Icon directory:	domino\icons					
Default home page: default.htm	Icon URL path:	licons					
Allow HTTP clients to • Yes • No browse databases:	CGI directory:	domino\cgi-bin					
Maximum requests over 1 a single connection:	CGI URL path:	/cgi-bin					
Number active threads: 40							
NOTE: The following setting is no longer used in You should use it only Domino.	DSAPI						
for servers running versions prior to 4.6.							
Minimum active threads: 20	DSAPI filter file name	95					
Enable Logging To:	Log File Settings		-				
		•					
	• 🔛 🔹	Disconnected					

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

Server: Mail01/ETEC - Domino Administrator	
File Edit View Create Actions Help	
]◇⊑ළ)]⊀⊑⊡)]ि℃♂∿∜	Ŷ ┺ TE + - t = M Q 届
] 🗘 • 🖒 - 🙆 🚱 Q [†] •	
9 IBMUS Domain	
🙀 🛿 Edit Server 🥥 Web	
SERVER: Mail01/ETEC	01001001
and the second s	101010
Basics Security Ports Server Tasks Internet Proto	cols MTAs Miscellaneous Transactional Logging
i 😥 🚬 🚬 🚬 🚬 🚬	
HTTP Domino Web Engine IIOP LDAP NNTP	
HTTP Sessions	Java Servlets
Session authentication: Multi-server	Java servlet support: None
	Servlet URL path: /servlet
~	Class path: domino\servlet
Generating to this Server	Servlet file extensions:
•	
	▲ 💭 ▲ Disconnected ▲ Etec ▲

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.

💮 Se	erver: Mail01/ETEC -	Lotus Notes						_ 🗆 🔀
File	Edit View Create Act	ions Help						
	∎ ċ-1 ¤∌]]	∦월│월]주오(ን 🖓 🏷 🖻 💽 🕂 — 🖯	<u>e</u> M Q				
Add	ress				•]) ۞ • ⇨	- 🚫 🚱 Q* -	•	
	🗑 Workspace 🛄 ET	EC's Address Book - Server >	Server: Mail01/ETEC 🗙					
	🕜 Edit Server 🌖	Web						
1	SERVER: M	lail01/ETEC		. 18	Har (A	0100	01010101010	
9	Basics Security F	Ports Server Tasks Inte	rnet Protocols MTAs Misco	ellaneous Tr	ansactional L	ogging Adm	inistration	
	Notes Network Po	rts Internet Ports Proxie	es					_
	Port	Protocol	Notes Network	Net Addr	ess	Enabled		
	TCPIP	TCP	NETWORK1	Mail01.rch	land.ibm.com	ENABLED		
				Mail01	k}	DISABLED		
				Mail01		DISABLED		
				Mail01		DISABLED		
				Mail01		DISABLED		
2				Mail01		DISABLED		
ଲ				Mail01		DISABLED		
6				Mail01		DISABLED	<u>_</u>	
								_
↑ ↓								-
				<u> </u>	🎝 🔺 🗙 Disco	onnected	Etec	• 🛄 (•

7. 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**.

ertificates:	C Yes 🖲 No	
ccept expired SSL ertificates:		
b Directory Mail [Veb HTTP/HTTPS)	DIIOP Remote Debug Manager	
CP/IP port number:	80	
CP/IP port status:	Enabled	-
inforce server access ettings:	No	
uthentication options:		
Name & password:	Yes	
Anonymous:	Yes	
SL port number:	443	
SSL port status:	Disabled	
uthentication options:		
Clinet and Contact	No	
Client certificate:		
Name & password:	Yes	

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

9. 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.

🤣 wpsadmin/ETEC - Domino Administrator	
Eile Edit View Create Actions Window Help	
Prev Main Next Previous Next Next Direction Direction Opat Statt Statt Statt Show/Hide	Iapse Expand All Collapse Al Properties Cut
B L Edit Person Cancel	
Person: wpsadmin/ETEC wpsadmin/ETEC@ETEC	and a
Basics Work/Home Other Miscellaneous Certificates Roaming Administration	
Basics	
First name: Mail s	vstem: Notes
Middle name: Doma	in: FTEC
Last name: wpsadmin Mails	arver: Mail01/ETEC
User name: wpsadmin/ETEC Mail fi	e: mail\wpsadmin
wpsadmin Eorwa	rding address:
Alternate name:	et address:
Forma	t preference for
Short name/UserID: wpsadmin incom	ing mail: Keep in senders' format
Personal title: When	receiving
Generational qualifier:	rypted mail, encrypt No
Internet password: (EAE198FC92F337E15652B5CE81652624) mailfil	e:
Preferred language:	73
Real-Colla	Time boration
Same	ime server:
UserID	

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.

<u>ا</u>	wpsadmins - Dom	ino Administrator						_ 0	X
File	Edit View Create	Actions Text Window	Help						
]	0 0	Attach	B Bold	J Italic Per	n Pen Spacing	Indent Outdent	ž	Properties 8	
	Chat Start Inst	ar Add to Inst Show/Hide							
	🧑 IBMUS Domain	🚰 Welcome 🗙 🛄 wpsa	admins 🗙						
1	Save & Close	ORefresh Sort	Member List 🗴 🔿	ancel					
) (2) (2) (2)	Multi-purpo	se group: wpsa	dmins				1.89	11 -2	IN
	Basics	AP St.			Group type	e description			
	Group name:	^r wpsadmins "							
	Group type:	[®] Multi-purpose			'Multi-purpo	se' groups are the de	efault group type a	nd used in most	
	Category:	° J I			situations.				
	Description:	г 			They can be	used for access con	trol and email pur	poses.	
	Mail Domain:	r _							
	Internet Address:	r J							
	Members:	[☞] Notes Admin/ wpsadmin/ETE	etec d_						
					1	🖌 🔜 🔺 🗶 Discon	nected 🔺 Offic	» •) 🛄	•

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 DIIOP 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.

- 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.

😣 N	New Configuration - Domino Administrator	
File	Edit View Create Actions Text Help	
	·	ABC 1
0		
	●● 含目	
	Etec Domain Win New Configuration X	
5	TI Save and Close	
	CONFIGURATION SETTINGS	1010101
	Basics LDAP Router/SMTP MIME NOTES.INI Settings iNotes Web Access Administration	N MET VICTOR
	LDAP Configuration	
	Choose fields that anonymous users can query via LDAP:	
	Anonymous users can query:	
	Allow LDAP users write access:	
	Timeout: 0_seconds	
	Maximum number of entries returned: [0]	
	Minimum characters for wildcard "1 search:	
	Allow Alternate Language Information "No J	
	Rules to follow when this directory is the 🙆 Don't modify any	
	primary directory, and there are multiple C Modify first match	
	being compared/modified:	
		-) [[] -)
<u> </u>		

- 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

LDAP Field List		? ×
Form Person	Show Fields	Ск
	Add > AltFullName Certificate FirstName FullName InternetAddress	Cancel
NOTE: The list of queriable fields pertain to the	all forms which have a field of the same name in directory	

- 7. 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
- 9. Click **OK** to close the LDAP Field List dialog box and return to the Configuration Settings document, the LDAP tab
- 10. 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
- 11. 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.
- 12. 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.

🤫 Etec Domain	
People & Groups Files Server Me	essaging Replication Configuration
Server: Mail01/ETEC Release 5.0.12 on OS40	0 V5R2M0 Use Directory on: Current Set
) V 🗍 Server	🕜 Edit Server 🥥 Web
All Server Documents	SERVER: Mail01/ETEC
Connections	Basics Security Ports Server Tasks Internet Protocols MTAs Miscellaneous Transactional Logging
 Frograms External Domain Network Info Messaging Replication Directory Policies Web Monitoring Configuration 	SSL settings SSL key file name: keyfile.kyr SSL protocol version (for Negotiated use with all protocols
 ♪ ஹ Cluster > @ Certificates > Miscellaneous 	Accept SSL site C Yes C No certificates:
	Accept expired SSL
	Web Directory News Mail IIOP Directory
	Image: TCP/IP port number: 389 TCP/IP port status: Enabled Authentication options: Xee
	Anonymous: Yes
	SSL port number: 636
	SSL port status: Disabled
	Authentication options:

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 > <u>ST01</u>	
	1
Directory type <u>*LDAP</u> *DOMINO, *LC	PAP
Name MAIL01.RCHLAND.IBM	
Port 389 1-65535 Allow HTTP Tuppeling *NO *YES *NO	
Event Server port <u>9092</u> 1-65535	
Token Server port <u>9094</u> 1-65535	
F2=Evit E4=Prompt E5=Refresh E12=Pancel E12=How to us	More
F24=More keys	e this display
	00-00-7
MIL a Session successfully started	09/03/
U 1792 Session addression storted	

(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.

1. 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:

 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.

🕘 AS/400 QuickPlace Setup Page 2 - Microsoft Internet Explorer						
File Edit View Favorites Tools Help						
🚱 Back 🔹 🐑 🔹 😰 🏠 🔎 Search 👷 Favorites 🜒 Media 🤣 🎯 - 🍑 🔛 - 🛄 🎇						
Address 🗃 http://ebcc03a:8585/setupqp.nsf/Setup/e246b6093c83bd3605256e140066d930?EditDocument&Seq=1						
Links 👸 IBM Business Tr	ransformation Homepage 🛛 👸	IBM Internal Help Homepa	ge 💰 ISSI 💰 ESPN Fantasy Games	≫ 🛱 SnagIt 🖺		
Google -	🖌 😚 Sea	rch Web 🔹 🥒				
all and						
	2. QuickPlace Settings			Quick Help		
Lotus. software	Please review and comple	te the following informat	ion.	For Help, click on the blue		
	Server Identity: Domino Server name:	QP01	Required	labels.		
Part States	Server ID password:	ne's Identity		Once the information is satisfactory, click the Finish buttee below to		
	Administrator's	anadmin	Required	add QuickPlace to your		
	name:	dhaannu		Domino server.		
(0)	Password:	•••••	Required			
	Confirm password:	•••••	Required			
TRM	Existing Domino Server:					
Variate .	Start the server:	⊙Yes ○No				
				Finish		
ē				S Local intranet		

- 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://gp01.rchland.ibm.com/QuickPlace/ and log in as qpadmin
- 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**.

🕘 User Directory - quick	place - Microsoft Internet Explorer	_ 🗆 🖂
File Edit View Favorite	es Tools Help	R
🚱 Back 🔹 🕥 🕤 🗶	📔 😭 🔎 Search 🤺 Favorites 🜒 Media 🧐 🔗 - 嫨 📰 - 🛄 🎉	
Address 🙆 http://qp01.rchla	nd.ibm.com/QuickPlace/quickplace/Admin.nsf/2a1fb3846ca143220525670800167222/b4ef119005fbd54a0525670800	016713b 💙 ラ Go
Links 👸 IBM Business Transfo	ormation Homepage 👸 IBM Internal Help Homepage 👸 ISSI 💰 ESPN Fantasy Games 🎽 🛱 SnagIt	₽
Google -	Search Web 🔹 🥒	
	Change User Directory You can specify a user directory from which place members can be selected.	Back Next
	Directory. You can specify a directory from which place managers can select Select the directory type and name below: Type: LDAP Server Name: mail01.rchland.ibm.com	members.
	Advanced Settings. You can enter specific settings for your directory or leave blank to make use of the default settings. Port 389 389	/e them
	Check for SSL connection with LDAP User Directory. Search base: 0=ETEC	
	□ Narrow searches to the place name.	
	Note: Specify the search base using the Distinguished Name format.	~
Applet STLinksApp started	🔮 Int	ernet 🧠

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.

 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)

lew Datat	oase	?
Specify	New Database Name and Location	
Server	QP01/ETEC	RK
<u>T</u> itle	Domino Web Configuration	Cancel
<u>File name</u>	domcfgnsf	
	Encryption	
	©reate full text index for searching	Ad <u>v</u> anced
Specify	Template for New Database	
Server	QP01/ETEC	
Temp <u>l</u> ate	 Domino Directory Domino LDAP Schema Domino MailTracker Store Domino R5 Certificate Authority Domino Web Administrator (R5) 	
File <u>n</u> ame	domcfg5.ntf	<u>A</u> bout
	 ✓ Show advanced templates ✓ Inherit future design changes 	

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

🥺 (Untitled) - Domino Administrator	
File Edit View Create Actions Help	
[◇묘疊] ᆊ월○ 주산수↔	🏷 🏷 🖻 📧 🕂 ㅋ 슈 ㅋ 🖊 ٩ 🤇 🖥
] (⊐ + ⊂) - <mark>(2)</mark> (®) (Q [*] +]	
🥮 ETEC Domain 🖆 Domino Configuration - Login 🗙 🌠	(Untitled) ×
Login Form Mapping	
a	
Site Information	
Server type: Primary Server	
Comment: QuickPlace Login	
Target Database file name: QUICKPLACE/RESOU	RCES.NSF
Target Form name: QuickPlaceLoginForm	
	×Disconnected

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)
- 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="" name="" schema=""></iseries>
	e.g. PortalDB1
UserName	<iseries useraname=""></iseries>
	e.g. wpsdbuser
Password	password
Default URL path	wps
http://bvilla.rchland.ibm.com:10000/ wps/ portal	
Default home path	portal
http://bvilla.rchland.ibm.com:10000/wps/ portal	
Personalized path:	myportal
http://bvilla.rchland.ibm.com:10000/wps/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	o=ETEC
Parent DN:	
Information describing the administrative group entry	*ROOT
Parent DN:	
Portal administrative group and administrator information:	
Administrative group name: wpsadmins Administrator name: wpsadmin	
Password:	wpsadmin
Confirm Password:	wpsadmin

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

 \bullet # 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

 \bullet # 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

 - \bullet # 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
- 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
 - # LDAPPort: The LDAP server port number
 - # For example, 389 for non-SSL or 636 for SSL
 - LDAPPort=389
 - # LDAPAdminUId: The LDAP administrator ID
 - LDAPAdminUId=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: { DOMIN0502 }
 - # Active Directory: { ACTIVE DIRECTORY }

- # SunOne: { IPLANET }
- # Novell eDirectory: { NDS }
- # Note: use IPLANET for SunONE
- LDAPServerType=DOMIN0502
- #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 wpconfig.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.

- Start the WebSphere Administration Console through a browser: http://<servername>:admin Port>/admin. Login using the user ID "wpsadmin" and the password "wpadmin".
- WebSphere Administrative Console Microsoft Internet Explorer File Edit View Favorites Tools Help 😰 😭 🔎 Search 👷 Favorites 🜒 Media 🥝 🎧 🕹 🥽 🛄 🏭 🕒 Back 🝷 🍙 🐇 Address 🗃 https://portal3.rchland.ibm.com:20211/admin/secure/securelogon.do?action=secure 🕶 🔁 Go Links 🧃 ISSI 🗃 Roch 💩 ThinkCU 🧃 ISeries Navigator for Wireless 🗃 IBM WebSphere Portal 🐉 IBM WebSphere Portal DomDev 💐 IBM Bus. Trans 👹 W3Help 👸 Portal3 Google v 💏 Search Web 🔹 🥒 WebSphere Application Server Administrative Console Version 5 Home | Save | Preferences | Logout | Help | BB User ID: wpsadmin PORTAL3_wps2 WebSphere Application Server on About your WebSphere Application Server + Servers IBM.com IBM WebSphere Application Server, 5.0.2 . F Applications The place for support; including WebSphere Build Number: ptf2M0325.01 E Resources Flashes, FAQs, Hints and Tips, and Technotes. Build Date: 06/23/2003 You will also find Downloads, Library, News, and E Security IBM WebSphere Application Server Enterprise, other useful information. Global Security 5.0.2 SSL Authentication Mechanisms LTPA User R_)stries WebSphere Developer Domain InfoCenter Get the latest technical articles, best practices, The complete source for product documentaton, Authentication Protocol tutorials and much more in the WebSphere including tasks, reference, and conceptual F Environment Application Server Zone. Influence the evolution of information on product features and functions. WebSphere Application Server and request new F System Administration product features WebSphere Status i January 13, 2004 5:05:06 PM UTC 🗘 < Previous Next > WebSphere Configuration Problem Total Configuration Problems :0 1 : 0 total A: 0 total E : 0 total F Preferences Inters://portal3.rchland.ibm.com:20211/admin/navigatorCmd.do?forwardName=LTPA.config.view 🔒 🥝 Internet
- 2. Select Security -> Authentication Mechanism -> LTPA

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

WebSphere Administrative Consol	le - Microsoft Internet Explo	orer				
File Edit View Favorites Tools F	Help					
🕒 Back 🔹 🐑 - 💌 🗟 🏠) 🔎 Search 🤺 Favorites	🔮 Media 🚱	🔊 · 🍃 🖻	📃 🛍		
WebSphere. Application Server Version 5	Administrative Console					
User ID: wpsadmin	LIPA					
ITCEBIZ1_wps1dIdap	Lightweight Third Party Authe GlobalSecurity panel and clic After security is enabled, a n press OK or Apply to genera button. The new set of keys	entication configuration k Apply or OK to valida ew set of keys can be te the keys (no need to will not be used until s	a settings. When secur the the changes. The L generated in two way press the Generate k aved. [i]	ity is enabled and an TPA keys are automa ys. If the password r Keys button). If passv	y of these properties are changed, please go atically generated the first time security is enab needs to be changed, change the password a word is the same, just press the Generate Key	to the vled. nd rs
Global Security	Configuration					
SSL Authentication Mechanisms	Generate Keys	Import Keys	Export Keys			
LTPA	General Properties					
 User Registries JAAS Configuration Authentication Protocol Environment System Administration Troubleshooting 	Password	*			The password to encrypt and decrypt LTPA keys. This password should be use when importing these keys into other WebSphere Application Server administra 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 automatii generated. This new set of keys will be u after saved.	t the ed ative s cally used
	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 si be longer than cache timeout configured Global Security panel.	n hould in the
	Key File Name				The name of the file used when import or exporting keys. Enter file name and the click either Import Keys or Export Keys. T imported keys will be used after saved.	ting n he
	Apply OK Reset	Cancel				
	Additional Properties Trust Association Enable Single Signon (SSO) Speci	e Trust Association. Tr ifies the configuration	rust Association is use values for single sign-(ed to connect reverse	ed proxies to Websphere.	
	WebSphere Status	Probleme	<u>< Previous</u> <u>Ne</u>	<u>xt></u>	January 14, 2004 5:49:07 PM	итс ሷ
	Total Configuration Problems :	1	💽 : <u>1 total</u>		C total	
						-
🙆 Done					🔒 🥥 Internet	

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

WebSphere Administrative Conso	le - Microsoft Internet Exp	lorer			
File Edit View Favorites Tools	Help			🥂	
🕞 Back 🝷 🐑 🔺 🛃 🎸	Search 👷 Favorites	🜒 Media 🖉	3• 🕹 🖃 🛄 🛍		
WebSphere. Application Server Version 5	Administrative Console				
nome save Freierences L					
User ID: wpsadmin	Message(s)				
ITCEBIZ1_wps1dldap	Changes have been made	e to your local configuration	. Click Sane to apply changes t	o the master configuration.	
Servers	The server may need to b	e restarted for these chang	es to take effect.		
Applications					
	LTPA				
Security	Lightweight Third Party Auth	entication configuration set	ings When security is enabled	and any of these properties are changed please on to the	
Global Security	GlobalSecurity panel and click Apply or OK to validate the changes. The LTPA keys are automatically generated the first time security is enabled.				
SSL	After security is enabled, a r	new set of keys can be gen te the keys (no need to pre	erated in two ways. If the pase as the Generate Keys button)	sword needs to be changed, change the password and	
 Authentication Mechanisms 	button. The new set of keys will not be used until saved.				
LIPA III. Haar Begintrice					
	Configuration				
Authentication Protocol					
	Generate Keys	Import Keys	Export Keys		
	General Properties				
Troubleshooting	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	
	WebSphere Status	03	Previous <u>Next ></u>	January 14, 2004 5:56:48 PM UTC 👲	
	WebSphere Runtime Mes	sages	***	Clear All	
	Total All Messages:493	🚳 : <u>1 new, 1 total</u>	A: 25 new, 25 total	L : 467 new, 467 total	
	Preferences				
https://itcebiz1.rchland.ibm.com: 20111/ad	lmin/syncworkspace.do?syncactior	n=list		🔒 🔮 Internet	

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

File Edit Wew Pavorites Tode Help Image: Second Se	WebSphere Administrative Consol	ole - Microsoft Internet Explorer	_ 🗆 🗙
Seck Image: Seck WebSphere Applications Applications Applications Applications Authentication Hiechanisms LTPA > Save	File Edit View Favorites Tools	Help	1
WebSphere Application Server Administrative Console Home Save Preferences Logout Help User ID: vpsadmin If CEBU21_vpsatidap Images have been made to your local configuration. Clck Save to apply changes to the master configuration. Images have been made to your local configuration. Clck Save to apply changes to the master configuration. If CEBU21_vpsatidap Images have been made to your local configuration. Clck Save to apply changes to the master configuration. Images have been made to your local configuration. Clck Save to apply changes to the master configuration. Images have been made to your local configuration. Images have been made to your local configuration. Images have been made to your local configuration. Images have been made to your local configuration. Images have been made to your local configuration Images have been made to your local configuration. Images have been made to your local configuration. Images have been made to your local configuration Images have been made to your local configuration. Images have been made to your local configuration. Images have been made to your local configuration Images have been made to your local configuration. Images have been made to your local configuration. Images have been made to your local configuration Images have been made to your configuration. Images have been made to your configuration. <tr< td=""><td>🚱 Back 👻 🕥 - 💌 🖻 🏠</td><td>Search 📌 Favorites 🜒 Media 🚱 🔗 - 🌺 📄 🛄 🎇</td><td></td></tr<>	🚱 Back 👻 🕥 - 💌 🖻 🏠	Search 📌 Favorites 🜒 Media 🚱 🔗 - 🌺 📄 🛄 🎇	
User ID: wpsadmin Message(s) ITCEBIZ1_wps1dldap Changes have been made to your local configuration. Click Save to apply changes to the master configuration. ID: The server may need to be restarted for these changes to take effect. ID: The server may need to be restarted for these changes to take effect. ID: Resources ID: The server may need to be restarted for these changes to take effect. ID: The server may need to be restarted for these changes to take effect. ID: Security Ssle Authentication Mechanisms ID: Save your workspace changes to the master configuration ID: User Registries JAAS Configuration Click the Save button to update the master repository with your changes. Click the Discard button to discard your changes and begin work agan using the master repository configuration. Click the Cancel button to continue working with your changes. ID: Environment ID: View fems with changes Save	WebSphere. Application Server Version 5 Home Save Preferences Lo	Administrative Console	
ITCEBI21_wps1didap Servers Applications Resources Security Global Security SSL Mathematication Mechanisms LTPA User Registries JAAS Configuration Environmet System Administration Troubleshooting WebSphere Status [] ≤Previous Nets: January 14, 2004 5:56:48 PM UTC © WebSphere Runtime Messages 4:33 1 new. 1 total Preferences Clear All	User ID: wpsadmin	Message(s)	
 Servers Servers Applications Resources Security Clobal Security SSI Authentication Mechanisms LTPA User Registries JAck Configuration Clobal Association Clobal Security Save to Master Configuration Clobal Security Save to Master Configuration. Click the Cancel button to discard your changes and begin work again using the master repository with your changes. Click the Discard button to discard your changes and begin work again using the master repository configuration. Click the Cancel button to continue working with your changes. Total changed documents: 1 View Items with changes Save	ITCEBIZ1_wps1dldap	Charges have been made to your least exciting. Click Save to each, shapeen to the master and fourthing	
 Applications Applications Resources Security Global Security SSL Authentication Mechanisms LTPA > Save your workspace changes to the master configuration Save to Master Configuration Authentication Protocol Environment System Administration Troubleshooting WebSphere Status [] < Previous Next ≥ Iotal YebSphere Status [] < Previous Next ≥ Iotal Total All Messages.493	⊡ Servers	The server may need to be restarted for these changes to take effect	
 Resources Security Securit	Applications	Er me server may need to be restance for these changes to take effect.	
Security Save Substained Security Save State Save your workspace changes to the master configuration LTPA Save to Master Configuration JAAS Configuration Authentication Protocol Authentication Protocol Click the Save button to update the master repository with your changes. Click the Discard button to discard your changes and begin work again using the master repository configuration. Click the Cancel button to continue working with your changes. System Administration View items with changes Troubleshooting View items with changes View Items with Changes Save Discard Cancel ViewSphere Status [] < Previous Next> ViewSphere Runtime Messages 1 new, 1 total @ : 25 new, 25 total Total All Messages:493 : 1 new, 1 total @ : 25 new, 25 total Preferences	E Resources	LTPA >	
Subbal Security SSL Authentication Mechanisms LTPA User Registries JAAS Configuration Authentication Protocol Environment System Administration System Administration Troubleshooting WebSphere Status [] Cancel WebSphere Status [] Clear All Total All Messages: 493 Total All Messages: 493 Total All Messages: 493 Total All Messages: 493 Previous Next 2: Status [] Previous Mest 2: Status [] Status [] Previous Next 2: Status [] Previous Mest 2: Status [] Previous Next 2: Status []	Security	Save	
WebSphere Status ii ≤ Previous Next ≥ January 14, 2004 5:56:48 PM UTC © WebSphere Runtime Messages Clear All Total All Messages:493 1 new, 1 total 1 : 25 new, 25 total 1 : 467 new, 467 total Image: Preferences Image: Preferences Image: Preferences Image: Preferences	Global Security SSL Authentication Mechanisms LTPA User Registries JAAS Configuration Authentication Protocol Environment System Administration Troubleshooting	Save your workspace changes to the master configuration Save to Master Configuration Click the Save button to update the master repository with your changes. Click the Discard button to discard your changes and begragain using the master repository configuration. Click the Cancel button to continue working with your changes. Total changed documents: 1 Image: Discard Cancel	in work
WebSphere Runtime Messages Clear All Total All Messages:493 Image: 1 new, 1 total		WebSphere Statue	
Preferences		WebSphere Runtime Messages Clear Total All Messages:493 : 1 new. 1 total	All
			-
🙆 Done	Cone	🔒 🧶 Interne	t ,

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

WebSphere Administrative Consc	ole - Microsoft Internet Exp	lorer	
File Edit View Favorites Tools	Help		
🚱 Back 🝷 🕥 - 💌 🗟 🎸	Search 👷 Favorite	s 🜒 Media 🚱 🔗 👹 🔜 🗾	11
WebSphere. Application Server Version 5	Administrative Console		
Home Save Preferences L	.ogout Help	Apple to demonstrate the new the mode to proce the con-	
User ID: wpsadmin	Generate Keys button. The r	new set of keys will not be used until saved. 🚺	· · · · · · · · · · · · · · · · · · ·
ITCEBIZ1_wps1didap ⊞ Servers	Configuration		
Applications	Our set to the set		
	Generate Keys	Import Keys Export Keys	
Security	General Properties		
Global Security SSL → Authentication Mechanisms LTPA → User Registries → JAAS Configuration → Authentication Protocol	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.
Environment System Administration	Confirm Password	* •••••	Confirm the password to encrypt and decrypt the LTPA keys.
■ Troubleshooting	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	Itpa.key	The name of the file used when importing or exporting keys. Enter file name and then click either Import Keys or Export Keys. The The
	WebSphere Status i	<pre>< Previous Next ></pre>	January 14, 2004 6:09:01 PM UTC 👲
	WebSphere Runtime Mes	ssages	Clear All
	Total All Messages:493	(): <u>1 new, 1 total</u> : <u>25 new, 25 total</u>	: 467 new, 467 total
	Preferences		
E Done			🔒 🥥 Internet

- 7. Click **Save** and then **Save** again for the Master Configuration. This is similar to steps 4 and 5.
- 8. 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



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.

Current Server Document	Add Server	🛿 Edit Server 🏻 🎝 Delete Server	Add to Cluster	🕤 Web.		
All Server Documents	Domain	Server ^	Title	Create	Virtual Server	Ph
 Configurations Connections Programs 	▼ ETEC	Hub01/ETEC	Administration Hub	Create Create Create	URL Mapping/Redirection File Protection Realm	
External Domain Network Infi		Mail01/ETEC	Mail and LDAP Serv	View Cu Create	rrent Configurations Web SSO Configuration	Ē
Replication		QP01/ETEC	Team WorkPlace Se	rver	Administrator/ETEC	
 Policies Web Monitoring Configuration Cluster Certificates Miscellaneous 		ST01/ETEC	Instant Messaging a Conferencing	nd Web	Notes Administrator/ETEC	

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.

🥪 Web SSO Configuration - Domino Administrator	
File Edit View Create Actions Text Help	
◇ ⊟ @ ,⊀ Ēē Ó ▼ B	- / ⋟ ⋷ ≣ := := := * ≣: 🏠 🗆 ⊘ 🔁 🛤 🍄 🍱
] (+ + -> - <mark>(2)</mark> (0 , Q (+)	
SSO Configuration X	
🙀 🛬 Save and Close 🔓 Keys	
Web SSO Configuration for :	Sand John Co
	The City of
	8 2 (-88
Token Configuration	Token Expiration
Token Name: LtpaToken	Expiration (minutes):
Token Domain:rchland.ibm.com	
Participating Servers	
Domino Server Names: ^C Mail01/ETEC, QP01/ETEC,	
STOT/ETEQ_	
I	
	A Disconnected

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.

nter Import F	ile Name	>
Enter the path to	the WebSphere LTPA Import file:	ОК
c:\ltpa.key	I	Cancel

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



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

figuration	×
ported WebSphere	e LTPA keys.
	figuration ported WebSphere OK

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.

😔 Web SSO Configuration - I	Oomino Administrator		
File Edit View Create Actions	Text Help		
] ◇日 母)]⊀��①]		B I 🌶 ≣ 🗄 🗄 🚟 ∗ 🗄 🛵 📼	0 🔁 🗛 💝 🛄
] (+ + 🙆 (+			
🔫 ETEC Domain 📳 Web	SSO Configuration ×		
🙀 🚡 Save and Close 🔒	Keys		
Web SSO Co	nfiguration for :	Long 30	re e
Basics Administration		in age	2
		* 2 1	- 5 8
Token Configuration		Token Expiration	
Token Name:	LtpaToken	Expiration (minutes): ¹⁷ 30 J	
Token Domain:	^r rchland.ibm.com _		
Participating Servers			
Domino Server Names:	^{IF} Mail01/ETEC, QP01/ETEC, ST01/ETEC ⊒		
WebSphere		Í.	
LDAP Realm:	^r mail01.rchland.ibm.com\:389 _		
LTPA Version:	1.0 T		
			•
	•	Etec	•

- 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**.

E IBM WebSphere Portal - Microsoft	Internet Explorer		
File Edit View Favorites Tools H	elp		A.
🕝 Back 🝷 🜍 - 💌 😰 🏠	Search 🔶 Favorites	Nedia 🧭	8 - 🕹 🖬 📮 *
WebSphere Portal			? Log out 🔺
Page Properties New page:Instant Messaging and We	eb Conferencing		
Title: Lotus Notes	n na dharta dhadh na		=
I want to make this page my priv	vate page		
4			~
🕘 Done			🌍 Internet 👘

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

File Edit View Equaritee Teels L	Jola	
File Eult view Pavorites 100IS F		-
🎯 Back 🝷 🐑 🔺 🗾 🐔) 🔎 Search 🥎 Favorites 🜒 Media 🧐 🔗 - 🌺 🔜 🛄 🎇	
/ebSphere Portal	? Log o	ut
Content Appearance Locks		
lit Layout	7 / ? - 1	
Page title: Lotus Notes		
Page title: Lotus Notes		
Page title: Lotus Notes		
Page title: Lotus Notes	+ Add portlets	
Page title: Lotus Notes	+ Add portlets	
Page title: Lotus Notes	+ Add portlets ms added to this container	
Page title: Lotus Notes	Add portlets ms added to this container	
Page title: Lotus Notes	Add portlets Ms added to this container Edit properties Delete this page	

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**.

街 IBM WebSphere Portal - Microsoft Interne	t Explorer				- D X
File Edit View Favorites Tools Help					.
🕞 Back 👻 🐑 - 💌 🗟 🏠 🔎 S	earch 😽 Favorites	🜒 Media	🖉 - 🍃	P	íð.
Edit Layout				1116	7/? ^
Search on: Title contains Search for: Sametime Search					
Showing 1 - 2 of 2 Page 1 of 2					
Select Portlet Title Unique	ame				=
Lotus Sametime Connect					
My Lotus Sametime Connect					
Showing 1 - 2 of 2 Page 1 of 2					
OK Cancel					×
E Done				Internet	

Elle Edit View Esverites Tools Help		
Back • 🕑 • 💌 😰 🏠 🔎 Search 🤶 Favorites 📢 Media 🍕	🔊 🔗 - 🍃 📄 🗖	12
Edit Layout	1116	7/? ^
 Search on: Title contains ▼ Search for: QuickPlace Showing 1 - 2 of 2 Page 1 of 1 Select Portlet Title Unique name Lotus QuickPlace Lotus QuickPlace Showing 1 - 2 of 2 Page 1 of 1 OK Cancel 		
		¥
Cone Cone	🧐 Internet	

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**.

IBM WebSphere Portal - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	an a
🔇 Back 👻 🚫 - 💌 😰 🏠 🔎 Search 👷 Favorites	🕙 Media 🔗 🍃 🎆
APCL0115I: New portlets are added successfully.	
Edit Layout and Content allows you to add and arrange portlet columns and rows. Modifications occur as you make them. Page title: Lotus Notes	s, columns and rows. You can also remove portlets,
Lotus Sametime Connect	Lotus QuickPlace
Done Ed	it properties Delete this page

😏 Back 🝷 💟 👘 본 😰 🕥 🔎 Search 🍸 Favorites 🎈	Media 🚱 🔗 😓 🔜 🚺	a
lebSphere Portal	My Portal Administration 🕂 Edit	: my profile ? Log out 🦄
Welcome Documents My Work My Finances My Newsroom	<u>New Page</u> <u>Edit Pa</u> Collaboration	<u>1e Assign Permissions</u> My Favorites
vius Sametime Connect	Lotus QuickPlace	/ ? - 0
LOUUS. Sametime	LOUUS. QuickPlace	
	Create a new QuickPlace	

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**.

El IBM WebSphere Portal - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	A*
😮 Back 🔻 🐑 - 😰 😭 🔎 Search 👷 Favorites 🜒 Media 🤣 🔗 - 🌺 🚍	, 12
WebSphere Portal Administration +	Edit my profile ? Log out 🛆
New Page Edi	it Page Assign Permissions
Welcome Documents My Work My Finances My Newsroom Collaboration	My Favorites 💙
Lotus Sametime Connect	4 7 - 8
Customize Sametime Enter your Sametime server name and port number. Server name: st01.rchland.ibm.com Server port: 1533 (Default: 1533)	
E Done	🔮 Internet

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

🕘 Lotu	us Sametime Conn 💶 🛙	
People	Meeting Options Help	
Qd		8
E 8+8 ×	Work wpsadmin	
■ Iam Connect	n Active ted	

- 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**.

IBM WebSphere Po	rtal - Microsoft Internet Explorer	
File Edit View Fav	vorites Tools Help	
🚱 Back 🔹 🕥 -	🖹 🗟 🏠 🔎 Search 👷 Favorites 📢 Media 🤣 🔗 - 🌄 🎉	
WebSphere Portal	New Page Edit Page /	Assign Permissions
Welcome My W	fork My Finances My Newsroom Collaboration My F	avorites 💌
Web Access Samet	ime and QuickPlace	
Lotus QuickPlace		< ? - ₽
You may enter up to s Default QuickPlace crea Name	ix QuickPlace URLs. These will be displayed in the instance and will launch the QuickPlaces. ation URL: http://www.lotus.com/home.nsf/welcome/quickplace URI	
test1	http://qp01.rchland.ibm.com	
NE		

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

E IBM WebSphere Portal - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	an a
🚱 Back 🔹 🕥 - 💌 😰 🏠 🔎 Search 🤶 Favorites 📢 Media 🧔	9 🔗 💺 🖃 🛄 🛍
WebSphere Portal	My Portal Administration 🕹 Edit my profile ? Log out 🛆
	New Page Edit Page Assign Permissions
Welcome My Work My Finances My Newsroom Collaboration Web Access Sametime and QuickPlace	My Favorites 💌
Lotus Sametime Connect / ? - 🗆	Lotus QuickPlace 🥒 ? - 🗆
Lotus. Sametime	Lotus. QuickPlace Select a QuickPlace
Domino Web Access changed	test1 V Q
Please customize your Domino server information.	Create a new QuickPlace
ê	🔮 Internet

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.

🖹 IBM WebSphere Portal - Microsoft Interne	et Explorer		
File Edit View Favorites Tools Help			a da se d
🚱 Back 👻 🐑 👻 🛃 🌈	Search travorites 🜒 Media	🚱 🍛 🗟 · 실 🛍	
and a state of the			New Page Edit Page Assign Permissions
Welcome My Work My Finances	My Newsroom Collaboration	DWA	My Favorites
Notes			
Domino Web Access			(? - B)
Functional Area:	Start with:		Instance number:
All	Mail	~	1
Application title:			
Domino Web Access	Hoight:		
	neight:		
O pixels	300 pixels		
Source:			
Automatically find my mail database			
Citet me manually select my mail database	2		
HTTPS (SSL)			
Oetect protocol automatically			
Use reverse proxy server			
O on the WebSphere Portal Server			
• on this proxy server:			
Port:			
✓ Use the Domino server name as the re-	verse provy junction name		
Protocol:			
• HTTP			
O HTTPS (SSL)			
Detect protocol automatically			
Save Cancel			
Done			🥥 Internet

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

E IBM WebSphere Portal - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🚱 Back 🔹 🐑 🔹 🛃 🏠 🔎 Search 🤺 Favorites 🜒 Media 🤣 🔗 - 💺	🗟 - 🛄 🛍
WebSphere Portal	ortal Administration 🕂 Edit my profile ? Log out 🛆
	New Page Edit Page Assign Permissions
Welcome My Work My Finances My Newsroom Collaboration	My Favorites
Domino Web Arress	/ 7 - 0
INOTES WED ACCESS. Inbox	
New Reply Forward Refresh Move Delete Mark Read	
Who Date Size Subject	Go to **
Notes Administrat(12/30/2003 1220 You are invited to join test1 Notes Administrat(12/23/2003 684 test	
, and the second s	
a	Internet

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\<instancename>\PortalServer5\config directory before beginning.
- 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\<instancename>\PortalServer5\config\helpers directory.
- 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=ETEC

WasPassword=wpsadmin

WpsHostName=rchland.ibm.com

Portal Config Properties - BEGIN

PortalAdminId=cn=wpsadmin,o=ETEC

PortalAdminPwd=wpsadmin

#WebSphere Portal Security LTPA and SSO configuration

LTPAPassword=wpsadmin

SSODomainName=rchland.ibm.com

LDAP Properties Configuration - BEGIN

LDAPHostName=Mail01.rchland.ibm.com

LDAPAdminUld=Notes Admin

LDAPAdminPwd=password

LDAPBindID=cn=wpsadmin,o=ETEC

LDAPBindPassword=wpsadmin

Advanced LDAP Configuration – BEGIN

LDAPUserSuffix=o=ETEC

- 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:



- 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 at 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.