



**Administrator's Guide**

## **Disclaimer**

THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS DOCUMENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS DOCUMENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS DOCUMENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENT GOVERNING THE USE OF IBM SOFTWARE.

## **Licensed Materials - Property of IBM**

©Copyright IBM Corporation 2004 All rights reserved.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GS ADP Schedule Contract with IBM Corp.

Lotus Software  
IBM Software Group  
One Rogers Street  
Cambridge, MA 02142

## **List of Trademarks**

IBM, the IBM logo, 1-2-3, AIX, AS/400, DB2, Domino, Domino Designer, Domino.Doc, Freelance Graphics, iNotes, iSeries, LearningSpace, Lotus, Lotus Discovery Server, Lotus Enterprise Integrator, Lotus Notes, Lotus Organizer, MQSeries, Netfinity, Notes, OfficeVision, OS/2, OS/390, OS/400, S/390, Tivoli, QuickPlace, Sametime, SmartSuite, WebSphere, and Word Pro are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Pentium is a trademark of Intel Corporation in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

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

---

# Contents

<b>1 Planning for WebSphere Portal in a Domino Environment</b> .....	1
Domino and Extended Products with WebSphere Portal .....	1
Planning for WebSphere Portal in a Domino environment .....	2
Planning for LDAP .....	3
Configuring LDAP Search in Portal and the Lotus products .....	6
LDAP user directories — one or multiple? .....	7
Planning for single-sign on .....	8
Planning scale and user communities .....	10
Planning security .....	10
Planning for high availability of servers .....	11
Other planning considerations .....	12
Guidelines for upgrading Domino and Extended Products .....	14
<b>2 A Pilot Configuration for Domino Extended Products and WebSphere Portal</b> .....	17
A pilot configuration for Domino Extended Products and WebSphere Portal .....	17
Installing WebSphere Portal .....	20
Installing Domino on the Team Workplace system — Critical steps .....	21
Installing Domino Administrator — Critical steps .....	22
Configuring LDAP .....	23
Specifying Domino server configuration settings for LDAP .....	23
Adding WebSphere administrators to the Domino Directory .....	26
Updating access control in the Domino Directory .....	27
Configuring WebSphere Portal for LDAP and enabling security .....	27
Installing Team Workplace .....	29
Configuring Team Workplace .....	30
Configuring the ability to search across team workplaces .....	34
Installing Domino Document Manager .....	36
Configuring Domino Document Manager .....	38

Setting up Lotus Workflow .....	41
Installing Domino on the Sametime system — Critical steps .....	42
Installing Sametime — Critical steps .....	43
Configuring Domino Administrator for use in two Domino domains .....	45
Additional LDAP configuration for Sametime .....	46
Configuring Sametime to support WebSphere Portal .....	49
Configuring SSO between WAS, Domino, and Domino Extended Products .....	50
Enabling SSO for WebSphere Application Server .....	51
Configuring SSO for Team Workplace .....	52
Configuring SSO for Sametime .....	56
Configuring WebSphere Portal for Domino extended products .....	58
Installing the Notes/Domino and Extended Products Portlets .....	59
Configuring the Notes/Domino and Extended Products Portlets .....	63
Setting up awareness and chat for Team Workplace .....	65
Setting up Web conferencing for Team Workplace .....	68
Setting up awareness and chat for Domino Web Access .....	72
Setting up awareness and chat for the Notes View portlet (Domino Databases) .....	74
<b>3 Troubleshooting</b> .....	75
Troubleshooting in the Domino-Portal Environment .....	75
Troubleshooting strategy .....	78
Troubleshooting a lack of Sametime awareness in portlets .....	80
Turning on LDAP tracing .....	81
Turning on HTTP tracing for the Domino Web server .....	82
Turning on DIIOP logging in Domino .....	83
Known issues .....	83
<b>4 Domino Application Portlet Reference</b> .....	87
Domino Application Portlet Reference .....	87
Installation .....	89
Configuration .....	94
Authentication in Domino .....	99
Authentication in WebSphere Portal .....	100
Caching .....	102
Transformation rules .....	104

Regular expression rules	105
Output functions	108
HTML rules	110
Troubleshooting	112
<b>5 Single Sign-on — Scenario for Using Non-Domino LDAP with Domino</b>	
Single sign-on — Scenario for using non-Domino LDAP with Domino	115
<b>Index</b>	123



---

# Chapter 1

## Planning for WebSphere Portal in a Domino Environment

This chapter introduces Lotus Domino and Extended Products 6.5.1 and WebSphere Portal 5.0.2, and discusses planning considerations, and offers general guidelines for upgrading from earlier Domino products.

---

### Domino and Extended Products with WebSphere Portal

This guide provides information on using IBM® Lotus® Domino™ with its extended family of products, as well as with WebSphere® Portal 5.0.2. The extended products include:

- Lotus Team Workplace — formerly QuickPlace®
- Lotus Instant Messaging and Web Conferencing — formerly Sametime®
- Lotus Domino Document Manager — formerly Domino.Doc®
- Lotus Workflow™ — formerly Domino Workflow

If you are adding WebSphere Portal to your environment, you will want to download the Lotus Notes®/Domino and Extended Products Portlets 6.5.1 from the WebSphere portal catalog at [https://www-306.ibm.com/services/cwi/portal/\\_pagr/105](https://www-306.ibm.com/services/cwi/portal/_pagr/105). These portlets come with sample portal pages that present users with a Lotus Workplace-like experience by integrating all core messaging and collaborative applications into a portal user interface (UI). The sample pages show how users in a portal environment can collaborate using portlets that rely on Notes/Domino and its extended products. Thus, the new release of Notes/Domino 6.5.1 is a bridge to the world of J2EE and open standards, extending Domino's capabilities by providing the means to connect different sources of data, regardless of vendor.

Both new and updated portlets are provided. These include standard Notes and Domino features such as e-mail, calendar and scheduling, discussion, teamrooms, and to-dos, as well as the Notes View capability that lets you work with the documents from any view of any Notes database. Portlets based on extended products let you conduct Web conferences, manage documents, see a list of your team workplaces, find people in your company directory, use other Domino applications as portlets, and more.

Starting with 6.5.1, versions of all of our Domino-based products are synchronized — meaning all version 6.5.1 products support each other and ship in the same time frame — helping to streamline your upgrade strategy. This guide helps you plan for a portal-Domino environment and guides you through installing and configuring all the components, using simplified procedures tailored to a pilot situation.

As with all portal solutions, the sample portal pages are easily customizable and allow you to manage user access with policies.

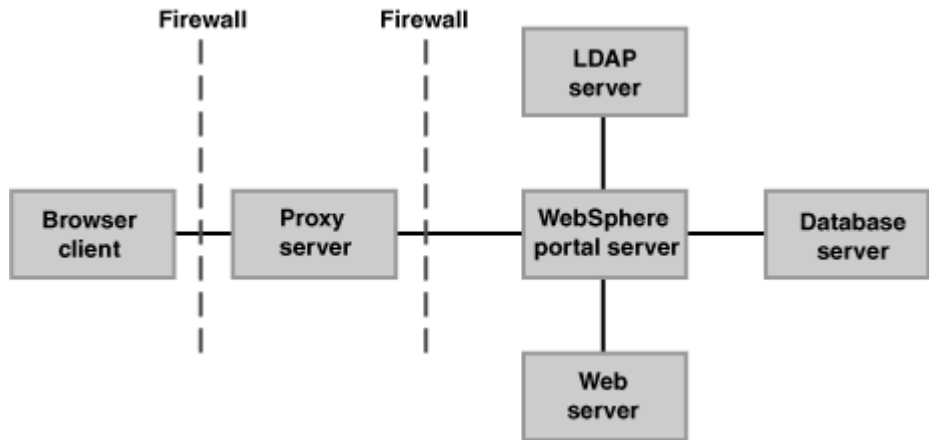
The sample portal pages bring together all of Notes/Domino and extended products portlets in one package so that you can quickly bring the power of Lotus collaboration, integrated into a single UI, to everyone with access to a Web browser. There are additional portlets in the Portal Catalog, where you can download many of the hundreds of portlets available at no charge.

---

## Planning for WebSphere Portal in a Domino environment

IBM WebSphere Portal server provides browser users with a single entry point for all their corporate applications. It is built on an open, non-proprietary computing framework, incorporating support for Java(TM), XML, Linux and emerging Web services standards, which allow ease of integration with existing systems and applications, regardless of vendor. Added to a Domino environment, the Portal server can be used to extend Domino's capabilities by providing the means to connect different sources of data. Users log on to Portal and collaborate using various Domino-based portlets that rely on the Domino server or one of the extended products servers for their data.

The standard (non-programming) Portal offering can work with various LDAP suppliers, reverse proxy and security providers, and database suppliers, and supports J2EE applications from any source. With adequate knowledge and planning, you can customize the Portal environment in a wide variety of ways.



To exploit the full resources of the Portal, you can write your own J2EE applications. Be aware, however, that the J2EE development environment requires training, for the following reasons:

- The J2EE environment may be new to your Domino Designer developers
- J2EE uses open standards, and is thus capable of supporting products and components from many sources, making it complex
- The J2EE environment is richer than Designer's, increasing the likelihood of mistakes

Planning is essential before deploying Portal in your Domino production environment. To help you plan, see the following topics:

Planning for LDAP

Planning for single sign-on

Planning scale and user communities

Planning for security

Planning for high availability of servers

Other planning considerations

**Note** This guide is not intended to serve as complete documentation for WebSphere Portal. Such documentation is available in the WebSphere Portal InfoCenter at <http://publib.boulder.ibm.com/pvc/wp/502/index.html>.

---

## Planning for LDAP

When users first log in to Portal, the user name and password they provide are checked against those in the Portal's user repository — usually an LDAP directory that the Portal has been configured to work with.

## LDAP directory structure

During Portal configuration, you will need to set values in a properties file so that Portal will know about your LDAP structure, since it has to write and read from it. If your company does not already have an LDAP structure in place, you need to plan it carefully.

In the Portal properties file, for the property “LdapUserPrefix,” you enter the value “uid” or “cn”, depending on which form your LDAP directory uses for the user’s distinguished name (DN).

If you are using the Domino LDAP service, you determine the form for the user’s LDAP DN attribute by how you fill in the fields in the Person document in Domino. Essentially, Domino maps the first line in the FullName field to the LDAP DN entry. For example, if you want the DN to be the uid, you must enter the uid in the first line of the FullName field (and also in the ShortName field). If you want the DN to be cn, enter the user’s Notes hierarchical name in the first line of the FullName field, and Domino considers everything before the first slash to be the cn.

For more information on how Domino maps fields in the Person document to LDAP attributes, see the topic “The Domino LDAP schema” in Lotus Domino Administrator 6.5.1 Help.

## WebSphere Portal considerations

Make sure you plan for the following if you will use WebSphere Portal server with LDAP:

- If WebSphere Portal uses a Domino server as the LDAP server, you must have entries in the Domino Directory for every level of hierarchy that includes an entry. For example, if you have user entries that look like this: cn=John Doe, ou=Boston, o=Lotus, you must have an entry in the directory for ou=Boston and o=Lotus. If you have used Notes registration to add users, you probably already have the necessary hierarchy for successful LDAP searching. However, if you manually created hierarchical user entries from the Notes user interface, and if these user entries contain a hierarchy different from that of the certifiers found in the directory, the entries are considered “orphan” entries (they have no parent hierarchy.) To resolve this issue by creating the necessary parent entries in a hidden view, run the following command from the Domino Administration Server console:

```
TE LDAP VerifyDIT
```

For more information on this command, see Lotus Domino Administrator 6.5.1 Help.

- When LDAP access is configured for WebSphere Portal administration or for People Finder lookup, the administrator can specify a user and password for LDAP binding (authentication). It is important to match this user's ACL entries in the Domino Directory with the requirements for accessing the portal. As examples, (1) if this user does not have write access to the Domino Directory, the sign-in feature of WebSphere Portal will not work, and (2) if the user does not have access to some parts of the directory tree, People Finder may experience problems doing LDAP searches.
- WebSphere Portal does not support a Domino LDAP that has been configured with Directory Assistance.
- A large number of nested groups in the LDAP directory can cause delays in the management of resource accesses by the Portal Administrator, who controls access to portlets and pages by adding users or groups to a role. Making additions to a role makes calls to LDAP to list every group in the directory before the administrator can continue.
- A large number of nested groups in the LDAP directory on a small LDAP server can cause a user login to the Portal server to time out before Portal can finish looking up every group that the user belongs to in the default time of 2 minutes.

If you think you might encounter the preceding problem with your directory, refer to Technote 1144006 at <http://www.ibm.com/support> for a possible solution.

### **Sametime considerations**

- Configure all Sametime servers to use the same directory so that all users will have awareness of each other.
- If your plans include using Sametime with an LDAP directory, configure Sametime for LDAP from the start. This avoids the Sametime contact lists not working when you migrate a Sametime server from Domino Directory to LDAP. If you find you do have to migrate your contact lists, there is a tool that converts your contact lists from Domino authentication format to LDAP format — see the Lotus Instant Messaging (Sametime) Buddy List Conversion Utility on [www.lotus.com/idd](http://www.lotus.com/idd).

### **Portlet considerations**

Many portlets do LDAP lookups in order to perform automatic configuration. Automatic configuration only works if you allow anonymous lookups and make the attributes available for anonymous lookup, or configure a bind user ID and password.

- The Domino Web Access portlet needs anonymous access to the MailServer, MailFile, and HTTP-HostName attributes.
- The Lotus Notes View portlet and the Domino Portlet Builder need Server documents to have anonymous access and be in the LDAP directory in order for the portlets to list servers.

For more information on LDAP configuration settings in Domino 6.5.1, see the WebSphere Portal InfoCenter topic *Configuring WebSphere Portal for Domino Directory*.

Alternatively, you can configure the portlets manually.

### **Configuring LDAP Search in Portal and the Lotus products**

Each product that uses LDAP to locate a person record must submit an LDAP search using the string entered by an end user. Examples of cases in which components submit LDAP searches are the user's first login to Portal server, Sametime, or Quickplace; adding a person to the instant messaging contact list; adding a person or group to a team workplace; and Sametime checking a user's online status. The LDAP search string for Portal, Sametime, and Team Workplace is configured separately in each product.

Problems can arise if a product's default LDAP search string does not support the way the user is entering the user ID. For example, the default search string in Team Workplace supports IDs that have both a first and last name. Adding a new user to a team workplace will fail if the user's name is entered as a single name, such as `wpsadmin`, in the search box of the directory dialog. (The LDAP search fails.) The fix is to modify the LDAP search string.

To modify the search filter for these products, see the following references.

<i>Product</i>	<i>Reference for configuring LDAP Search</i>
WebSphere Portal	See the topic “Configuring WebSphere Portal for LDAP” in the Portal 5.0.2 InfoCenter.
Lotus Domino	See the topic “ldapsearch Utility,” in IBM Lotus Domino 6.5.1 Administration Help  <b>Note</b> You do not have to use ldapsearch from a machine that uses the Domino LDAP service.
Lotus Team Workplace	See the topic “Customizing search filters” in the IBM Lotus Team Workplace 6.5.1 Administrator’s Guide
Lotus Sametime	See the topic “Configuring the LDAP Searching setting” in the IBM Lotus Instant Messaging and Web Conferencing 6.5.1 Administrator’s Guide  <b>Note</b> When the Lotus Notes client is configured for instant messaging, but the Lotus Instant Messaging (Sametime) server is using a non-Domino LDAP directory, the Notes hierarchical form (“John Smith/Boston/Acme”) of the name must exist as a searchable attribute in the directory that the Sametime server uses. If the Sametime server is version 3.0 or 3.1, you need to modify the LDAP search filter to include the hierarchical name. In Lotus Notes 6.5.1, the administrator can push down a user preference setting for using the canonical name for instant messaging status lookups, which makes modifying the LDAP search filter unnecessary.
People Finder portlet	People finder uses the WebSphere Member Manager to contact LDAP. For more information, see the WebSphere Portal InfoCenter topic People Finder configuration mode.

## LDAP user directories — one or multiple?

It is best to have a central LDAP directory for all users, because it allows the most commonly performed administrative task — adding and modifying user names — to be done only once, thereby lowering administrative costs.

The use of multiple directories increases administrative costs and can introduce complexities into the Domino-Portal environment, but can be made to work if you understand how to avoid problems resulting from the multiple identities that users have in different directory structures. Setting up single sign-on (SSO) in a Domino-Portal environment with multiple user identities is complex.

As an example, WebSphere Portal in a Domino environment is configured to work with the corporate LDAP directory, which contains records on all users in the company. The Domino Directory contains records of only the company's Lotus Notes users. SSO is configured on both the Portal server and on the Domino servers. When a user logs in to Portal, the user information stored in the LTPA cookie is in a format consistent with the schema for the LDAP directory. If this format is different than that of the Domino Directory, Domino will not be able to authenticate the user when they access a portlet.

For possible solutions, see the chapter “Single sign-on — Scenario for using non-Domino LDAP with existing Domino.”

---

## Planning for single-sign on

In WebSphere Portal server, authentication for backend applications can be handled by one or more of the following single sign-on (SSO) mechanisms: the Portal's Credential Vault, Lightweight Third-Party Authentication (LTPA), or an external product that uses a DSAPI filter. For example, when a user first logs in to Portal, the credentials he provides are stored in an “LTPA cookie” in the user's Web browser, and then passed to backend applications (such as Lotus Domino) so that users are not challenged to authenticate with each application.

The Portal server's Credential Vault is an encrypted database table that stores user names and passwords that can be accessed by portlets. For a portlet to be able to access the vault when it connects to a backend application, the portlet must have special coding.

Both WebSphere Portal and Lotus Domino can use LTPA for single sign-on. When Portal and Domino are used in the same environment, you export a secret key from Portal to Domino, which all servers can then use in order to authenticate users. When a user logs in to the Portal, an LTPA cookie, containing the token, is generated in the user's browser; when the user then accesses a Domino-based portlet, the Domino server authenticates the user by decrypting the token in the cookie.

As an alternative to LTPA in your Domino environment, you can implement SSO across Web-based applications using a product like Netegrity SiteMinder or Tivoli® Access Manager. Such products use DSAPI (Domino Server API) to essentially replace Domino's authentication process.

For guidelines on implementing SiteMinder on Domino, Lotus Team Workplace, and Lotus Instant Messaging and Web Conferencing (Sametime), see the article “Netegrity SiteMinder and Domino-based collaborative services” on [www.ibm.com](http://www.ibm.com).

**Notes:**

- It is best to use Netegrity SiteMinder or Tivoli Access Manager only for WebSphere Portal authentication, not authorization.
- To use Tivoli Access Manager (TAM) with WebSphere Portal and Domino and Extended Products 6.5.1, a TAM LTPA junction should be used. In this situation, it is not necessary that all servers that participate in SSO be in the same Internet domain.
- When planning to use any product that interacts with WebSphere Portal and Domino, always check with the product vendor about supported versions and configurations.

**LTPA planning considerations**

- To participate in SSO, servers must be in the same Internet domain.
- Servers may be in different Domino domains. If this is the case, you must create a Web SSO configuration document on one server in each Domino domain. You must edit the Server document for every Domino server that participates in SSO.
- Within a Domino domain, to use SSO, either all servers must use the Internet Sites feature, or no servers use the feature. Since you must create only one Web SSO configuration document to handle SSO for the Domino domain, and since this document cannot be filled out to include both servers using Internet Site documents and those not using them, you cannot mix the two approaches in an SSO environment.
- Lotus Team Workplace (QuickPlace) 6.5.1 and Lotus Instant Messaging and Web Conferencing (Sametime) 6.5.1 do not support the Domino Internet Sites feature. Therefore, for Domino domains in which there are Team Workplace or Sametime servers, you must leave the Organization field in the Web SSO configuration document blank. (Filling in the field causes the document to appear in the Internet Sites view instead of the Web Configurations view.)
- To successfully install Lotus Team Workplace after SSO is enabled, you must follow the instructions in the chapter “Setting Up Security” in the *Lotus Team Workplace Administrator’s Guide*.
- Installing Sametime does some automatic SSO setup, but not in a way that can be used with WebSphere Portal. You will need to replace the Web configuration document generated during Sametime install with one you create.
- If your organization has the multiple identity problem, setting up SSO is complex.

See the chapter “Single-sign-on — Scenario for using non-Domino LDAP with existing Domino” for possible solutions to the multiple identity problem.

---

## Planning scale and user communities

How you configure directories in your environment (whether you have one central LDAP directory or multiple directories) affects how your users interact — what other users they can chat or have online meetings with, what team workplaces they can be members of, what other users they can locate with the People Finder portlet, and so on. Consider whether your organization will function best as a collection of smaller groups, or as one large group, in which case you might be able to gain the cost savings of having a central LDAP directory.

If your current administrative structure does not lend itself to central management of services, consider changing it so that you can take advantage of the lower costs associated with centralized configuration and administration of your computer infrastructure.

---

## Planning security

Use the following guidelines to get started planning security for Domino in a Portal environment:

- Decide whether WebSphere Portal will allow automatic sign-in by (unauthenticated) users. If you allow automatic sign-in, any user can create Person documents in your LDAP directory, and the LDAP user you configure must have write access to the LDAP directory. If you decide not to allow automatic sign-in, disable it either by not allowing the LDAP user write access to LDAP or by modifying the JSP in which the sign-in is displayed, removing the user interface for it.
- Decide whether to manage LDAP users and groups exclusively from the LDAP side, or to also use the WebSphere Portal Administration portlet to manage them. If you don't want to use the Administration portlet, limit the LDAP user's access to the directory to read-only.
- For the security of each backend application, set up firewalls and DMZs. Designate reverse proxy servers and test before deploying.

- Be aware that you need to manage access control in each of these products: Domino, Team Workplace, Document Manager, and Portal. Adding a user to the environment involves modifying a series of groups in addition to the LDAP directory, and must be carefully planned. As administrator, you must establish the process to add or remove a user in your specific environment. For example, in a Domino-Portal environment in which WebSphere Portal and Sametime both use Domino LDAP and user administration is done from the Domino side, your process for adding a new user would be as follows:
  - a. Use Domino Administrator to add the new user. The user can now log in to WebSphere Portal.
  - b. Add the user to the appropriate user groups. If WebSphere Portal's resource access is managed by groups in LDAP, there are no steps to complete on the Portal side — membership in the proper group gives the user access to the proper portlets and resources.
  - c. If the user will be a member of one or more team workplaces or will access Document Manager libraries, use the administrative interface for that product to add the user, or use groups to add the user automatically, as in step b.

**Note** The user is automatically a member of the Sametime community.

- Consider using an external security manager such as Tivoli Access Manager or Netegrity SiteMinder for authentication. When using external authentication, WebSphere Portal can exist as part of a larger single sign-on infrastructure that is provided by the external security manager.
- Determine which connections between servers are a security risk for your organization, and consider enabling the Secure Sockets Layer protocol (SSL) on them. (SSL provides encrypted transmissions to ensure that data remains confidential.) Since enabling SSL is resource intensive and involves setup/testing in each software product, you may want to limit it to the connection with the highest risk — that from the browser to the firewall — and let physical security suffice for the machines behind the firewall. Make sure you set up each product without SSL first, test the product, enable SSL, and then test the product again — one connection at a time.

---

## Planning for high availability of servers

If the nature of your business requires an uninterrupted level of service, planning for high availability of the Domino, LDAP, Sametime, and Portal servers, as well as of the reverse proxy servers within the firewall or DMZ, is essential.

- Set up Domino clusters to provide failover for Notes clients.
- WebSphere Portal can have awareness of only one LDAP server. To provide failover for the LDAP server, add a network splitter such as the IBM Edge Server to your environment, configure it as the LDAP server for Portal, and then set up multiple LDAP providers behind the Edge Server.
- Most HTTP services also require a network splitter to provide failover to a set of machines.
- Sametime uses HTTP for some clients and a TCP/IP port for other clients. For Sametime high availability, set up a MUX (acts like a network splitter) and multiple Sametime servers.
- WebSphere Application Server, on which the Portal server runs, includes WebSphere Application Server Network Deployment , which has a built-in server clustering technique. For information on installing WebSphere Portal server in a cluster, see the InfoCenter topic “Installing WebSphere Portal in a cluster environment.” Enhanced support of Network Deployment is planned for Portal Server 5.x.

For more information on high availability for WebSphere Application Server, see *IBM WebSphere V5.0 Performance, Scalability and High Availability* at [www.redbooks.ibm.com](http://www.redbooks.ibm.com)

---

## Other planning considerations

Note these considerations if you are planning on adding the following extended products to your Domino environment.

### Lotus Team Workplace

- If you plan to deploy both Team Workplace (QuickPlace) and Instant Messaging and Web Conferencing (Sametime), there are benefits to setting up each server in its own Domino domain, and letting them share a common LDAP directory. Each of these powerful applications places numerous requirements on the configuration of the Domino server. You reduce the chance of a conflict in these requirements if you run these two applications outside of the production Domino domain. Cross-certification of the domains is not required.

## **Lotus Instant Messaging and Web Conferencing**

- If you plan to deploy both Instant Messaging and Web Conferencing (Sametime) and Team Workplace, there are benefits to setting up each server in its own Domino domain, and letting them share a common LDAP directory. Each of these powerful applications places numerous requirements on the configuration of the Domino server. You reduce the chance of a conflict in these requirements if you run these two applications outside of the production Domino domain. Cross-certification of the domains is not required .
- Hosting Web applications on a Domino server that also hosts Sametime can confuse users when they try to access a Web application. Instead of the Domino Web Server authentication screen, they see the Sametime logon screen. Completing the Sametime screen, however, does allow them to access the Web application.

## **Lotus Domino Document Manager**

- If you are using LDAP, a dedicated Domino server is required for Domino Document Manager (Domino.Doc), as LDAP lookups are done using a directory referenced by Directory Assistance on the server on which Document Manager is installed.
- If you want to install more than one Document Manager master server in a Domino domain, you need to change two of the group names (Domino.Doc Site Administrators and Domino.Doc Servers) for the second installation. For a Technote that tells you how to do this, search on 7003550 (the Technote number) at [www.ibm.com/support](http://www.ibm.com/support).
- To ensure that users can access the Document Manager “Who Is Online” feature, Lotus Instant Messaging and Web Conferencing must be configured correctly. The Lotus Instant Messaging and Web Conferencing (Sametime) server must be separate from the Document Manager server, and the Sametime Secrets database (STAuthS.nsf) and Tokens database (STAuthT.nsf) must be replicated to the Sametime server’s data directory (typically c:\lotus\domino\data) on both the Document Manager master server and replica server.

## **Lotus Domino Web Access**

- When SSL is enabled, the Domino Web Access (iNotes™) portlet does not detect the protocol until you select the HTTPS protocol in the portlet configuration.

- For Sametime awareness to work with the Domino Web Access portlet, if the Sametime server and the Domino server are in different Domino domains, the domains must be cross-certified. To configure Sametime to work with Domino Web Access, use both the Lotus Domino 6.5.1 Administration Help and the Domino 6.5.1 Release Notes, as the release notes contain essential information.

**Tip** To avoid having to record the host name of the Sametime server in each user's Person document, use the NOTES.INI setting `iNotes_WA_SametimeServer=host name`, where *host name* is the fully qualified domain name of the Sametime server.

### People Finder portlet

- To display photographs of people in People Finder, you must use an external LDAP administration tool to store the jpegPhoto LDAP attribute in the LDAP directory for each person.

---

## Guidelines for upgrading Domino and Extended Products

The individual documentation for each of the products in a Domino-Portal environment includes a section on upgrading that product to the current release from a previous release. This topic provides general guidance for when you plan to upgrade multiple products.

### Upgrade considerations

In general, when a new version of a product is released, it is tested with and supports the newest version and at least one version back of each product that it interacts with. For example, WebSphere Portal version 5.0.2 supports the LDAP directory provided by Domino 6 as well as the LDAP directory provided by Domino 5. Similarly, it is not possible to test a product against the versions of other products with which it might interact in the future.

Since upgrading each product in the Domino extended family is normally done over a period of time, it is important that the overall configuration keep working after you perform each upgrade. Therefore, it is essential to check the individual product documentation of each product to be upgraded for the specific versions of other products supported in each case.

For example, because WebSphere Portal 5.0 was released before Domino and Extended Products 6.5.1, it was not tested with the 6.5.1 products. If you are running WebSphere Portal 5.0 and were to upgrade your Domino products to 6.5.1, you would risk your Portal 5.0 installations not working properly.

## **Upgrade strategy**

- 1.** Plan the entire configuration before you start upgrading.
- 2.** If you plan to upgrade multiple products, address any order-of-upgrade issues by doing the following:
  - a.** Check the individual product documentation to make sure all requirements for a product are met before you install it. If you need to install a prerequisite first, make sure all requirements for the prerequisite are met.
  - b.** Refer to Technote 1162481 at [www.ibm.com/support](http://www.ibm.com/support) for important information on supported configurations and planning your upgrades to Domino and Extended Products 6.5.1.
- 3.** Delay using new server features until all the upgrade steps are complete. For example, if you want to enable extended ACLs — a Domino 6 feature — in your Domino Directory, Domino 5 does not support this feature. It is best to wait until all servers are upgraded to Domino 6 before the feature is enabled.



---

## Chapter 2

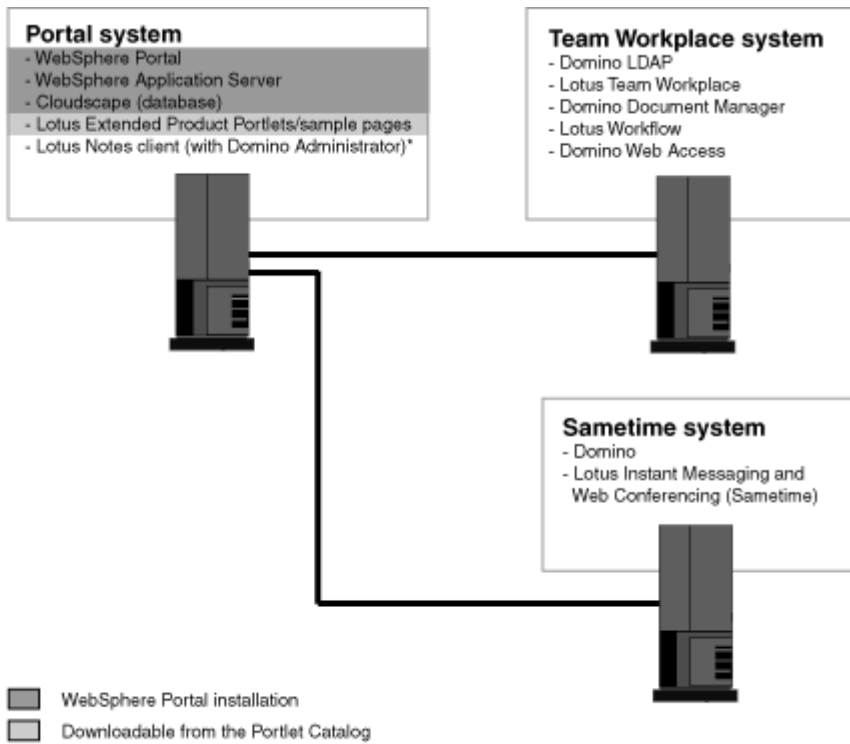
# A Pilot Configuration for Domino Extended Products and WebSphere Portal

This chapter describes how to install and configure WebSphere Portal, Domino and Extended Products, and the Notes/Domino and Extended Products Portlets in a three-machine pilot configuration.

---

### A pilot configuration for Domino Extended Products and WebSphere Portal

Domino and Extended Products servers can provide data to Lotus Domino-based portlets. WebSphere Portal is the base component that allows you to use those portlets. Since deploying Domino Extended Products and WebSphere Portal in a production environment is a major undertaking, this guide gets you started by letting you learn the process through setting up a simpler pilot configuration on three Windows® machines, outside of your production environment. The machines will be referred to as the “Portal system,” “Team Workplace system,” and “Sametime system.” The following diagram shows all the software components that you can install on each Windows system.



\*The Notes client would not normally be installed on the same system as WebSphere Portal. It is included there for this pilot to limit the number of machines you need to use.

### Notes:

- You need only install the software components that you are interested in piloting — for example, you can choose to install Sametime but not install Team Workplace, in which case you would just skip any instructions about Team Workplace.
- Although the installation instructions provided in this section are for Windows systems only, the configuration techniques and the process you will learn will still help you to understand much that you need to do on other platforms.

### System requirements

Check the documentation for WebSphere Portal 5.0.2 and each Domino 6.5.1 extended product that you want to install to make sure that you select Windows systems that meet the minimum requirements.

## Overview of process to set up the pilot

The WebSphere Portal server runs on top of WebSphere Application Server, which must also be installed. For this pilot configuration, you will use WebSphere Portal with its own integrated Cloudscape database for storing information. (In a production environment, you will want to use a more robust database, such as DB2.) A Notes client, required to administer Domino and its extended products, will also reside on this machine.

Lotus Team Workplace (formerly QuickPlace) and Lotus Instant Messaging and Web Conferencing (Sametime) each require Domino to run; Domino on the Team Workplace system will serve as the LDAP server for WebSphere Portal, Team Workplace, and Sametime. You will configure each Domino extended product to make it work in a Portal environment, and sometimes configure one Domino product to make it work with another Domino product.

You will also configure WebSphere Portal to work with LDAP-based authentication and integrate with Domino and the extended products.

You will then download the Notes/Domino and Extended Products Portlets from the WebSphere portal catalog, and install them on the Portal system. Installing the portlets also installs some sample portal pages that acquaint you with the look and feel of a portal environment with collaborative portlets.

The following table summarizes the roles and user names of users you will create for this pilot:

<i>Role</i>	<i>User or Group Name</i>
WebSphere Portal administrator	wpsadmin
WebSphere Portal administration group	wpsadmins
WebSphere Application Server administrator	wpsbind
Domino administrator on Team Workplace system	wpsadmin
Notes client user	wpsadmin
Team Workplace administrator — temporary administrator, stored locally, whose purpose is to configure LDAP	qpadmin
Team Workplace administrator — permanent administrator who authenticates with LDAP	wpsadmin
Domino administrator on Sametime system	STadmin
Sametime administrator	STadmin
Domino Document Manager administrator	wpsadmin

**Note** In Domino Directory, when user names are a single word, the “First name” field is blank.

**Important** Performing the procedures that follow in the order they are presented is crucial to setting up the pilot successfully. A table summarizing all of the products you can set up for this pilot and highlighting where you are in the process introduces each major task.

### Additional documentation resources

Throughout this section, procedures to set up the Lotus products for this pilot are provided. References to specific topics in the WebSphere Portal InfoCenter provide information that you need to set up WebSphere Portal for this pilot. To quickly find a referenced topic, click Search in the InfoCenter's menu bar and type the exact title of the topic.

For additional information that you do not immediately need to set up this pilot, you are referred to the product-specific Lotus and WebSphere Portal documentation. Most documentation can be installed as online Help along with the product (Domino and its extended products) or be configured to be accessed locally (the WebSphere Portal InfoCenter).

You can always find the referenced documentation on the Web at the following locations:

- WebSphere Portal 5.0.2 InfoCenter:  
<http://publib.boulder.ibm.com/pvc/wp/502/index.html>
- Lotus documentation: <http://www.lotus.com/ldd/doc>

## Installing WebSphere Portal

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal ( <b>Install now</b> )	Domino Enterprise Server	Domino Enterprise Server
WAS ( <b>Install now</b> )	Domino LDAP	Sametime
Cloudscape ( <b>Install now</b> )	Team Workplace	
Portlets/sample pages	Domino Document Manager	
Lotus Notes	Workflow	
	Domino Web Access	

To install WebSphere Portal and its associated applications:

1. Download the Portal 5.0.2 MultiPlatform version from <http://websbuild.raleigh.ibm.com/portals/portalsgold.html>.  
**Tip** See CDlayout.html for a list of all the files.
2. Follow the instructions in the WebSphere Portal Version 5.0.2 Fix Pack Installation Readme at <http://publib.boulder.ibm.com/pvc/wp/502/indexrm.html>.

The readme's instructions are different depending on whether you are installing on Windows 2000 or 2003.

**Note** Even though IBM HTTP Server is installed during this process, you do not need to configure it for use with WebSphere Portal for this pilot configuration. By default WebSphere Portal uses the internal HTTP transport within WebSphere Application Server to handle requests.

3. Perform the steps in the InfoCenter topic "Verifying and launching WebSphere Portal."

---

## Installing Domino on the Team Workplace system — Critical steps

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed)</i>	Domino Enterprise Server <b>(Install now)</b>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <b>(Enable now)</b>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace	
Portlets/sample pages	Domino Document Manager	
Lotus Notes	Workflow	
	Domino Web Access	

The following sections highlight only those steps that are specific requirements for Domino to work with WebSphere Portal and the Domino extended products in this pilot configuration. For complete installation and setup procedures, see Lotus Domino Administrator 6.5.1 Help.

**Note** The user who will administer this Domino server must be the same as the user who will administer the WebSphere Portal server.

### Install Domino

- During the Domino installation, make sure you complete the following steps:
  - Make note of the directories where the installation program will install Domino. When you install the Team Workplace server on this system, you will need to install it in the same program directory where Domino is installed.
  - Select Domino Enterprise Server for the server type.

### Run Domino Setup

- Select "Set up the first server or a stand-alone server."

- For your Domino server name, for this pilot you must use the (unqualified) DNS name. For example, if the fully qualified domain name of the server is domserver1.acme.com, use “domserver1” for the Domino server name.
- For the Domino administrator name, enter wpsadmin. You will also use this user name for the WebSphere Portal administrator.  
**Tip** Select the option to save the administrator’s ID locally, as you will need to retrieve it later when you create a Location document in Notes from which to manage this Domino domain.
- For which Internet services to provide, do the following:
  - Select “Web Browser (HTTP services).”
  - Make sure “Directory services (LDAP services)” is selected, as this Domino server will serve as the LDAP server for WebSphere Portal, Lotus Team Workplace, and Lotus Instant Messaging and Web Conferencing (Sametime).
  - Click Customize, and select DIIOP CORBA services.

## Installing Domino Administrator — Critical steps

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Enabled)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace	
Portlets/sample pages	Domino Document Manager	
Lotus Notes <b>(Install now)</b>	Workflow	
	Domino Web Access	

The following sections highlight only those steps that are specific requirements for this pilot configuration. For complete installation and setup procedures, see Lotus Domino Administrator 6.5.1 Help.

### Installing Domino Administrator

- For this pilot configuration, install Domino Administrator on the Portal system, as running Domino Administrator on a system that is also running Domino is not supported.
- During the Lotus Notes client installation, select “Domino Administrator” for the setup type.

## Running Domino Administrator Setup

- The user name must be the same as the administrator name you entered during Domino configuration on the Team Workplace system — wpsadmin.
- You can accept all the default settings, except that you must select “Directory server (LDAP)” on the Additional Services screen, and then specify the LDAP account and the FQDN of the Domino server on the Team Workplace system.

---

## Configuring LDAP

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed)</i> <b>(Configure for LDAP now)</b>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Enabled)</i> <b>(Configure now)</b>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace	
Portlets/sample pages	Domino Document Manager	
Lotus Notes <i>(Installed)</i>	Workflow	
	Domino Web Access	

To configure Domino LDAP for use in this pilot configuration, perform the steps in the following topics:

1. Specifying Domino server configuration settings for LDAP
2. Adding WebSphere administrators to the Domino Directory
3. Updating access control in the Domino Directory

To configure WebSphere Portal to use Domino LDAP for authentication, see the topic “Configuring WebSphere Portal for LDAP and enabling security.”

## Specifying Domino server configuration settings for LDAP

Use the domain Configuration Settings document for the Domino server on the Team Workplace system to specify which information anonymous LDAP users can search in the Domino Directory.

Features of WebSphere Portal require that LDAP users access specific attribute types in Domino. For example, within the edit mode of some collaborative portlets, a picker list of available servers displays if the user has access to the attributes shown in the steps below. The following instructions provide steps that enable anonymous LDAP users to access these attributes.

To configure anonymous access for LDAP users, you must include all the attributes shown in the following steps, including the attribute HTTP-HostName. Because the attribute HTTP-HostName does not display for the default LDAP schema of Domino 6.x, you must extend the schema to add the attribute.

For details about setting up the LDAP service and methods for extending the schema, refer to Lotus Domino Administration 6.5.1 Help. To allow anonymous users to query LDAP, follow these steps:

**Step 1: Add the HTTP-HostName attribute to the schema.**

1. Start the Domino server on the Team Workplace system.
2. When the server is completely started, launch the Domino Administrator on the Portal system.
3. Make sure that you have Manager access to the Schema database (SCHEMA.NSF) on the Team Workplace system.
4. Open the Schema database.
5. Select the All Schema Documents view, then click New Document - Add Attribute Type.
6. Complete these fields on the Basics tab.

<i>Field</i>	<i>Action</i>
LDAP name	For the attribute, enter the following name: HTTP-Hostname
OID	Enter the following object identifier: 2.16.840.1.113678.2.2.2.2.461
Syntax name	From the drop-down list, select "Directory String"

**Note** For this pilot, you do not need to specify anything for the other fields on the Basics tab.

7. Click Save & Close.
8. Select the Draft Documents - Draft Attribute Types view.
9. Open the HTTP-HostName draft document, and click Approve - Approve Selected Drafts.

**Step 2: Complete the configuration**

1. Use the Domino Administrator interface to open the Domino Directory, names.nsf, for the server.
2. Navigate to the view Configuration - Servers.

3. Highlight Configurations and then open the Configuration Settings document. If a global configuration document does not exist, click Add Configuration to create a new configuration document and display Configuration Settings.
4. On the Basics tab, for the option Use these settings as the default settings for all servers, click Yes.  
**Note** You must select Yes to cause the LDAP tab to appear for use in the next step.
5. On the LDAP tab, click the button next to Select Attribute Types to open the LDAP Attribute Type Selection dialog box.
6. From the Object Classes drop-down list, select \*, and then click Display Attributes.
7. From Selectable Attribute Types box, select the following fields, and then click Add to add them the Queriable Attribute Types box.  
HTTP-HostName  
MailFile  
MailServer  
NetAddresses  
Sametime  
**Note** In a production environment, you might need to select additional fields. See the WebSphere Portal InfoCenter for complete information.
8. Click OK to close the LDAP Attribute Type Selection dialog box, and return to the Configuration Settings document.
9. Ensure that the Anonymous users can query field displays the following attributes:  
HTTP-HostName  
MailFile  
MailServer  
NetAddresses  
Sametime
10. Click OK.
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.
13. Click “Save and Close” to close Configuration Settings.

14. Restart the Domino server so that the option “Allow LDAP users write access” has been loaded prior to any additional configuration.

### **Adding WebSphere administrators to the Domino Directory**

You will later configure the WebSphere Portal server to use the Domino LDAP service to perform authentication. As a result, the Domino Directory must contain the following two accounts required by the Portal server: WebSphere Application Server, or WAS, administrator (WebSphere Portal server runs on top of WAS) and portal administrator (for WebSphere Portal server itself.)

**Note** The administrative user you created in Domino (on the Team Workplace system) will act as the portal administrator, and already exists in the Domino Directory.

Create a new user in the Domino Directory (on the Team Workplace system) to act as the WebSphere Application Server administrator. Navigate to the People view of the Domino Directory and, from the action bar, click “Add Person.”

1. In the New Person form, enter the following values in the fields shown:
  - Last name: wpsbind (for your WAS administrator’s last name).
  - User name:
    - wpsbind/acme (acme is your Domino organization)
    - wpsbind (for the WAS administrator’s common name)

**Note** Make sure that you enter two values in the User name field, where the first value includes the Domino organization.

  - Short name: wpsbind (for the user ID)
  - Internet password: *password*, where *password* is the Internet password you assign for the WAS administrator
2. Click “Save and Close” to save the new person document for the WAS administrator and return to the People view of the Domino Directory.
3. Edit the Person document of the Domino/portal administrator (wpsadmin), which was created when you set up Domino on the Team Workplace system, to include the administrator’s Internet password.
4. Click “Save and Close.”
5. Navigate to the Groups view of the Domino Directory and, from the action bar, click Add Group.

6. In the New Group form, on the Basics tab, enter the following values in the fields shown to create a portal administrators group, for example, wpsadmins, and add the WAS and portal administrative users to the group. You can add additional users to administer the portal, if desired.
  - Group name: wpsadmins
  - Group type: Multi-purpose
  - Members:
    - wpsbind/Acme (the user name for the WAS administrator)
    - wpsadmin/Acme (the user name for the portal administrator)
7. Click “Save and Close” to save the group.
8. See the topic “Updating the Access Control List of the Domino Directory” to assign the necessary permissions to the new administrative group and users.

### **Updating access control in the Domino Directory**

You must ensure that the administrator group, wpsadmins, has the proper permissions and roles in the Domino Directory on the Team Workplace system.

1. From the Domino Administrator, open the Domino Directory (names.nsf) on the Team Workplace system, and from the main menu, choose File - Database - Access Control to open names.nsf.
2. In Access Control List - Basics, ensure that the portal administrators group “wpsadmins” has either Author access or Editor access.
3. For the wpsadmins group, add and assign the following Role Types:
  - GroupCreator
  - GroupModifier
  - UserCreator
  - UserModifier
4. Click OK.

### **Configuring WebSphere Portal for LDAP and enabling security**

In this pilot configuration, you need to configure WebSphere Portal to work with Domino LDAP. You do this by customizing the Portal server’s configuration properties file to reference the Domino LDAP server. You also must run configuration tasks to enable Global Security on the WebSphere Application Server.

1. Follow the steps in the InfoCenter topic “Configuring WebSphere Portal for Domino Directory.”

**Tips:**

- There is no configuration template in this case.
  - In Step 3, enter values specific to this pilot, as shown below in Details.
  - Skip steps 4, 11, 13, 15, and 16
  - Make sure you complete Step 5.
  - Step 12 enables Global Security on the WebSphere Application Server.
  - Step 17 is optional.
2. Verify the LDAP is working by doing the following:
    - a. Go to WebSphere Portal and create a new user by clicking Sign-up in the upper-right hand corner.

- b. Log in to WebSphere Portal as the user you have just created.

If the login is successful, your LDAP server should be working correctly.

**Note** The content resulting from login may vary according to user role. If you do not receive an error message, you can assume that the LDAP server is functioning properly.

3. Verify the WebSphere Application Server Global Security is enabled by doing the following:
  - a. Stop and restart the WebSphere Application Server.
  - b. Make sure that the only way you can log in to the WebSphere Application Server’s administrative console is with the WebSphere Application Server administrator’s ID and password.

**Details**

In the `wpconfig.properties` file, here are the LDAP and security-related values appropriate for this pilot:

WebSphere Application Server Properties

`WasUserid=cn=wpsbind, o=acme`

`PortalAdminid=cn=wpsadmin, o=acme`

`PortalAdminidShort=wpsadmin`

`PortalAdminGroupid=cn=wpsadmins`

`LTPATimeout=120`

`SSODomainName=.yourInternetDomain.com`

Note the period that precedes *yourInternetDomain*.

LDAPHostName=*hostname.acme.com*, where *hostname* is the host name of the Domino server on the Team Workplace system  
 LDAPPort=389  
 LDAPAdminUid=cn=wpsadmin, o=acme  
 LDAPServerType=DOMINO502  
 LDAPBindID=cn=wpsbind, o=acme  
 LDAPUserFilter= (&(|(cn=%v)(uid=%v)(objectclass=inetorgperson))  
 LDAPGroupFilter=  
 (&(CN=%v)(|(objectclass=groupofnames)(objectclass=groupofuniquenames)))  
 LDAP Suffix=<none>  
 LdapUserPrefix=cn  
 LDAPUserSuffix=o=acme  
 LdapGroupPrefix=cn  
 LDAPGroupSuffix=<none>  
 LDAPUserObjectClass=dominoPerson  
 LDAPGroupObjectClass=dominoGroup  
 LDAPGroupMember=member  
 LDAPsslEnabled=false

---

## Installing Team Workplace

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace <b>(Install now)</b>	
Portlets/sample pages	Domino Document Manager	
Lotus Notes <i>(Installed)</i>	Workflow	
	Domino Web Access	

The following sections highlight only those steps that are specific requirements for this pilot configuration. For complete installation procedures, see the *Team Workplace 6.5.1 Installation and Upgrade Guide*.

Install Team WorkPlace on the Domino server you have already installed on the Team Workplace system.

### Critical steps

- Shut down the Domino server.
- From the Team Workplace CD, or from a network directory with the Team Workplace installation kit, click setup.exe to start the install.
- On the Choose Destination Location screen, the install program has already detected the existing Domino program directory. This is the location to which you want to install Team Workplace — just click Next.
- On the Specify Name and Password screen, supply an administrative user name and password for a user who does *not* exist in the Domino Directory, for example, qpadmin.

**Note** This administrative user is stored only in the local NOTES.INI file. This administrator will log in to the Team Workplace administrative interface and configure Team Workplace server settings for Domino LDAP, specifying the LDAP server name and making the portal administrator (already in the LDAP directory) the administrator of the Team Workplace server. The *qpadmin* administrator cannot be a portal user, since *qpadmin* does not exist in the LDAP directory.

- Restart the Domino server.

---

## Configuring Team Workplace

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed)</i> <b>(Configure now)</b>	
Portlets/sample pages	Domino Document Manager	
Lotus Notes <i>(Installed)</i>	Workflow	
	Domino Web Access	

Complete the following tasks to allow Lotus Team Workplace to work properly with WebSphere Portal and other Domino extended products.

## Accessing the administrative interface for Team Workplace

1. With the Team Workplace server running, open a browser and enter the URL for the Team Workplace server, for example, `http://servername.enterprise.com/Quickplace`
2. On the Team Workplace home page, click Sign In at the top-left corner of the screen.
3. Enter the Team Workplace server administrator user name and password that you specified during the install.

## Specifying the LDAP server

For this pilot, you configure the Team Workplace server to use the Domino LDAP server on the same system that Team Workplace is installed on.

1. In the Team Workplace administrative interface, click Server Settings and then click User Directory.
2. Click the “Change Directory” button, and select “LDAP Server.”
3. Enter the FQDN of the LDAP server, for example `servername.enterprise.com`.
4. Under New Users, select “Disallow new users,” and click Next.  
“OK with Anonymous access” should now display under the server name. If not, go back a page and check that you entered the name in Step 3 correctly.

## Editing Team Workplace server access

Do the following to add the administrator of the WebSphere Portal server (wpsadmin) to the list of users who can administer the Team Workplace server.

**Note** You will be asked to enter a user name and password each time you click a button, as the Team Workplace administrator (qadmin) is not in the Domino Directory. Once you have added the portal administrator (wpsadmin) as a Team Workplace administrator and logged back in as wpsadmin, this behavior will stop.

1. In the Team Workplace administrative interface, click Security.
2. Under “Who can administer this server,” click Add, and then click Directory to locate the Portal server administrator.

**Note** In this pilot, clicking “Show All” or searching by letter will fail to locate the portal administrator, since the LDAP search filter in Team Workplace is by default configured to find users whose user name consists of a first and last name, not a single name such as we are using (wpsadmin). As a workaround, search on groups and select wpsadmins, or enter wpsadmin manually instead of trying to select it from the list.

3. Click Add, and then click Close.
4. Confirm that the Portal server administrator has been added to the list for this server, and click Next.

For more information on LDAP search filters, see the chapter “Planning for WebSphere Portal in a Domino Environment.”

## Specifying the Sametime server

Do the following to prepare Team Workplace to use Sametime awareness, chat, and Web conferencing within team workplaces.

**Note** After you have installed Sametime, you will need to perform the steps in the topic “Setting up awareness and chat for Team Workplace,” later in this section.

1. In the Team Workplace administrative interface, click Other Options.
2. Click Edit Options.
3. Enter the fully qualified domain name of the Sametime server in both the Sametime Community Server and Sametime Meeting Server fields — for example, `http://servername.enterprise.com`.

**Note** You may have to restart the Team Workspace server after Sametime has been installed and configured to work with Team Workplace in order for integration to take effect.

4. Click Next.

## Configuring the NOTES.INI file

1. Locate and open the NOTES.INI file for Team Workplace server (Lotus\Domino\notes.ini).
2. Ensure that DIIOP is one of the ServerTasks in the NOTES.INI file. If not, type DIIOP to add it as one of the ServerTasks.

**Note** Setting DIIOP as a server task enables the “picker” feature in the Lotus Notes View portlet’s edit mode, which enables browsing of Domino databases on a given server. In addition to adding DIIOP as a server task, you must ensure that you enable HTTP clients to browse databases for your Team Workplace server. To enable this, use Domino Administrator to locate the Server Document for your Team Workplace server. Edit the server and on the Internet Protocols tab, select Yes in the “Allow HTTP clients to browse databases” field; then, in the “Host name” field, enter the fully qualified host name of the Team Workplace server.

3. Save and close the NOTES.INI file.

## Adding the Team Workplace servlet

To enable Team Workplace to work in your collaborative portal, you need to add the QuickPlaceServlet (stored in the Collaborative Components Java archive file cs.jar) to your Team Workplace server. The QuickPlaceServlet ensures that the records of portal users who are registered in portal are synchronized with Team Workplace membership records.

1. Create a directory under Lotus\Domino\Data\Domino called Servlet, if it does not already exist.

2. Find the Domino Data servlets.properties file, typically in this default location:

```
<installation_drive>:\Lotus\Domino\Data\servlets.properties
```

If this file doesn't exist, create it with a text editor.

3. Open the servlets.properties file in a text editor and add this line:

```
servlet.QPServlet.code=com.lotus.cs.util.QPServlet
```

4. Save and close the file.

5. Extract the Collaborative Services Web archive file (cs.war) from the Collaborative Services Enterprise Application file (cs.ear) and then extract the Collaborative Services Java archive file (cs.jar) from cs.war. Find the cs.ear file on the server in the directory:

```
<wp_root>/installableApps/cs.ear
```

6. Extract the cs.war file from cs.ear.

**Note** Use an unzip program to extract files from .war and .ear files.

7. Extract the cs.jar file from cs.war.

8. Copy the cs.jar into the Lotus\Domino\Data\domino\java directory.

**Note** Do not create subdirectories such as WEB-INF in the Lotus\Domino\Data\domino\java directory in which to store the cs.jar file. The cs.jar file must be in the Lotus\Domino\Data\domino\java directory.

9. On the Team Workplace server, find the NOTES.INI setting that begins with JavaUserClassesExt and append the following to that line:

```
QPJC6
```

10. Add the following line to the end of that section of settings:

```
QPJC6=C:\LOTUS\DOMINO\data\domino\java\cs.jar
```

11. In the Domino Server document (Domino Web Engine tab), in the "Java servlet support" field, select "Domino Servlet Manager."

**Note** For Sametime awareness and Web conferencing to work in team workplaces, after you have installed Sametime on the second Domino system, you will need to perform the steps in the topics “Setting up awareness and chat in Team Workplace” and “Setting up Web conferencing for Team Workplace.”

## Testing Team Workplace

Make sure that Team Workplace is working by doing the following:

1. Log in to Team Workplace as the portal administrator who you gave administrative access to earlier in this topic.
2. Create a team workplace.
3. Add a new member, create a document, and close the browser.
4. Log in again, click My Places, and open the new place.

## Configuring the ability to search across team workplaces

Team Workplace has a Search Places feature, based on Domino Domain Search, that allows users to search all places of which they are a member. Search Places requires a Domain Catalog server (a Domino server that has a Domain Catalog and that builds a domain index), and all search requests are handled by a Team Workplace server running on the Domain Catalog server. For this pilot, you will make the Domino server on which you installed Team Workplace the Domain Catalog server.

For more information on the Search Places feature, see the *Team Workplace 6.5.1 Administrator's Guide*.

For information on enabling advanced search for a place, see the place's Help.

### To set up the Search Places feature

1. From Domino Administrator, edit the Server document for the Domino server on which you installed Team Workplace:
  - a. Click the Server Tasks - Domain Catalog tab, and select Enabled in the Domain Catalog field. This step starts the Catalog task and creates the Domain Catalog. You run the Catalog task to keep the Database Catalog up to date. You might do this on a schedule, for example, by including the task in the NOTES.INI setting, ServerTasksAt1.
  - b. After the Catalog task stops on the Domain Catalog server, in the Server document, click Server Tasks - Domain Indexer and click Enabled in the Schedule field to enable the Domain Indexer task. Specify a schedule for running the Domain Indexer.

## To configure Search Place settings

You use the qpconfig.xml file to configure Search Places settings on the Team Workplace server.

1. Make a copy of the qpconfig\_sample.xml file (located in the data directory).
2. Rename the copy qpconfig.xml.
3. Open the qpconfig.xml file with WordPad and search for “search\_places”
4. Replace the domino\_server\_name, hostname (FQDN), and port with the correct information for this server.
5. Delete the “Start of Sample” and “End of Sample” comment lines.
6. Save the file.
7. Opening the qpconfig.xml file in a browser. Confirm that your edits are there — the section you edited should be in color.

Use the following settings in the qpconfig.xml file to configure Search Places settings on the Team Workplace server. Values in bold are sample values that you customize.

---

```
<server_settings>
<search_places enabled="true" anonymous="true">
  <domain_catalog_server ssl="false">
    <port>80</port>
    <domino_server_name>servername/Acme</domino_server_name>
    <path_prefix></path_prefix>
    <hostname>servername.enterprise.com</hostname>
  </domain_catalog_server>
</search_places>
</server_settings>
```

---

For more information on creating and using the qpconfig.xml file, see the chapter “Team Workplace Administration Overview” in the *Team Workplace 6.5.1 Administrator’s Guide*.

---

## Installing Domino Document Manager

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <b>(Install now)</b>	
Lotus Notes <i>(Installed)</i>	Workflow	
	Domino Web Access	

### Pre-installation tasks

While the actual installation of Lotus Domino Document Manager is simple and straightforward, it does require some preplanning on your part. Use the checklist below to ensure a smooth installation.

1. Gather and have on hand information that you will need to provide during setup. See the chapter “Planning your Document Manager Installation” in the *Domino Document Manager Installation 6.5.1 Guide*.
2. Verify that you have administrator access to Windows on the Team Workplace system.
3. Have on hand the following information, which you will need when you create a library as part of the installation:
  - Notes/Domino server name
  - Notes/Domino domain name
  - HTTP host name of the server
  - Name of the library to be created
  - Configuration options for the library
  - Document Manager Group names to be associated with the the library
  - Library Administrator user names
  - File Cabinet Creator user names
4. Follow the next procedure to install the master server.

### Installing the master server

1. Shut down the following to prevent conflicts:
  - Notes client
  - Domino server software on the Team Workplace system

2. Insert the Document Manager CD into the CD-ROM drive of the Team Workplace system.
3. Choose Run from the Start Menu.
4. In the Command Line text box, type <CD drive letter>:\w32\install\setup.exe (for example, d:\w32\install\setup.exe).
5. Read the Software License Agreement, and click Yes if you agree, to continue the installation.
6. Click Next at the Welcome window of the Document Manager Server Setup.
7. At the first Choose Destination Location window, confirm or enter the path to the Domino server program directory, and click Next. This must be the same directory where Domino is installed.
8. At the second Choose Destination Location window, confirm or enter the path to the Domino data directory, and click Next.
9. At the third Choose Destination Location window, confirm or enter the path to the directory where you want to install Document Manager, and click Next.  
This directory must be either the Notes data directory, or below it.
10. At the Select Components window, select Master Server Install.
11. It takes a few minutes to install the components; when the install program is done, click Finish at the Install Complete window.
12. Start the Domino server on the Team Workplace system.  
**Note** You will encounter an expected error (“Transaction Manager...Initialization Failed”) at server startup until after you create a library.
13. Remove the CD from the drive.  
**Note** You may also install Document Manager from a network directory with a Document Manager installation kit.

---

## Configuring Domino Document Manager

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configure now)</i>	
Lotus Notes <i>(Installed)</i>	Workflow	
	Domino Web Access	

You must create at least one Library to have any access to Document Manager.

The setup procedure:

- Modifies Access Control Lists
- Creates Address Book group names
- Creates the Document Manager databases

Setup creates library and log databases in the Document Manager install directory. The names of these databases are based on the library name you specify. If databases of those names already exist, Setup will warn you of that condition and will prompt you to correct it before proceeding.

For more detailed explanations of the terms and concepts used in setting up Document Manager, see the *Document Manager 6.5.1 Administrator's Guide*.

**Note** The setup procedure is run from the Site Administration database. This database must be accessed from the server, not locally.

### Setup procedure

This procedure has been tested on a Notes client running Windows XP Professional, 2000 Professional, or NT. If, for this pilot procedure, the Portal system on which you installed the Notes client runs Windows 2003, unexpected behavior could result.

You must also be able to use the Notes client to send e-mail to yourself. To verify this, click the Mail (or Quickpick) icon in the lower right corner of the Notes workspace, and choose Open Mail. If that works, you are all set. If not, you may need to create a location document that specifies the correct mail server and mail file.

To start the library setup, perform these steps at the Notes client:

1. Start the Domino server if it is not already running.
2. Enter the administrator's user name (wpsadmin) and password.
3. In Notes, choose File - Database - Open.
4. Open the address book or Domino directory on the server where you installed Document Manager.

If the Domino.Doc Site Administrators group does not exist, or does not include the site administrator performing the setup, you must create the group in the Domino Directory and/or add the appropriate user(s) to the group before proceeding.

5. Close the address book.
6. Enter the following command at the Domino server console:

```
load updall -r names.nsf
```

7. Open the Domino.Doc Site Admin database (ddadmin.nsf), located on the Document Manager server in the subdirectory where you installed Document Manager.

**Note** The Site Administration database must be accessed from the server, not locally. If you get the message "You are not authorized to access this database," verify that you have created the Domino.Doc Site Administrators group in the Domino Directory and that you are a member. If so, close Notes, re-open it, then try again to open the Site Administration database.

8. Click Create Library.
9. Enter a unique name for the new library.

If you change the library name after navigating to the second page of this procedure, be sure to click Update Group Names on the second page.

10. Accept the default Binder Table of Contents control, or choose the Notes folders view.

The default setting provides better performance; using Notes folders allows greater customization, and does not require any client-side components to be installed. For more information, see "About the Binder Table of Contents" in the *Document Manager Administrator's Guide*.

11. Accept the default Library Design Template (domdoc.ntf) or specify a different template name if you have a customized template that you need to use.

**Note** The Template Title (as found in Database - Properties - Design) must be of the format **DominoDocLibraryxxx**. If the name is not in this format, errors will occur.

For more information, see “Customizing the library design template” in the *Document Manager 6.5.1 Administrator’s Guide*.

12. Accept the default File Cabinet DesignTemplate (filecab.ntf) or specify a different template name if you have a customized template that you need to use.

13. Click Continue.

Document Manager automatically fills in the current user as the first administrator.

14. In the “Name of HTTP Host” field, enter the TCP/IP address of your Domino Web server.

15. Accept or change the Group names.

**Note** You can change the group names associated with this library; however, we recommend using the defaults to avoid name conflicts.

16. Check the Enable Sametime Integration box to enable the Who Is Online feature for documents in this library. (You can enable this feature for individual file cabinets; however, you cannot enable it for a cabinet unless it is also enabled for the library. You can enable or disable it later by editing the System Profile.)

17. Enter the name of the Sametime server in the space provided in the format *servername.domainname.com* (for example, “testserver.lotus.com”).

18. For the purposes of this pilot, do not enable LDAP integration. Enabling LDAP integration in a production environment would require that Lotus Document Manager reside on a different system and in a different Domino domain than that of the LDAP server.

19. Click Finish.

**Note** It may take a couple of minutes for the library databases to be created.

20. Take note of the setup information, then click Done.

21. Shut down the Domino server and restart it.

22. Close the Notes client and then start it again to make Document Manager accessible from the client.

**Note** When you open the library from Notes, if you see a message that the Document Manager client is not fully loaded, you do not need to take any action. This message refers to the Document Manager Desktop Enabler, a client that you can optionally install on the Notes workstation using the Notes client. The Enabler lets you access documents in a Document Manager library directly from document-creation applications. It is not necessary for this pilot.

23. (Optional) If users will be accessing Document Manager libraries from the Web, create database links to the new libraries.

---

## Setting up Lotus Workflow

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed)</i>	Workflow <b>(Install and configure now)</b>	
	Domino Web Access	

Lotus Workflow is a set of Lotus Notes databases and Windows programs that allow your organization to plan, schedule, track, monitor, and archive its document-based work and projects.

You can install and explore Lotus Workflow in this pilot configuration (use the Team Workplace system) if you are planning on using it in your Domino environment; however, as Domino and Extended Products 6.5.1 does not include any portlets that rely on Lotus Workflow, it not critical to install it in order to make use the sample portal pages.

For more information, see the *Lotus Workflow Installation and Administration Guide*.

---

## Installing Domino on the Sametime system — Critical steps

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <b>(Install now)</b>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

The following sections highlight only those steps that are specific requirements for this pilot configuration. For complete installation and setup procedures, see Lotus Domino Administrator 6.5.1 Help.

### Install Domino

During the Domino installation, make sure you complete the following steps:

- Make note of the directories where the installation program will install Domino. When you install the Sametime server on this system, you will need to install it in the same program directory where Domino is installed.
- Select Domino Enterprise Server for the server type.

### Run Domino Setup

- Select “Set up the first server or a stand-alone server,” as Sametime needs to be in separate Domino domain in order for Web Conferencing to work properly.
- For your Domino server name, for this pilot you must use the (unqualified) DNS name. For example, if the fully qualified domain name of the server is domserver2.acme.com, use “domserver2” for the Domino server name.
- Enter stadmin for the administrator name, and enter a password. This administrator will administer only the Sametime server. This administrator must have a different name than the Domino administrator on the Team Workplace system (wpsadmin), or problems may result.

**Tip** Select the option to save the administrator’s ID locally, as you will need to retrieve it later when you create a Location document in Notes from which to manage this Domino domain.

- For which Internet services to provide, do the following:
  - Select “Web Browser (HTTP services).”
  - Deselect “Directory services (LDAP services).”
  - Click Customize, and select DIIOP CORBA services.

## Installing Sametime — Critical steps

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <b>(Install now)</b>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

The following sections highlight only those steps that are specific requirements for this pilot configuration. For complete installation and setup procedures, see the *Lotus Instant Messaging and Web Conferencing 6.5.1 Installation Guide for Windows*.

### Installing Sametime

- Shut down the Domino server (on which you are installing Sametime) before you start the Sametime installation program.
- Access the Sametime installation program on the Sametime installation CD (CD 1).
 

**Note** You may also install Sametime from a network directory with a Sametime installation kit.
- During the installation, make sure that you install Sametime in the same directory where Domino is installed. The default Sametime installation directory that is presented by the Sametime installation program might be different from the installation directory where Domino is installed.

## Running Sametime Setup

- Browse to the Domino data directory that you specified when you installed Domino, for example, C:\Lotus\Domino\Data directory, and select the server.id file.
- When you are prompted for a user directory, select LDAP directory. The setup procedure then prompts you for the following information:
  - LDAP Server Name - Enter the fully-qualified DNS name or IP address of the Domino LDAP server that you set up on the Team Workplace system.
  - Port Number for LDAP - Specify the TCP/IP port number on which the LDAP server listens for LDAP connections. The default port number for LDAP connections is port 389.
- When the “Sametime Server Connectivity” dialog box displays, deselect (uncheck) the check box.

Sametime clients will attempt HTTP-tunneled connections to the Community Services on port 8082, the Meeting Services on port 8081, and the Broadcast Services on port 554.

- Make sure the LDAP server (Domino on the Team Workplace system) is running.
- Sametime Setup will now finish.
- Start the Domino server. The Sametime server starts automatically when the Domino server starts. It may take several minutes more for all of the Sametime services to load. You can use the Task Manager to see what Sametime services have loaded.
- Once the Sametime server is running, you can select the Welcome to Sametime icon on the Windows desktop to access the Sametime server home page.

**Note** In order for Domino's Single Sign-On functionality to work between Sametime and WebSphere Portal, you must replace the default Web SSO Configuration document that results from running Sametime setup. The topic “Configuring SSO for Sametime” will help you do this.

---

## Configuring Domino Administrator for use in two Domino domains

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configure now)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

Because the Domino servers on the Sametime system and the Team Workplace system must be in two different Domino domains, the easiest way to administer Domino on the Sametime system is to create another Location document, configured to use the administrative ID for the Domino server that is installed on the Sametime system. (The Location document for the administrator of the Domino server installed on the Team Workplace system was created when you ran the setup program for Domino Administrator.)

### To create a Location document for the Domino administrator of the Sametime system

1. From the menu, choose File - Mobile - Locations. Notes opens the Locations view of your Personal Address Book.
2. Click the “New” button and choose “Location.”
3. On the Basics tab in the “Location name” field, enter a name for this location.
4. In the “Location type” field, select “Local Area Network.”
5. In the “Internet mail address” field, enter the Internet version of your organizational Notes mail address, for example jsmith@acme.com.
6. Click the Servers tab.
  - In the “Home/mail server” field, enter the name of the Domino server on the Sametime system.
  - (Optional) In the “Domino directory server” field, enter the name of the Domino server on the Team Workplace system.
  - (Optional) In the “Sametime server” field, enter the name of the Sametime server.

7. Click Ports and select at least one of the ports that Notes lists.  
**Note** You can enable additional ports using File - Preferences - User Preferences.
8. Click the Advanced tab.
9. In the “User ID to switch to” field, specify the User ID file for the Domino administrator of the server installed on the Sametime system (you can click the search icon to browse the operating system).
10. Click “Save & Close.”

---

## Additional LDAP configuration for Sametime

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed)</i> <b>(Configure now)</b>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed)</i> <i>(Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed)</i> <i>(Configured)</i>	Workflow <i>(Installed)</i> <i>(Configured)</i>	
	Domino Web Access	

For background information on how LDAP works with Sametime, as well as more detail on the following procedures see the "Using LDAP with the Sametime server" chapter of the *Lotus Instant Messaging and Web Conferencing 6.5.1 Administrator's Guide*.

### Alter the Directory Assistance document for the LDAP directory

The Sametime server installation creates a Directory Assistance database (da.nsf) on the Sametime server. This database contains a Directory Assistance document that enables Sametime to connect to the LDAP server to authenticate Web browser users.

You must ensure the “Base DN for search” setting in this Directory Assistance document is set appropriately for the Domino LDAP directory on the Team Workplace system. To alter the “Base DN for search” setting in the Directory Assistance document:

1. From the Lotus Notes client, open the Directory Assistance database on the Sametime server.
  - Choose File - Database - Open.
  - Select the name of the Sametime server.
  - Select the Directory Assistance database (da.nsf).
  - Click Open.
2. Double-click the name of the Directory Assistance document for the LDAP server to open the document.
3. Click the LDAP tab.
4. In the “Base DN for Search” field, make an entry such as the following example: “O=OrganizationName,” where “OrganizationName” is the Domino organization (for example O=Acme) for the Domino server on the Team Workplace system.
5. Click Save and Close to save the Directory Assistance document.

## Configure the LDAP Directory settings

You must configure the LDAP Directory settings on the LDAP document in the Configuration database to ensure that the Sametime server can search and authenticate against entries in the LDAP directory. You can configure these settings using either the Lotus Notes client, as described in the following procedure, or using the Sametime Administration Tool, as described in the chapter “Using LDAP with the Sametime server” in the *Lotus Instant Messaging and Web Conferencing Administrator’s Guide*.

**Note** For the purposes of this pilot, you can just accept all default values. You need to perform the following steps only if something about your configuration, for example, a port, is different.

1. From the Lotus Notes client, open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
  - Choose File - Database - Open.
  - Select the name of the Sametime server.
  - Select the Sametime Configuration database (stconfig.nsf).
  - Click Open.

2. Open the LDAP document in the Configuration database that is associated with the LDAP server. To open the LDAP document:
  - In the right pane of the Configuration database, locate the LDAP server entry in the Form Name column of the Configuration database.
  - Each LDAP Server document is listed to the right and beneath the LDAP Server entry under the Last Modified Date column. The date represents the last time the LDAP server document was modified.
  - To open an LDAP Server document, double-click the date in the Last Modified Date column that represents the document.
  - When the LDAP Server document opens, double-click the document to put it in edit mode.
3. To configure the LDAP Directory settings, you can enter values directly into the editable fields in the LDAP Server document.

Consult the “Using LDAP with the Sametime Server” chapter in the *Lotus Instant Messaging and Web Conferencing Administrator's Guide* for information on individual LDAP Directory settings.

**Note** The LDAP Directory settings that are available from the LDAP document in the Configuration database are the same LDAP settings that are available from the Sametime Administration Tool. However, some LDAP Directory settings in the LDAP document are worded differently and arranged in a different order from the LDAP Directory settings in the Sametime Administration Tool. The *Lotus Instant Messaging and Web Conferencing Administrator's Guide* assumes that the administrator is using the Sametime Administration Tool to configure these settings, but includes a topic that correlates what the settings are called in the Configuration database with those in the Sametime Administration Tool.

---

## Configuring Sametime to support WebSphere Portal

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed)</i> <b>(Configure now)</b>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed)</i> <i>(Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed)</i> <i>(Configured)</i>	Workflow <i>(Installed)</i> <i>(Configured)</i>	
	Domino Web Access	

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

1. Use a text editor to open the Sametime.ini file located on the Sametime server. This file is located in the Domino program directory, typically c:\lotus\domino.
2. To set a security level, configure Sametime to accept all IP addresses as trusted. To do this, add a Debug section and then add the following line:

```
[Debug]
```

```
VPS_BYPASS_TRUSTED_IPS=1
```

**Note** In a production environment, you could add the IP address of the portal server machine to the list of IP addresses of trusted servers. To do this, you would add the following line to the Configuration section, taking care to separate your new entry from the previous entry using a comma, and using the IP address — not the host name:

```
[Config]
```

```
VPS_TRUSTED_IPS=trusted IP address, trusted IP address
```

3. Save and close the Sametime.ini file.

4. Enable the PurgeMeeting agent on the Sametime server to improve performance.

The Sametime Meeting Center on a Sametime server includes a PurgeMeeting agent. You should enable this agent to automatically delete Meeting Details documents when the documents reach a certain age. This is necessary to ensure good performance of the Lotus Web Conferencing portlet. The PurgeMeeting agent deletes the documents of finished meetings from the database on a scheduled interval. The interval is based on the following notes.ini setting:

```
STPurgeMeetingPastDays={number of days, or 0 to disable}
```

For more information about the PurgeMeeting agent, including the procedure for enabling the agent, see *Lotus Sametime Administrator's Guide*, Maintaining the Sametime Meeting Center.

5. Add the WebSphere Portal administrator (wpsadmin) to the ACL of the Sametime Configuration database, STConfig.nsf. Assign that administrator user Manager access and the role of [SametimeAdmin].

For more information, see the *Lotus Sametime Administrator's Guide*, Using the Sametime Administration Tool, Adding a new Sametime administrator.

6. Restart the Sametime server.

---

## Configuring SSO between WAS, Domino, and Domino Extended Products

If single sign-on (SSO) is configured between WebSphere Application Server (WAS) and Domino, a user can sign on to the portal and then access portlets that contain information from a Domino-based application or service without having to enter additional credentials for authentication. All participating servers must be in the same Internet domain.

**Important** A best practice is to install and configure all servers prior to enabling SSO. For example, in this pilot configuration, we have installed the WebSphere Portal, Lotus Team Workplace, and Lotus Sametime servers before enabling SSO.

To enable single sign-on, you must enable the IBM LTPA capabilities included in both WebSphere Application Server and Domino. Domino imports the WebSphere LTPA token generated by WebSphere Application Server, and this token can be used for all servers (Domino Extended Products) within each Domino domain.

Enabling LTPA capabilities in Domino involves creating a Web SSO Configuration document on one system within each Domino domain, and editing the Server document for all participating servers in each domain. Since this pilot configuration involves two Domino domains, you must set up both domains to use the same key information. Two conditions must exist in order to do this:

- You must be a registered Notes user and your server must be a registered server. This gives you and the server the rights to decrypt the Web SSO Configuration document in your current domain, and the right to create documents in the Domino Directory for the new domain.
- The server document and the administrator's person document must exist in the domain for which you will be creating the Web SSO Configuration, as the public keys that are used for encryption and decryption are stored in each registered person and server document.

**Note** Each user's Web browser must have cookies enabled since the authentication token that is generated by the server is sent to the browser in a cookie.

For procedures to configure SSO for this pilot configuration, see the following topics:

- Enabling SSO for WebSphere Application Server
- Configuring SSO for Team Workplace
- Completing SSO setup for Team Workplace
- Configuring SSO for Sametime

## Enabling SSO for WebSphere Application Server

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configure for SSO now)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

Do the following to create the WebSphere LTPA key:

1. Start the WebSphere Administration Console and log in as the WebSphere Application Server administrator (wpsbind).
2. Select Security - Authentication Mechanisms - LTPA.
3. Type a password in the Password field.  
**Tip** Remember the password because you must type it when you import the LTPA key into each Domino domain.
4. In the Key File Name field, provide a path and file name for the LTPA file. The path must be on the WebSphere Application Server.
5. Click the Export Keys button above the Password field.
6. Click Save on the Admin console action bar to apply the changes to the master configuration.
7. Click the Save button on the next screen.
8. Log out from the WebSphere Administration Console.
9. Copy the key file that you created to a location that is accessible to the Domino Administrator client (for this pilot, on the Portal system). You will need this key to import into your Domino servers when you create a Web SSO Configuration document for each Domino domain.

## Configuring SSO for Team Workplace

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configure for SSO now)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

You configure single sign-on (SSO) for Team Workplace by creating a Web SSO configuration document, and then performing a series of short procedures to complete the setup.

### Creating a Web SSO configuration document

The Web SSO configuration document is a Domino domain-wide configuration document stored in the Domino Directory. This document, which, in a production environment, should be replicated to all servers participating in single sign-on in the Domino domain, is encrypted for participating servers and administrators, and contains a shared secret key used by servers for authenticating user credentials.

To set up single sign-on for a Team Workplace server, first create a Web SSO Configuration document. A Web SSO Configuration document is stored in the Web - Configurations view of the Domino Directory (names.nsf).

1. From Domino Administrator, click Files, and open the Domino Directory (names.nsf) on the Team Workplace system.
2. Select the Configuration - Servers - All Server Documents view.
3. Click Web - Create Web SSO Configuration.
4. Click Keys at the top of the Web SSO Configuration document.
5. To import the WebSphere LTPA key, do the following.
  - a. Select "Import WebSphere LTPA Keys."
  - b. Enter the path to and name of the WebSphere LTPA export file.
  - c. Enter the password (specified when generating the keys in WebSphere). The document is updated to reflect the information in the export file.
6. Complete the rest of the document as follows:

<i>Field</i>	<i>Action</i>
Configuration Name	Accept the default entry, LtpaToken.
Organization	Leave this field blank so the document appears in the Web Configurations view.
DNS Domain	(Required) Enter the DNS domain (for example, acme.com) for which the tokens will be generated. The servers enabled for single sign-on must all belong to the same DNS domain.
Domino Server Names	Enter the names of all the Domino servers in this Domino domain to participate in single sign-on: in this case, the Domino server on the Team Workplace system, for example, server1/acme. This document is encrypted so that only you, the members of the Owners and Administrators fields, and the servers specified have access to it. <b>Note</b> Enter only Domino server names in this field; group names, wildcards, and WebSphere server names are not allowed.

*continued*

<i>Field</i>	<i>Action</i>
Expiration (minutes)	Specify the time period, in minutes, after which the token will expire. The default is 30 minutes. Change this to 120 minutes to match the WebSphere setting.
Idle Session Timeout	Select Enabled and enter a Minimum Timeout value, in minutes, to indicate the number of minutes of inactivity after which the token will expire.

7. **Important** Click the Basics tab and add a \ to the LDAP realm so that it reads yourLDAPhostname\ :389
8. Click “Save & Close” to save the Web SSO Configuration document in the Web - Web Configurations view. A message on the status bar indicates the number of servers/people for whom the document is encrypted.
9. Follow the steps in the next topic to complete the single sign-on setup.

### **Completing SSO setup for Team Workplace**

After you have created the Web SSO Configuration document for the domain, follow these steps to complete single sign-on setup for the Team Workplace server.

1. Add the following setting to the notes.ini file of the Team Workplace server to prevent anonymous access to files in the html directory:  
NoWebFileSystemACLs=1
2. Enable multi-server single sign-on authentication.  
To enable single-sign on authentication in the Server document, follow these steps on the Team Workplace server:
  - a. Open the Domino Directory (names.nsf) on the server.
  - b. Select the view Configuration - Servers - All Server Documents.
  - c. Select the Server document for the server and click Edit Server.
  - d. Click Internet Protocols - Domino Web Engine, and select Multiple Servers (SSO) in the Session authentication field.
  - e. In the Web SSO Configuration field, select “LTPA token” from the drop-down list.
  - f. Save and close the Server document.

3. Create the Domino Web Server Configuration database (domcfg.nsf).
  - a. From the Notes client, choose File - Database - New.
  - b. Next to Server at the top of the dialog box, select the Domino server that runs Team Workplace.
  - c. Next to Title, enter a descriptive title, for example, Web Server Configuration.
  - d. Next to File name, enter domcfg.nsf. You must use this file name.
  - e. Next to Server in the middle of the dialog box, select any server.
  - f. Click “Show advanced templates.”
  - g. Next to Template, select “Domino Web Server Configuration (6)” (domcfg5.ntf).
  - h. Click OK.
4. Create a mapping form in the Domino Web Server Configuration database to allow the *qadmin* account to work.
  - a. Open the Web Server Configuration database (domcfg.nsf).
  - b. Click Add Mapping.
  - c. Next to Applies To, select “All Web Sites/Entire Server” (default)
  - d. Next to “Target Database,” enter quickplace/resources.nsf, replacing the default entry.
  - e. Next to “Target Form,” enter QuickPlaceLoginForm.
  - f. Click Save & Close.
5. At the server console, enter the following command to stop and restart the server:

```
restart server
```

You should see the message “QuickPlace: Successfully loaded Web SSO Configuration.”

## Configuring SSO for Sametime

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configure for SSO now)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

The Sametime install enables SSO on its Domino server, but the Web SSO Configuration document it creates uses the Domino LTPA key, as opposed to the WebSphere LTPA key that is needed in a Portal-Domino environment. You need to delete the Web SSO configuration document and create a new one, just as you created one for Team Workplace. In this pilot configuration, since Sametime is in a different Domino domain than Team Workplace, Sametime needs its own Web SSO Configuration document.

1. Delete the Web SSO Configuration document from the Domino Directory on the Sametime system.
2. From Domino Administrator, click Files, and open the Domino Directory (names.nsf) on the Team Workplace system.
3. Select the Configuration - Servers - All Server Documents view.
4. Click Web - Create Web SSO Configuration.
5. Click Keys at the top of the Web SSO Configuration document.
6. To import the WebSphere LTPA key, do the following.
  - a. Select "Import WebSphere LTPA Keys."
  - b. Enter the path to and name of the WebSphere LTPA export file.
  - c. Enter the password (specified when generating the keys in WebSphere). The document is updated to reflect the information in the export file.

7. Complete the rest of the document as follows:

<i>Field</i>	<i>Action</i>
Configuration Name	Accept the default entry, LtpaToken.
Organization	Leave this field blank so the document appears in the Web Configurations view.
DNS Domain	(Required) Enter the DNS domain (for example, acme.com) for which the tokens will be generated. The servers enabled for single sign-on must all belong to the same DNS domain.
Domino Server Names	Enter the names of all the Domino servers in this Domino domain to participate in single sign-on: in this case, the Domino server on the Sametime system, for example, <i>SThostname/acme</i> . This document is encrypted so that only you, the members of the Owners and Administrators fields, and the servers specified have access to it. <b>Note</b> Enter only Domino server names in this field; group names, wildcards, and WebSphere server names are not allowed.
Expiration (minutes)	Specify the time period, in minutes, after which the token will expire. The default is 30 minutes. Change this to 120 minutes to match the WebSphere setting.
Idle Session Timeout	Select Enabled and enter a Minimum Timeout value, in minutes, to indicate the number of minutes of inactivity after which the token will expire.

8. **Important** Click the Basics tab and add a \ to the LDAP realm so that it reads yourLDAPhostname\.:389
9. Click “Save & Close” to save the Web SSO Configuration document in the Web - Web Configurations view. A message on the status bar indicates the number of servers/people for whom the document is encrypted.
10. At the server console, enter the following command to stop and restart the server:  

```
restart server
```

## Configuring WebSphere Portal for Domino extended products

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO)</i> <b>(Configure for Lotus products now)</b>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configured for SSO)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i>	
Portlets/sample pages	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

The following references are to the WebSphere Portal InfoCenter. You need to complete only the InfoCenter tasks whose titles match those below. You have already completed the InfoCenter tasks before or after the given task if you have followed all the procedures in this pilot.

1. Follow the steps in the InfoCenter topic “Configuring Collaborative Components to use Domino Directory.”
2. Follow the steps in the InfoCenter topic “Configuring WebSphere Portal to use Lotus QuickPlace.”
3. Follow the steps in the InfoCenter topic “Run the configuration task to configure WebSphere Portal to use Lotus Sametime.”
4. In `<wp_root>\shared\app\config\cseenvironment.properties`, specify the character to use to separate distinguished names, as follows:

The property is: `CS_SERVER_SAMETIME_1.dnNameSeparator`

The value is a character that is used to resolve names with the Sametime server, and the name used to log in to Sametime from a browser. A valid value for Domino servers is a slash (/)

For example: `CS_SERVER_SAMETIME_1.dnNameSeparator= /`

For the complete WebSphere Portal InfoCenter, go to <http://publib.boulder.ibm.com/pvc/wp/502/index.html>

## Installing the Notes/Domino and Extended Products Portlets

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO) (Configured for Lotus products)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configured for SSO)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i>	
Portlets/sample pages <b>(Install now)</b>	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

This topic describes the IBM Lotus Notes/Domino and Extended Products Portlets and provides instructions for installing the portlets on the WebSphere Portal server. Several sample portal pages that incorporate some of the portlets are also installed to show you the look and feel of the portal environment.

You will install the following portlets:

- Domino Extended Products Portlets Welcome Page
- Domino Web Access (formerly iNotes)
- Domino Application Portlet (formerly Domino Web Application Portlet)\*
- Lotus Domino Document Manager (formerly Domino.Doc)
- Lotus Notes Discussion\*\*
- Lotus Notes Mail\*\*
- Lotus Notes Teamroom\*\*
- Lotus Notes View
- Lotus Web Conferencing (formerly Sametime)
- Lotus Instant Messaging Contact List (formerly Sametime Contact List)
- My Lotus Notes To Do\*\*
- My Lotus Team Workplaces (formerly QuickPlace)
- People Finder

\*This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

\*\* Discussion, Mail, Teamroom, and To Do are installed as views in the Lotus Notes View portlet. You must create instances of Lotus Notes View and change each instance's name to be able to use these services. For more information, see the InfoCenter topic "Notes and Domino Version 5.02."

Each sample pages contains the following portlets:

<i>Sample portal page</i>	<i>Portlets</i>
Welcome	Domino Extended Products Portlets Welcome Portlet
Mail	Mail (view using Domino Web Access) People Finder My Contacts (from Instant Messaging Contact List)
Calendar	Calendar (view using Domino Web Access) People Finder My Contacts (from Instant Messaging Contact List)
Address Book	Address Book (view using Domino Web Access) People Finder My Contacts (from Instant Messaging Contact List)
Web Conferencing	Web Conferences (from Lotus Web Conferencing) People Finder My Contacts (from Instant Messaging Contact List)

<i>Sample portal page</i>	<i>Portlets</i>
Team Spaces	Team Spaces (from My Lotus Team Workplaces) People Finder My Contacts (from Instant Messaging Contact List)
Documents	Documents (Document Manager)
Domino Application Portlet	Domino Application Portlet
Domino Databases	Domino Databases (Lotus Notes View portlet)
Administration	Bookmarks

**Note** Some of the portlets in the sample pages are instances of installed Extended Products portlets, developed specifically for these sample pages — for example, My Contacts is an instance of Lotus Instant Messaging Contact List (formerly Sametime Contact List).

### Installing the portlets and sample pages

1. Download the Notes/Domino and Extended Products Portlets 6.5.1 from the WebSphere portal catalog at [https://www-306.ibm.com/services/cwi/portal/\\_pagr/105](https://www-306.ibm.com/services/cwi/portal/_pagr/105).
2. On the machine where WebSphere Portal is installed, create the directory <wp\_root>/EPPUpdate, and copy the Notes/Domino and Extended Product Portlets files into that directory.
3. Verify that the WAS\_HOME and WPS\_HOME environment variables are set. If not, you can specify them in the Deploy command line with the following parameters:

```
-washome <wasHomeDirectory>
-wpsHOME <wpsHomeDirectory>
```

**Note** Directory names that contain space characters need to be enclosed in double quotes.

4. Make sure that the WebSphere Portal server is running.
5. To deploy the portlets/sample pages, run the following command:  

```
Deploy [-f] [-v] <serverdns:port> <wpsadmin> <wpspassword>
[<nodename>] ([-portlets] | [-samplepages])
```

where the parameters have the following values:

<i>Parameter</i>	<i>Description</i>
serverdns:port	The DNS address and port of WebSphere Portal. For example, austria.lotus.com:9081
wpsadmin	The administrative user for WebSphere Portal
wpspassword	The administrator's password

*continued*

<i>Parameter</i>	<i>Description</i>
nodename	The name of the WebSphere Application node. This should be the same as the host name of your WebSphere Portal. The node name will appear as a subdirectory under the <wasHomeDirectory>/installedApps. If this name is different than your host name, enter the node name.
-portlets	Deploys only the portlets
-samplepages	Deploys only the sample pages
-f	Forces a copy of the portlets or theme. Normally, the deployer only copies files if they are not already present on WebSphere Portal. If you have already deployed the portlets or the theme and need to refresh the files, you can use this flag to force the files to copy again.
-v	Verbose mode

### Notes:

- You can also enter simply “Deploy” and press enter, and you will be prompted for each parameter.
  - You can also specify the server, administrative user, and administrator’s password using the following parameters:
    - s <server dns name>
    - u <admin user>
    - p <admin password>
  - You can enter the parameter -h to display command line help.
6. Log in to WebSphere Portal and select My Workplace to confirm that the sample portal pages and portlets have deployed.

### Example

The following command deploys the portlets and the sample pages to server “austria.”

```
deploy austria.lotus.com:9081 wpsadmin wpsadmin
```

## Configuring the Notes/Domino and Extended Products Portlets

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO) (Configured for Lotus products)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configured for SSO)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i>	
Portlets/sample pages <i>(Installed) (Configure now)</i>	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

The following sections describe the required steps to configure the Notes/Domino and Extended Products Portlets.

### Team Spaces and Web Conferences

Change these parameters so that the Team Spaces (from My Lotus Team Workplaces) and Web Conferences (from Lotus Web Conferencing) portlets can find the servers that host them.

1. Log in to WebSphere Portal as an administrator.
2. In the administration section of the portal, click Portlets and then click Manage Portlets.
3. For the Team Spaces portlet, click “Modify parameters.”
4. Change the QuickPlaceHostname to the server name of your team workplace.
5. Verify that QuickPlacePort is set to the correct port — the default port is 80.
6. Click the Save button at the bottom of the screen.
7. After the settings are saved, click Cancel to return to the Manage Portlets screen.
8. For the Web Conferences portlet, click “Modify parameters.”
9. Change the SametimeServer1 parameter to the Sametime server name.

10. Change SametimeUserName1 to the same administrative user (wpsadmin) that you specified earlier in step 3 of the topic “Configuring Sametime to support WebSphere Portal,” and change SametimePassword1 to the password for this user.
11. Verify that SametimePort1 is set to the correct port - the default port is 80.
12. Click the Save button at the bottom of the screen.
13. After the settings are saved, click Cancel to return to the Manage Portlets screen.
14. Click on My Portal and then My Workplace.

### **People Finder**

1. From My Workplace, click on Mail.
2. Follow the on-screen instructions in the People Finder portlet.

**Note** If ibmPersonalTitle is displayed as missing, click on Configuration Basics and deselect carLicense.

### **My Contacts**

No additional configuration is required for the My Contacts (from Instant Messaging Contacts List) portlet.

### **Lotus Notes Mail**

Although no Domino Web Access (iNotes) users were configured for this pilot, the Mail portlet will work for Domino Web Access users.

### **Domino Application Portlet**

Follow the on-screen instructions to edit and configure the Domino Application Portlet.

- On the Source/Display tab, enter the host name, port, and path and file name of the Domino Directory for Domino on the Team Workplace system.
- On the Authentication tab, select “Single Sign-On (SSO).”
- Click Done and then click Close to save your changes and exit.

## Bookmarks

Click the Edit button to create bookmarks that point to the appropriate servers.

**Note** The administration portlet is a demonstration of the usefulness of the Bookmarks portlet. It provides a single point of access to all of the Web-based administration tools needed by an administrator. Since it is only useful for an administrator, you should assign only administrators to its manager role, not end users. Since the Bookmarks portlet must be configured for each end user, you must configure it for each administrator separately in WebSphere Portal's Administration tool.

---

## Setting up awareness and chat for Team Workplace

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO) (Configured for Lotus products)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configured for SSO)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i> <b>(Configure for Sametime now)</b>	
Portlets/sample pages <i>(Installed) (Configured)</i>	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

These instructions assume that the Awareness feature has been independently tested on the Sametime server and is functioning properly, and that multi-server single sign-on is set up between the Sametime and Team Workplace servers.

Do the following to enable online Awareness and Chat for Lotus Team Workplace users:

- Manually copy Java files from the Sametime Java toolkit and from the Team Workplace server to a subdirectory of the Domino data directory on the Sametime server.
- Specify the name of the Sametime server in the Team Workplace Server Settings room.

**To copy the Java files required for Chat and online Awareness**

1. On the Sametime server, install the Sametime 6.5.1 Java Toolkit. You can download the toolkit from from the Lotus section of the IBM developerWorks web site ([www.ibm.com/developerworks](http://www.ibm.com/developerworks)).
2. In the Domino data directory of the Sametime server, create the following subdirectory:

```
<domino data directory>\Domino\html\QuickPlace\peopleonline
```

For example, on a Windows computer, if the path to the Domino data directory is C:\Lotus\Domino\Data, the path to the peopleonline subdirectory will be:

```
c:\lotus\domino\data\domino\html\QuickPlace\peopleonline
```

3. Copy the files STComm.jar, CommRes.jar, and PeopleOnline31.jar to the QuickPlace\peopleonline subdirectory you created in the previous step. These files can be found in the following location:

**Files to copy from the Sametime server**

<i>File name</i>	<i>Location</i>
STComm.jar	<data dir>\domino\html\sametime\toolkits\st651javatk\bin where <data dir> is the Domino data directory on the server. For example: c:\lotus\domino\data\domino\html\sametime\toolkits\st651javatk\bin\STComm.jar
CommRes.jar	<data dir>\domino\html\sametime\toolkits\st651javatk\bin where <data dir> is the Domino data directory on the server. For example: c:\Lotus\Domino\Data\domino\html\sametime\toolkits\st651javatk\bin\CommRes.jar

**Files to copy from the QuickPlace server**

<i>File name</i>	<i>Location</i>
PeopleOnline31.jar	<data dir>\QuickPlace For example: c:\lotus\domino\data\QuickPlace\PeopleOnline31.jar

**To designate the Sametime Community server for Team Workplace to use**

1. In a browser, enter the URL of the Team Workplace server. For example: `http://servername.enterprise.com/QuickPlace`
2. Log in as an administrator.
3. Click Server Settings in the table of contents.
4. Click Other Options in the table of contents.
5. Click Edit Options.
6. Under the Sametime Servers heading, make sure that the Sametime Community Server is in the community field. Use the server's URL. For example, `http://meetingserver.enterprise.com`.

**Note** The Team Workplace server is not immediately integrated with Sametime. Wait a few minutes for the setting to take effect, or restart the Team Workplace server to integrate immediately.

7. Do the following to enable places for instant messaging. This setting is enabled by default, but you should check to ensure it is actually enabled in any Place where members will be collaborating online.
  - a. Sign in to Team Workplace.
  - b. Click My Places, and open a place.
  - c. Click Customize.
  - d. Click Basics.
  - e. Click Change Basics.
  - f. On the Change Basics page, scroll down to the bottom. Under the Real-time collaboration heading, make sure "Members can see who is online and send instant messages" is checked.
  - g. Click Done.
8. Enter a place and verify that Awareness is working by checking for the Awareness icon next to the name you entered when you logged in.

**Note** You must log in as an external user. Sametime features are not available to local users.
9. To test Chat, find a document that was created by a user listed online and click their name. Then select Chat, or click the Chat link beside your name in the top left corner of the screen.

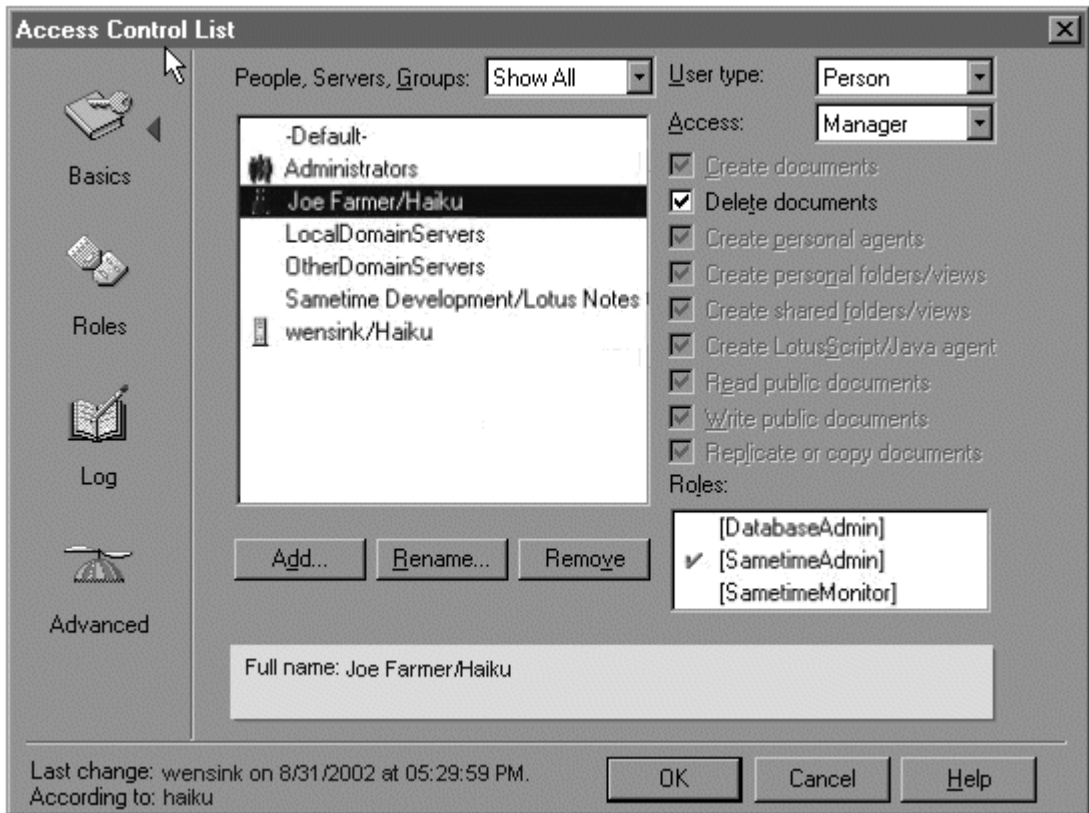
## Setting up Web conferencing for Team Workplace

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO) (Configured for Lotus products)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configured for SSO)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i> <b>(Configure for Sametime now)</b>	
Portlets/sample pages <i>(Installed) (Configured)</i>	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access	

These instructions assume that the Meetings feature has been independently tested on the Sametime server and is functioning properly.

Do the following to set up Team Workplace to correctly create and update Sametime Meetings on a Sametime server.

1. On the Sametime server, add a user name to the local Domino Directory. This user name should be used only for integration of Sametime and Team Workplace.
2. On the Sametime server, add the user as a manager in the ACL of the STConfig.nsf database. Make their user type Person, and give them the [SametimeAdmin] role at minimum. For example, see the picture below.



3. Shut down and restart the Sametime server.
4. Copy the following files from the Domino program directory of the Sametime server (default is \lotus\domino) to the Domino program directory of the Team Workplace server (default is \lotus\domino): STMTgManagement.jar, STCore.jar, ibmjsse.jar
5. On the Team Workplace server, find the notes.ini setting that begins with JavaUserClassesExt and append the following to that line: QPJC7, QPJC8, QPJC9. Then, add the following three lines to the end of that section of settings:
 

```
QPJC7=C:\LOTUS\DOMINO\ibmjsse.jar
QPJC8=C:\LOTUS\DOMINO\STCore.jar
QPJC9=C:\LOTUS\DOMINO\STMTgManagement.jar
```

You should end up with a section that looks like this:

```
JavaUserClassesExt=QPJC1, QPJC2, QPJC3, QPJC4, QPJC5, QPJC6,
QPJC7, QPJC8, QPJC9
```

```
QPJC1=C:\LOTUS\DOMINO\quickplace.jar
```

```
QPJC2=C:\LOTUS\DOMINO\xercesImpl.jar
```

```
QPJC3=C:\LOTUS\DOMINO\xalan.jar
```

```
QPJC4=C:\LOTUS\DOMINO\xml-apis.jar
```

```
QPJC5=C:\LOTUS\DOMINO\log4j-118compat.jar
```

```
QPJC6=C:\LOTUS\DOMINO\data\domino\java\cs.jar
```

```
QPJC7=C:\LOTUS\DOMINO\ibmjsse.jar
```

```
QPJC8=C:\LOTUS\DOMINO\STCore.jar
```

```
QPJC9=C:\LOTUS\DOMINO\STMtManagement.jar
```

6. On the Team Workplace server, create a qpconfig.xml file in the data directory if one does not exist. Then open the qpconfig\_sample.xml file and copy the following <sametime> XML section to qpconfig.xml. Within the <credentials> element, add the name and password of the user you created in Step 1. More detailed information on the XML is provided in qpconfig\_sample.xml.

```
<sametime local_users="false" ldap="true">
  <meetings invite_servers="false">
    <tools>
      <audio enabled="true"/>
      <video enabled="true"/>
    </tools>
    <credentials>
      <dn>cn=John Doe/o=Enterprise</dn>
      <password>password</password>
    </credentials>
  </meetings>
</sametime>
```

**Note** The <local\_users> attribute should be "false." Team Workplace 6.5.1 does not support local users using Sametime.

7. Open a browser and enter the URL of the Team Workplace server. For example, <http://servername.enterprise.com/QuickPlace>.
8. Click SignIn in the left corner of the screen.

9. Enter the user name and password of a QuickPlace server administrator.
10. Click Server Settings in the table of contents.
11. Click Other Options in the table of contents.
12. Click Edit Options.
13. Under Sametime Servers, enter the full URL of the Sametime Meeting Server. For example, <http://meetingserver.enterprise.com>
14. Click Next.
15. Do the following to enable place members to schedule online meetings. This setting is enabled by default, but you should check to ensure it is actually enabled in any Place where members will be collaborating online.
  - a. Sign in to Team Workplace.
  - b. Click My Places, and open a place.
  - c. Click Customize.
  - d. Click Basics.
  - e. Click Change Basics.
  - f. Scroll down to the bottom of the Change Basics page. Under the Real-time collaboration heading, make sure “Members can schedule online meetings” is checked.
  - g. Click Done.
16. To test Meeting Services, create a calendar entry in a Place. Choose Calendar - New - Online Meeting. Fill in the relevant fields, and click Publish. Users who subscribe to calendar events should receive an invitation in their mail, with a link to the meeting. For more information on subscribing to calendar events, see the Team Workplace Help by clicking Help in a place.

## Setting up awareness and chat for Domino Web Access

<i>Portal system</i>	<i>Team Workplace system</i>	<i>Sametime system</i>
WebSphere Portal <i>(Installed) (Configured for LDAP) (Configured for SSO) (Configured for Lotus products)</i>	Domino Enterprise Server <i>(Installed)</i>	Domino Enterprise Server <i>(Installed)</i>
WAS <i>(Installed)</i>	Domino LDAP <i>(Configured)</i>	Sametime <i>(Installed) (Configured) (Configured for SSO)</i>
Cloudscape <i>(Installed)</i>	Team Workplace <i>(Installed) (Configured) (Configured for SSO)</i>	
Portlets/sample pages <i>(Installed) (Configured)</i>	Domino Document Manager <i>(Installed) (Configured)</i>	
Lotus Notes <i>(Installed) (Configured)</i>	Workflow <i>(Installed) (Configured)</i>	
	Domino Web Access <i>(Installed as part of Domino) (Configure now)</i>	

The Domino Web Access (iNotes) portlet integrates Sametime so that users can send and receive instant messages, maintain a Sametime contacts list, and have the names of people in mail messages, views and folders be online-aware.

In Domino Web Access, the Sametime integration features rely on the ability of the browser to communicate directly with the Sametime server. This means that the fully-qualified Internet hostname of the Sametime server must be resolvable from the browser (for example, the fully qualified Internet hostname for a Domino server named IM/Acme might be im.acme.com). Therefore, either DNS must be able to resolve this address or it must be resolved to the proper IP address by some other mechanism (such as editing the local operating system's hosts file).

As for security, the single-sign on configuration you have already completed for Domino on the Team Workplace system will handle authentication in Domino Web Access.

Perform the steps in the following sections to in order to be able to use awareness and chat in the portlet.

### Part 1 - Set up Domino Web Access on the Team Workplace system

1. In the Domino Administrator, make sure that the Fully Qualified Domain name (FQDN) (such as acme.lotus.com) for Domino on the Team Workplace system is specified on the Basics tab of the Server document.
2. Register users with the Domino Web Access (iNOTES6.NTF) mail template.
3. Add the following setting to the NOTES.INI file:  
iNotes\_WA\_SametimeServer=*hostname* where *hostname* is the fully qualified domain name of the Sametime server.

### Part 2 - Copy the Sametime server related files between the Sametime server and the Domino server

Use the following steps to copy the files needed to provide awareness in Domino Web Access to the Domino server so that the browser will be able to access them.

1. Create a Sametime folder under the Domino server directory on the Team Workplace system (if one does not exist):  

```
<data directory>\domino\html\Sametime\stlinks\
```
2. Copy the contents of the Sametime server stlinks folder to the stlinks folder you just created, using the OS File Manager.  
**Note** Another way to do this is, on the Sametime server, zip the \domino data directory\domino\html\sametime\stlinks\ directory. Be sure to include all the files under the stlinks directory on the Sametime server. Copy the zip file to the Domino server and unzip it to the same directory on the Domino server.
3. (Mozilla only) If the stlinks.jar file in the stlinks directory is not a signed version, replace it with a signed stlinks.jar file. In Sametime 6.5.1 this file is on the Sametime server in the folder <server directory>\Data\domino\html\sametime\stlinks\signed.

### Part 3 - Verify that Sametime works with Domino Web Access

1. Restart the Team Workplace server.
2. Follow the instructions in the *Sametime Installation Guide* for logging into the Sametime server using the Sametime Connect Client. Sametime must be functioning properly before you can test whether it is working with Domino Web Access clients.
3. Launch Domino Web Access in a browser and log in.
4. Choose Preferences - Other, and then select "Enable Instant messaging."

5. Click “Chat” to test the Sametime connection.

**Note** If the chat link does not appear in Domino Web Access, check that `iNotes_WA_SametimeServer=hostname` has been added to the NOTES.INI file, making sure that *hostname* is the fully qualified domain name of the Sametime server, and check that the “Enabling instant messaging” preference is selected.

For a list of NOTES.INI settings you can use to modify the default Sametime setup for Domino Web Access, see Lotus Domino Administrator 6.5.1 Help.

---

## Setting up awareness and chat for the Notes View portlet (Domino Databases)

The Domino Databases portlet in the sample pages (created from the Lotus Notes View portlet) lets you work with the documents from any view of any Notes database. You can include the awareness and chat features in a view by doing the following:

1. Select the Edit button (pencil) in the upper right corner of the portlet.
2. In the Available Views section, select Add.
3. In the View Title section, enter “Inbox”.
4. In the Server section, specify the server name where the mail file is located (for example, `king.notesdev.ibm.com`). Select the checkbox next to the Server section.
5. In the Database filename section, select the mail file path, for example, “mail”, and then select “ptest1.nsf”. Select the checkbox next to the Database filename section.
6. In the View section, select the view name (“Inbox”) that corresponds to the View Title entered earlier.
7. Select Next at the top/bottom of the page.
8. Select a column that contains names from the “Column for showing people awareness” drop-down list.
9. Select Done at the top/bottom of the page.
10. Select Save at the top/bottom of the page.
11. Add more views to the portlet (steps 4 - 7) if desired.

---

## Chapter 3 Troubleshooting

This chapter describes how to recognize problems in the Domino-Portal environment and offers a general strategy as well as some specific techniques for solving them. A Known Issues section provides information on known problems in Domino and Extended Products 6.5.1 and WebSphere Portal 5.0.2.

---

### Troubleshooting in the Domino-Portal Environment

Using Lotus Extended Products portlets with WebSphere Portal involves installing a set of products and configuring them to work together. Because there are so many points of interaction between products, there are many points at which things can go wrong, and problem isolation can be difficult.

This section assumes that you already have a detailed knowledge of how to troubleshoot server products in general, but provides product-specific information that you will need in order to isolate a problem in the portal environment.

The following list of the major points of interaction between products in the portal should help you focus on the areas you need to check when products aren't working together as they should:

<i>This product</i>	<i>May interact with these products</i>
WebSphere Portal/WebSphere Application Server	Database server Web server LDAP/single sign-on
Portlets	LDAP Domino server Instant Messaging and Web Conferencing (Sametime) Team Workplace (QuickPlace) Document Manager (Domino.Doc) Domino Web Access (iNotes)
Sametime	LDAP/SSO

*continued*

<i>This product</i>	<i>May interact with these products</i>
Team Workplace	LDAP/SSO Sametime
Document Manager	LDAP/SSO Sametime
Workflow	LDAP/SSO Sametime
Domino Web Access	LDAP/SSO Sametime

## How the products interact

To isolate a problem, you must first understand how all the products interact when things are working properly. Here's what should happen:

### WebSphere Portal login

1. A user enters the URL to load a page served by the WebSphere Portal server (for example, <http://myServer.myOrg.com/wps/portal>), and then clicks "Log in." Or, the user directly connects to the authentication page via <http://myServer.myOrg.com/wps/myPortal>.
2. The user enters their login credentials (user name and password). The user's credentials are then validated against an LDAP directory by performing an LDAP bind operation, or they are validated against the custom user registry used by the WebSphere Portal Server. This is dependent on how WebSphere Portal is configured.
3. If single sign-on (SSO) has been configured, a Lightweight Third Party Authentication (LTPA) token is generated by the WebSphere Application Server, which contains the user's LDAP name associated with their user name and password encrypted using the special SSO key. This is sent to the user's browser as a cookie. A session cookie is also sent. (The user's Web browser must be configured to accept cookies.)

### Administration of LDAP users and groups

The WebSphere Portal administrator can use the Administration tool to modify access control records in the database associated with WebSphere Portal (Cloudscape, DB2, and so on), as well as to modify LDAP entries themselves. In either case, WebSphere Portal must be able to communicate with LDAP. Modifying access control for a user starts with an LDAP search to find the user. An action like deleting a user writes to LDAP.

### Authentication by portlets

1. When a page loads containing a portlet (Sametime, Team Workplace, Notes View, and so on), the portlet will attempt to contact a collaborative service such as Team Workplace or Sametime, usually using HTTP, or use HTTP or IIOP to open a remote Notes database. If single sign-on is enabled, the cookie generated in the previous step is retrieved and the LTPA token contained within the cookie is passed to the remote service.
2. The remote Domino service extracts the user's LDAP name from the LTPA token. Each Domino domain has its own Web SSO Configuration document. This document must exist in each server's copy of the Domino Directory. The single sign-on key contained within the Web SSO Configuration document is used to decrypt the user's credentials.
3. The user's credentials are then used to search either the local directory or an LDAP directory (depending on what service is being used and how directory assistance is configured for that service) in order to establish the user's identity and access rights.

### Sametime awareness integration

The portlets use STLinks for awareness integration. STLinks enables a developer to place Sametime "live names" into an HTML page or other application. Users can click on live names to chat with other users.

1. When a user accesses a STLinks-enabled portlet, an STLinks applet loads from the portlet to the Web browser on the user's machine. This applet supports the live names.
2. The applet connects from the user's machine back to the Community Services on the Sametime server using the HTTP protocol with a default port of 8082. This port is configurable by the administrator.

The following table lists the various Sametime clients and their connection methods for awareness integration. Except in the case of Lotus Notes, the administrator can configure alternate ports. For Sametime Connect, the administrator can configure alternate protocols.

<i>Instant Messaging (Sametime) client</i>	<i>Connection method</i>
Lotus Notes	VP protocol: port 1533
Domino Web Access (iNotes)	HTTP: port 8082
Team Workplace (QuickPlace)	HTTP: port 8082
Java Connect	Sametime protocol over TCP: port 1533
Sametime (non-Java) Connect	Sametime protocol over TCP: port 1533
Contact List portlet	HTTP: port 8082

### **Common problems**

Most of the problems that occur involve the LDAP service, as each configuration may use a different form of LDAP distinguished names, and the LDAP search algorithm must be configured to match the chosen form of the LDAP name. There are also problems with Sametime-based portlets and with Sametime awareness in other portlets, as there are multiple mechanisms to contact the Sametime server, and as the Sametime server may be exposed to multiple name forms for the same person.

For an overall strategy for isolating problems, see the next topic, “Troubleshooting strategy.”

---

## **Troubleshooting strategy**

Many problems that do not result in the display of an error message are recorded in server logs by default. Also, many problems that display an error message display additional information in logs. If reviewing the logs does not reveal a problem, raise the logging level on the protocol that the two products use to communicate. As examples, if a user can't log in to WebSphere Portal, assume that the problem has something to do with LDAP, and turn on LDAP tracing. If the My Lotus Team Workplaces portlet is not working, turn on tracing for the HTTP protocol, which most portlets use to access the services of Domino or one of the extended products.

Use the following strategy whenever you approach a problem:

1. Read any error messages carefully to see if they suggest a solution. For example, if a message says “You must allow cookies for WebSphere Portal to work,” the user probably has the browser set to refuse cookies. If you still can't solve the problem, proceed to step 2.
2. See if a workaround for the problem exists by checking the Known Issues section of this chapter, as well as the individual release notes for the product or products in which the problem is occurring. If not, proceed to step 3.

3. Examine all the operation log files on all the servers involved. If the problem is installation, examine all the installation log files. You can find the log files for each server in the following locations:
  - WebSphere Portal: <wps\_root>\log
  - WebSphere Application Server: <wps\_root>\log (installation); <was\_root>\logs (operation)
  - IBM HTTP server: <wps\_root>\log (installation); <ihs\_log>\logs (operation)
  - Domino: LOG.NSF in the Domino data directory, or the ASCII console log
  - Other LDAP directories: See the documentation for the LDAP directory you are using
  - Sametime: STLOG.NSF in the Domino data directory
  - Team Workplace: LOG.NSF in the Domino data directory
  - Document Manager: *librarynameLog.nsf*, in the Document Manager directory (typically \domdoc)
  - Domino Web Access: HTTP logging is off by default. DOMLOG.NSF in the Domino data directory and/or text file logging can be enabled during problem analysis to provide additional information.

For descriptions of the various WebSphere logs, see the Portal InfoCenter topic “Using Logs.”

If a message in the log files does not lead you to the solution, proceed to step 4.

4. Do one of the following, depending on the nature of the problem:
  - If it appears a service is not responding at all, first check that, from the accessing system, you can ping the server that is hosting the service. If so, check that the service is available independently of the accessing application. For example, use an LDAP client such as LDAPSEARCH (located in the Domino directory) to verify that the LDAP server is available and that the search returns the proper result. If the service is not available, solve that problem first and then go back and try the portlet again.
  - If the service is available, but there is a problem with security, login, or authentication, turn on tracing on the LDAP server, and use a Web browser to test single sign-on. From the browser, access a Web page on a server that requires authentication — for example, your mail file on a Domino server. Then, without exiting from the browser, access a Web page on another server that also requires authentication. Single sign-on is working if you are not prompted for a name and password.

- If the service is available, but there is a functional problem with a portlet, investigate that server and its service by turning on HTTP or IIOP tracing.
- Turn on single sign-on (SSO) tracing by adding `DEBUG_SSO_TRACE_LEVEL=2` to the NOTES.INI file.

### Notes

- You can log all incoming TCP/IP connections in Domino by entering the following command at the console:  

```
Set config log_connections=1
```
- To get a more accurate picture of the HTTP or LDAP communications between a client and a server, a useful tool is to place a proxy application between the client and server for the protocol under investigation and log what goes through the proxy.

## Troubleshooting a lack of Sametime awareness in portlets

If you do not see awareness in a portlet, do the following to try to determine what the problem is:

1. Verify that the server name is configured properly.
  - a. Ping the server by host name to determine if you have access to the server.
  - b. Do an nslookup on the host name to determine if the host name exists at all.
  - c. Telnet the host name port number to determine if you have access from the client to the server and if the server is listening on the right port.
  - d. Use the `netstat -a` command to list all connections. If you see a connection from any port on the local machine to the specified port on the server, you have a connection.
2. Verify that proxy settings are configured correctly.
  - a. Verify the settings.
  - b. Use the same steps that you did for the server name above to check connectivity to the proxy.
3. Verify that the Sametime server is configured properly.
  - a. Telnet from the client to the server to determine if the server is configured properly.
  - b. On the Sametime server, use the `ipconfig -na` command to provide a list of all connections. The connections that are specified as LISTENING are the ones that the server is listening on.

## Turning on LDAP tracing

### For Domino LDAP

Enter the following command at the console:

```
Set config ldapdebug=15
```

For Technotes that contain more information on troubleshooting Domino LDAP, search on 7003663 and 7003823 (the Technote numbers) at <http://www.ibm.com/support>.

### For other LDAP directories

Enable LDAP logging for the LDAP directory you are using and then search in the log for the failure associated with the problem that you are experiencing.

The following are some examples of LDAP operations messages you may find in the log of your LDAP directory:

<i>Message</i>	<i>Description</i>
resultCode 32 (No such object)	Indicates that a search operation was attempted but the BaseDN supplied was not found. It may also occur if a bind operation is attempted using a user name with an invalid format. For example, you could get this error if you attempt to bind with the user name "John Doe" instead of the hierarchical name of "cn=John Doe, o=YourOrg".
resultCode 49 (Invalid credentials)	Indicates that a bind operation was attempted but the user name or password supplied was invalid or incorrect.
resultCode 65 (Object class violation)	Indicates that an LDAP operation was attempted but failed schema checking.
resultCode 50 (Insufficient access)	Indicates that an LDAP operation was attempted by a user who did not have sufficient privileges to complete the operation.
resultCode 0 (Success)	Indicates a successful operation. <b>Note</b> If you are doing a search for a specific entry and the entry cannot be found in the DIT, a Success message will be passed back because the search has completed successfully.

## Turning on HTTP tracing for the Domino Web server

You can log Domino Web server requests to a database or to text files. Text files are smaller and can be used with third-party analysis tools. Logging to the Domino Web Server Log database (DOMLOG.NSF) allows you to create views and view data in different ways. However, the size of the database can become large so that maintenance becomes an issue.

You can log to both text files and a database. These options are not mutually exclusive.

**Note** Some information may increase the size of the log files without providing meaningful information — requests for graphics or icons, for example, so you may want to exclude that type of information from the logs.

For more information, see Lotus Domino Administrator 6.5.1 Help.

### Setting up logging for text files

To set up text file logging for the Domino Web server, you must enable first logging. By default, Domino stores log files in the data directory. While the Web server is running, new log files are created based upon the log file duration setting. By default, these log files are stored in the Domino data directory.

To enable logging to text files

1. From the Domino Administrator, click the Configuration tab.
2. Open the Server document for the Web server.
3. Click the Internet Protocols - HTTP tab.
4. Under “Enable Logging To,” select Enabled in the Log Files field.
5. Complete the remaining fields.
6. Save the document.

### Setting up DOMLOG.NSF

To set up Domino Web server logging for the Domino Web server, you must first enable logging. Domino then creates the Web server log database when the HTTP task is started. You can restrict the amount of information captured in the Domino Web server log to better analyze log file results.

To enable logging to the Domino Web server log

1. From the Domino Administrator, click the Configuration tab.
2. Open the Server document for the Web server.
3. Click the Internet Protocols - HTTP tab.
4. Under “Enable Logging To,” select Enabled in the DOMLOG.NSF field.
5. (Optional) Complete the remaining fields.

6. Save the document and then restart the HTTP task so that the changes take effect.

### **Logging HTTP transactions by individual threads**

If text files and the Web server log do not provide sufficient information, you can also log HTTP transactions by individual threads, or sessions. For more information, see the white paper “Domino 6: Overview of HTTP Request Logs,” no. 7003598, at <http://www.ibm.com/support>.

## **Turning on DIIOP logging in Domino**

A few portlets use the DIIOP protocol to access Domino services. To turn on DIIOP logging in Domino, enter the following command at the console:

```
tell diiop log=4
```

For more information on troubleshooting DIIOP, see the Troubleshooting section of the LDD Today article “Java access to the Domino Objects, Part 2.” available at [www.lotus.com/ldd](http://www.lotus.com/ldd).

---

## **Known issues**

This is a supplemental list of known issues involving extended product installation and interoperability for Domino and Extended Products 6.5.1 and WebSphere Portal 5.0.2. To learn of all known issues, you must read the release notes for every product you are using. Release notes for individual products may be updated more frequently than this guide.

Release notes for Lotus products are available at <http://www.lotus.com/ldd/doc>.

Release notes for WebSphere Portal 5.0.2 are available at <http://www.ibm.com/websphere/portal/library>.

For guidelines on troubleshooting Domino Application Portlet, see the chapter “Domino Application Portlet Reference.”

## **WebSphere Portal**

If a portlet launches another browser window with a full application user interface that includes a logout, such as Team Workplace, and if you log out of that Team Workplace browser window and try to return to WebSphere Portal, you get a WebSphere Portal login prompt. For a Technote that describes a workaround, search on 1158270 (the Technote number) on <http://www.ibm.com/support>.

## Lotus Team Workplace

Installing Team Workplace on a Domino server modifies the local server document. If this server is not the administration server, it is possible for the administration server to modify the server document at the same time, creating a replication conflict. If you encounter a problem with Team Workplace, check for a replication conflict server document.

## Lotus Instant Messaging and Web Conferencing (Sametime)

The following are known issues involving Sametime.

### **Problem with userID's when Sametime pointing to Active Directory using LDAP**

When authenticating to Sametime using a full DN, or when adding a user to the Contact List by the full DN, the userID may be incorrect. The returned userID is returned as requested, and not as stored in the directory. Other LDAP servers (IBM Directory Server, Domino, SunOne, and so on) do not have this problem.

**Solution:** In `stconfig.nsf`, change the "Attribute of the person entry that defines the internal ID of a Sametime user" to `DistinguishedName`. This is a special attribute in Active Directory that is equivalent to the DN, and always returned as stored in the directory.

### **Sametime Toolkits availability**

The Sametime 6.5.1 Toolkits will be provided as a separate Web download, available 60 days from product ship from the Lotus section of the IBM developerWorks web site ([www.ibm.com/developerworks](http://www.ibm.com/developerworks)). The toolkits are self-extracting files available only on W32. Once extracted, they can be moved on to any OS.

### **Sametime Java process doesn't exit on a Domino server shutdown on AIX**

There is an intermittent problem where a Sametime Java process doesn't exit upon shutting down Domino on AIX(R). When Domino is restarted, the Java process doesn't start, as Domino detects it is already running.

**Solution:**

On the UNIX(R) shell, enter the following commands:

1. `ps -elf | grep <notesuser>` (to verify that all Domino and Sametime processes are terminated)
2. `kill -9 PID` (to kill the Java process PID)
3. `ipcs -a` (to check for IPCs)

4. cd into the Notes data directory, and run /opt/lotus/bin/nsd -kill (to remove IPCs)
5. ipcs -a (to double check all are gone, if not use ipcrm to remove them)

## Lotus Domino Document Manager

The following are known issues involving Domino Document Manager.

### Correcting a registry problem detected by the Install program

The Document Manager Install program uses the server's Windows registry to locate Notes and to load the LotusScript Notes classes. The Install program looks for a registry key in the HKEY\_LOCAL\_MACHINE tree named SOFTWARE\Lotus\Components\LotusScriptExtensions\2.0. This key should contain the full path name of the Notes DLL nlsxbe.dll. If this key is missing, or refers to a file that does not exist, the Install program asks you whether you want it to try to repair your registry.

- If you answer Yes, the Install program checks the server's registry to find where Notes is currently installed and looks for the nlsxbe.dll file. If nlsxbe.dll is present, then Install writes the full path into the registry. Install looks for the Notes installation by checking the Path value under the HKEY\_LOCAL\_MACHINE\Lotus\Notes\4.0 key. If the Notes registry key is missing or incorrect, or the Path value is missing or incorrect, Install terminates without attempting to repair the registry. You must either repair the registry by hand or reinstall Notes.
- If you answer No, Install terminates. You must either repair the registry by hand, or reinstall Notes.

### Selecting "Who is Online" displays a blank gray box

Workaround for Web client users:

1. On the Document Manager server, Open domdoc.ntf in designer.
2. Open the WhoIsOnlineWeb form.
3. Modify the formula for the LDAP field to "true" (remove ALL contents and replace with "true").
4. Save and close the form.
5. Do a load design on the Document Manager server.

Workaround for Notes users:

1. On the Document Manager server, Open filecab.ntf in designer.
2. Open the WhoIsOnlineNotes form.
3. Make sure the Design pane is showing.
4. Click on the gray box (the embedded applet).
5. In the Design Pane, select “Applet Properties.”
6. Select the LDAP property, and change its value to “true” (remove ALL contents and replace with “true”).
7. Save and close the form.
8. Do a load design on the Document Manager server.

### **Notes/Domino and Extended Products Portlets**

If your configuration includes Sametime 6.5.1, you may see an “Object Error” message when you are in a portlet. Click OK to close the message box. This will be addressed in a future release.

### **My Contacts portlet**

A user can add a public group to the My Contacts portlet in the sample portal pages.

However, if Sametime is configured to use LDAP and the LDAP being used is not the Domino LDAP service but rather a service such as Active Directory, IDS, or iPlanet, the group name is added but no awareness is displayed for the users.

To see awareness, users must add individual user names.

---

## Chapter 4

# Domino Application Portlet Reference

This chapter describes how to install and configure the Domino Application Portlet for use with WebSphere Portal 5.0.2, 5.0, 4.2 or 4.1.2.

The Domino Application Portlet is included with the Notes/Domino and Extended Products Portlets 6.5.1. For more information, see the chapter “Setting Up a Pilot Configuration.”

---

### Domino Application Portlet Reference

The Domino Application Portlet allows users to access HTML-enabled Domino applications via WebSphere Portal. The portlet is installed on a portal page, like any other portlet, and acts as a window through which users interact with a Domino application.

**Note** The Domino Application Portlet includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Apache is a trademark of The Apache Software Foundation.

The following topics explain how to install and configure the portlet:

- Installation
- Configuration
- Transformation rules
- Troubleshooting

#### Overview

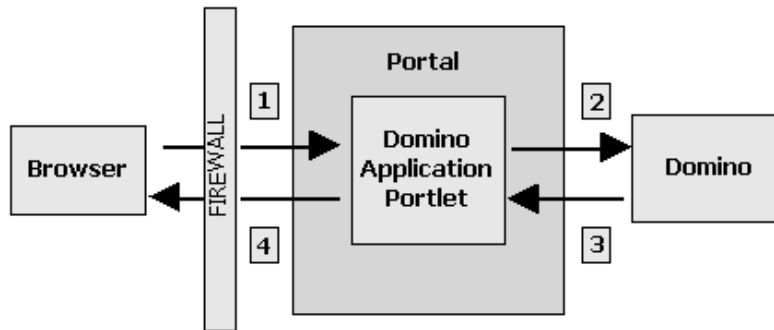
To summarize Domino Application Portlet features and operation:

- The Domino Application Portlet acts like a tunnel, channelling all requests from the user client (browser) through the portal and on to the Domino HTTP server in the back end.
- It manages cookies, caching, user authentication and framing.
- Rules-based parsers rewrite the content produced by the Domino HTTP server. The architecture allows for additional parsers to be plugged into the system.

- The Domino Application Portlet functionality is exposed as a portal service, allowing portlets to take advantage of the proxy with the minimum of coding effort.

The Domino Application Portlet acts like a reverse proxy server. Browsers are often configured to use a *forward* proxy server which intercepts browser requests and routes them through to the required back end server. A *reverse* proxy server works by proxying the content from the back end servers through to the browser. It appears to the browser to be the real content server.

Here is an overview:



All browser requests are directed to the portal:

- 1 A portal-page is requested by the browser; the portlet is called.
- 2 The “real” address is determined and a request is made to the Domino server.
- 3 The retrieved HTML is “transformed” to redirect any references to Domino server to the portal server.
- 4 The transformed HTML is returned to the browser.

### From Domino to the browser

The portlet intercepts the content generated by Domino and rewrites all URLs to point to the portlet itself.

A set of pattern matching rules is used to identify and rewrite URLs within the content. Rules can be configured for individual applications.

The portlet contains two components, a portlet and a servlet. The portlet handles requests such as href links and the servlet handles requests for graphics.

## From the browser to Domino

The portlet intercepts browser requests, passes these on to Domino and passes the results after modification back to the browser.

## iFrame

The Domino Application Portlet uses an HTML iframe (inline frame) tag to display Domino applications. This allows it to handle framesets. In such cases, the browser still communicates with the portal.

---

## Installation

For WebSphere Portal 5.0.2, Domino Application Portlet is one of the portlets installed as part of Notes/Domino and Extended Products Portlets 6.5.1.

For information on installing the Notes/Domino and Extended Products Portlets, see the chapter “A pilot configuration for Domino Extended Products and WebSphere Portal.”

For earlier versions of WebSphere Portal, the installation of Domino Application Portlet is the same as for any other portlet. For detailed information about WebSphere Portal procedures go to <http://publib.boulder.ibm.com/pvc/wp/500/ent/en/InfoCenter/index.html>.

The following sections describe the procedure:

- Prerequisites and system requirements
- Installing on WebSphere Portal 5.0
- Installing on WebSphere Portal 4.2
- Installing on WebSphere Portal 4.1

### Prerequisites and system requirements

- The application that the Domino Application Portlet is to access must be installed on Domino Release 5.0.12, 6.5 or 6.5.1.
- WebSphere Portal 5.0.2, 5.0, 4.2 or 4.1.2 must be installed on a different machine from the Domino server.
- The Domino server must be accessible from WebSphere Portal.
- Supported browsers are Internet Explorer 5.5 and 6. Mozilla 1.3.1 for Linux is supported only for the following templates: Mail6.ntf, Mail6ex.ntf, Mail50.ntf, and Mail50ex.ntf, and only for 5.0.12 (or greater) and 6.0.2 (and greater).

- The standard transformation rules shipped with Domino Application Portlet have been tested with the following standard Domino templates:

6.5/6.5.1 Discussion Database (DISCSW6.NTF)

6.5/6.5.1 Teamroom Database (TEAMRM6.NTF)

6.5/6.5.1 Resource Reservations Database (RESRC60.NTF)

6.5/6.5.1 Mail Database (MAIL6.NTF)

5.0.x Discussion Database (DISCSW50.NTF)

5.0.x Teamroom Database (TEAMRM50.NTF)

5.0.x Resource Reservations Database (RESRC50.NTF)

5.0.x Mail Database (MAIL50.NTF)

For other Domino applications, you may need a different rule set. You can either customize the shipped rule set or create a new rule set from scratch.

## Installing Domino Application Portlet on WebSphere Portal 5.0

To install Domino Application Portlet:

- 1 Copy the Domino Application Portlet install file (.war) for WebSphere Portal 5.0 to the machine that you will use to carry out the installation, and launch a browser on that machine.
- 2 On the WebSphere Portal opening display, click **Log in**.
- 3 Type your User ID and Password (you must have administrator access rights).
- 4 Click **Administration** in the banner.
- 5 Click **Portlets** in the navigation tree.
- 6 Click **Install** in the Portlets section of the navigation tree.
- 7 Browse for the Domino Application Portlet install file.
- 8 Click **Next**.
- 9 Verify that the portlet information that appears is correct.
- 10 Click **Install**. After the installation has completed, a message should appear at the top of the screen indicating a successful installation.

To add Domino Application Portlet to a page:

- 1 On the WebSphere Portal opening display, click **Log in**.
- 2 Type your User ID and Password (you must have appropriate access rights).
- 3 Navigate to the page where you want to add the portlet.
- 4 Click **Edit Page** in the banner.

- 5 Click **Content** to view the available containers.
- 6 Click the icon in an empty container to add portlets.
- 7 Click **Search** to locate the Domino Application Portlet. There may be several copies of the Domino Application Portlet (concrete portlets) with different settings.
- 8 Check the box next to the copy of the portlet you want to base the new instance on.
- 9 Click **OK** to add the portlet to the page.

Once Domino Application Portlet has been added to a portal page you must configure it.

The result of the installation is a concrete portlet with default title, rules and language. If you need to modify these default settings:

- 1 Select **Administration** in the banner.
- 2 Select **Portlets** in the navigation tree.
- 3 Select **Manage Portlets**.
- 4 Select the Domino Application Portlet.
- 5 Click **Modify parameters** (wrench icon).
- 6 Edit the parameters. For information about rules see Transformation rules.
- 7 Click **Save** to save your changes or **Cancel** to abandon them and return to the previous display.

## Installing Domino Application Portlet on WebSphere Portal 4.2

To install Domino Application Portlet:

- 1 Copy the Domino Application Portlet install file (.war) for WebSphere Portal 4.2 to the machine that you will use to carry out the installation, and launch a browser on that machine.
- 2 On the WebSphere Portal opening display, click **Log in**.
- 3 Type your User ID and Password (you must have administrator access rights).
- 4 Click **Portal Administration** in the banner.
- 5 Click **Portlets** in the navigation tree.
- 6 Click **Install Portlets** in the Portlets section of the navigation tree.
- 7 Browse for the Domino Application Portlet install file.
- 8 Click **Next**.
- 9 Verify that the portlet information that appears is correct.

- 10 Click **Install**. After the installation has completed, a message should appear at the top of the screen indicating a successful installation.

To add Domino Application Portlet to a page:

- 1 On the WebSphere Portal opening display, click **Log in**.
- 2 Type your User ID and Password (you must have appropriate access rights).
- 3 Click **Work with Pages** in the banner.
- 4 Select **Edit My Pages**.
- 5 Click **Edit page composition**.
- 6 From **Available places**, select the place that contains the page where you want to add the portlet.
- 7 From **Pages in the place**, select the page.
- 8 Click **OK**.
- 9 Click **Add content** to display all available portlets.
- 10 Select Domino Application Portlet from the list.
- 11 Click **OK** and then **Done**.

Once Domino Application Portlet has been installed you must configure it.

The result of the installation is a concrete portlet with default title, rules and language. If you need to modify these default settings:



- 1 Select **Portal Administration** in the banner.
- 2 Select **Portlets** in the navigation tree.
- 3 Select **Manage Portlets**.
- 4 Select the Domino Application Portlet.
- 5 Click **Modify parameters**.
- 6 Edit the parameters. For information about rules see Transformation rules.
- 7 Click **Save** to save your changes or **Cancel** to abandon them and return to the previous display.

## Installing Domino Application Portlet on WebSphere Portal 4.1

To install Domino Application Portlet:

- 1 Copy the Domino Application Portlet install file(.war) for WebSphere Portal 4.1 to the machine that you will use to carry out the installation, and launch a browser on that machine.
- 2 Log in to WebSphere Portal. You must have administrator access rights to install the portlet.
- 3 Select **Portal Administration** from the dropdown list in the banner.
- 4 Select the **Portlets** tab and then **Install portlets**.
- 5 Browse for the Domino Application Portlet install file.
- 6 Click **Next**.
- 7 Verify that the portlet information that appears is correct.
- 8 Click **Install**. After the installation has completed, a message should appear at the top of the screen indicating a successful installation.

To add Domino Application Portlet to a page:

- 1 On the WebSphere Portal opening display, click **Log in**.
- 2 Type your User ID and Password (you must have appropriate access rights).
- 3 Select the **Work with Pages** from the dropdown list in the banner.
- 4 Select **Edit Layout and Content**.
- 5 From the **Place** dropdown list select the place that contains the page where you will add the portlet.
- 6 From the **Page** dropdown list select the page where you will add the portlet.
- 7 Click **Get Portlets**.
- 8 Locate the Domino Application Portlet. Either:
  - Select **Show all portlets**, or
  - Select **Search for portlets / Name contains** and enter part of the portlet name.
  - Click **Go**.
- 9 Click **Add to portlet list**  
  
and then **OK**.
- 10 Highlight the Domino Application Portlet and click **Add portlets**  


- 11 Highlight the Domino Application Portlet and click **Activate**

Once Domino Application Portlet has been installed you must configure it.

The result of the installation is a concrete portlet with default title, rules and language. If you need to modify these default settings:

- 1 Select **Portal Administration** from the dropdown list in the banner.
- 2 Select **Portlets** in the navigation tree.
- 3 Select **Manage Portlets**.
- 4 Select the Domino Application Portlet.
- 5 Click **Modify parameters**.
- 6 Edit the parameters. For information about rules see Transformation rules.
- 7 Click **Save** to save your changes or **Cancel** to abandon them and return to the previous display.

### Concrete portlets

It is possible to create many copies of a concrete portlet (see “Portlet API concepts” in the WebSphere Portal InfoCenter), and you can create different default settings for each. When you add Domino Application Portlet to a portal page you create an instance of a concrete portlet, with default settings taken from the concrete portlet on which it is based.

---

## Configuration

You can configure the Domino Application Portlet in either of the following ways:

- By using the portlet’s configuration mode (described here), or
- By using Portal Administration to modify the parameters of the concrete portlet (see Installation).

In either case, you must have administrator access rights. Any configuration changes you make will affect:

- All current portlet instances of the concrete portlet.
- All future portlet instances created from the installed concrete portlet.

For information about concrete portlets see “Portlet API concepts” in the WebSphere Portal InfoCenter.

To configure the Domino Application Portlet using configuration mode:

- 1 Navigate to the page that contains the portlet.
- 2 Click the wrench icon at the right of the Domino Application Portlet title bar. You will see the configuration display. Click the tabs to move between the various sections of the configuration display.

**Note** If the wrench icon is not displayed, check that you do have administrator access.

- 3 Select the **Source and Display** tab. Under **Domino Source Server** enter the following information:
  - For **Protocol**, select the protocol that the Domino server uses for Web access: HTTP or HTTPS. Select HTTPS to connect to Domino over SSL (secure sockets layer).
  - For **Host**, enter the name of the server that hosts the Domino application. The format must be the internet name format, for example **myserver.mycompany.com**.
  - For **Port**, enter the port number used for Web access to the Domino server. This will normally be 80 for HTTP and 443 for HTTPS.
  - For **Path and file name**, the path and filename of the Domino database application to be accessed, relative to the Domino data directory. Optionally, you can include a command that manipulates an item such as a document or view, for example **discussion.nsf/By+Author?OpenView&ExpandView**. For more information see Domino Designer 6 Help - Application Design - URL comands for Web applications - Domino URL commands.

Under **Proxy Source Server** enter the following information if a proxy server is used to access the Domino Server:

- For **Host**, enter the name of the proxy server.
- For **Port**, enter the port number used by the proxy server.
- Under **Frame** enter the following information:
  - The Domino Application Portlet uses an HTML iframe (inline frame) tag to display Domino applications. For **Width**, enter a width for the iframe. 100% is the default setting.
  - For **Height**, enter a number of pixels. 500 is the default setting.
  - For **Border**, enter a number of pixels if you want to add a border to the iframe. Enter 0 if you do not want a border.
- For **Portlet title** enter the text that will appear in the portlet's title bar, for example the name of the Domino application the portlet will access.





If you want any of the settings to appear on the edit mode display available to users, check the appropriate **Show in edit mode** boxes.


- 4 Select the **Authentication** tab and specify:
  - The authentication model used by the Domino application. The options are **None**, **Basic**, **Session**, or **Single Sign-on (SSO)**. For more information see Authentication in Domino.  
**Note** It is possible to authenticate by configuring the Domino Application Portlet with a lower model than the Domino server requires. For example, you can authenticate against a Domino server configured for single-session authentication by specifying Basic authentication in the Domino Application Portlet. However, you should generally match the portlet authentication model with the Domino server it is accessing.
  - If you selected Basic or Session as the Domino authentication model, then select the appropriate WebSphere Portal Credential vault setting: **Private slot**, **Shared slot** or **System slot**. And if you select System slot as the credential vault setting, enter the name of the slot under **System slot identifier**. For more information, see Authentication in WebSphere Portal.
- 5 Select the **Caching** tab. The Domino Application Portlet can cache data items from the Domino server that are unlikely to change between requests. For more information, see Caching. Specify the following parameters:
  - Caching methods to use. Select one or more of **User and application**, **User**, **Application** and **Shared** (the default, implying that the cached items are the same for every user and application). If you do not select any of these, no caching will be carried out.
  - Objects to cache. In the **Mime types** list, select the mime types of the objects that are to be cached by each of the methods you have selected. Use Ctrl+click to select several objects. To select mime types that are not on the list, enter them under **User-defined mime types**, separated by spaces. By default, all image and applet mime types are selected.
  - For shared caching, under **URL contains**, you can enter one or more text strings separated by semi-colons (;). An object will only be cached if its URL contains one or more of the strings. If you do not enter any strings, all objects with the selected mime types will be cached.
  - For **Maximum number of items**, enter the maximum number of items that are to be held in the cache. The default is 100.

- For **Maximum item size**, enter the maximum size, in kilobytes, for items in the cache. Items larger than this will not be cached. The default is 250 Kb.
- 6 Select the **Rules** tab if you want to modify the rules that will transform the data flowing from the Domino application to the client.
- The portlet uses the rules displayed here for data transformation (see Transformation rules). To switch from regular expression rules to HTML and JavaScript rules, or vice versa, select Regular Expression or HTML as the **Rule Type**.  
Data is preserved when you select the Rule Type. For example, if you select HTML to display HTML and JavaScript rules, any regular expression rules you have entered will be preserved.  
**Caution** Before editing rules it is advisable to create a backup copy of the existing rules by clicking Export (see below). Also, remember to click Save to save any rule changes you make, otherwise they will be lost.
  - If you selected regular expression rules, the **Regular Expression Rules** table is displayed. In the left hand column enter a regular expression for the input. In the central column enter the output model, which determines how any text that matches the input expression is to be transformed. In the right hand column you can enter a note that explains what the rule does. See Regular expression rules. Regular expressions in Domino Application Portlet are not case-sensitive by default. To make the regular expression for an input expression case-sensitive, tick the **Case sensitive** checkbox for the rule. This only affects matching of the input: it does not affect the output.
  - If you selected HTML and JavaScript rules, the **HTML Rules** and **JavaScript Rules** tables are displayed. Enter HTML rules in the upper table and JavaScript rules in the lower table. For information about the columns see HTML rules and Regular expression rules (JavaScript rules use regular expressions).

The following buttons and icons are available in the Rules tab:

- Click **Export** to export the currently displayed rules to an XML file. See Importing and exporting rules, below.
- Click **Import** to import a set of rules from an XML file.  
**Caution** Importing will overwrite any existing rules.

- Icons:
  -  moves the rule one position up in the list.
  -  moves the rule one position down in the list.
  -  inserts a blank row for a new rule.
  -  deletes the rule.

- 7 Click **Save** to save the current settings and  or **Close** to close the Configuration display.

## Importing and exporting rules

You can save the rules currently displayed by clicking Export and supplying a file name. An XML file is created. The rules are exported in ascending order, with no breaks in the incrementing index, for example:

```
{rule_rex0,rule_output0,rule_comment0}
```

followed by

```
{rule_rex1,rule_output1,rule_comment1}
```

and so on. This is the format that the input function expects. If you decide to make changes to an exported rule set, and then import it back into the portlet, you must ensure that the content follows this formatting. We recommend, however, that you make any changes to the rules in the configuration display.

**Caution** If you import only a certain type of rule (for example regular expression rules), and edit the input file to reflect this, the resulting rule set in Domino Application Portlet will contain only rules of that type. All other rules will be deleted. The same is true if a you import a blank file or no file: the rules lists in the portlet will be emptied.

---

## Authentication in Domino

Internet access to Domino is authenticated against Domino's LDAP directory (usually NAMES.NSF, but may be external) and ACL of the target database, except in the case where Anonymous access is granted in the ACL. In order to configure the Domino Application Portlet you will need to know which authentication model the Domino application uses:

- No authentication
- Basic authentication
- Session-based authentication
- Single sign-on (SSO)

### No authentication

There is no authentication only if the target server and database have "Anonymous" access.

### Basic authentication

Basic password authentication, also known as name-and-password authentication, uses a basic challenge/response protocol to ask users for their names and passwords and then verifies the accuracy of the passwords by checking them against a secure hash of the password stored in Person documents in the Domino Directory. When set up for this, Domino asks for a name and password only when an Internet/intranet client tries to access a protected resource on the server. Internet/intranet access differs from Notes client and Domino server access in that a Domino server asks a Notes client or Domino server for a name and password when the client or server initially attempts to access the server.

For more information please refer to Notes Administrator Help (in Notes 6 the relevant topic is "Name-and-password authentication for Internet/intranet clients" under Security).

### Session-based authentication

Session-based authentication differs from basic password authentication in that the user name and password is replaced by a cookie. The username and password is sent over the network only the first time the user logs in to a server. Thereafter the cookie is used for authentication.

For more information please refer to Notes Administrator Help (in Notes 6 the relevant topic is "Session-based name-and-password authentication for Web clients" under Security, Name-and-password authentication for Internet/intranet clients).

## Single sign-on (SSO)

Single sign-on (multi-server session-based authentication) allows Web users to log in once to a Domino or WebSphere server, and then access any other Domino or WebSphere servers in the same DNS domain that are enabled for single sign-on (SSO) without having to log in again.

User Web browsers must have cookies enabled since the authentication token that is generated by the server is sent to the browser in a cookie.

You can set this up by creating a domain-wide configuration document — the Web SSO Configuration document — in the Domino Directory. You initialize the configuration document by importing LTPA keys from WebSphere (you will need the password specified when generating the keys in WebSphere). See “Creating a Web SSO configuration document” under Security, Name-and-password authentication for Internet/intranet clients in the Administrator Help for Notes 6.

You can enable single sign-on across multiple Domino domains.

For more information please refer to Notes Administrator Help (in Notes 6 the relevant topic is “Multi-server session-based name-and-password authentication for Web users (single sign-on)” under Security, Name-and-password authentication for Internet/intranet clients).

---

## Authentication in WebSphere Portal

The Domino Application Portlet uses the WebSphere Portal *credential vault* to handle authentication if the authentication model in Domino is basic or session-based. In such cases you will need to enter:

- The slot type to be used.
- For system slots, the slot name (identifier).

If no authentication is used in Domino (anonymous access) no credential vault settings are required.

If single sign-on (SSO) is used in Domino, access is inherent in the SSO framework and no credential vault settings are needed.

## The credential vault

The credential vault is organized as follows:

- The portal administrator partitions the vault into several vault *segments*. Vault segments can be created and configured only by portal administrators.
- Each vault segment contains one or more vault *slots*. Vault slots are the “drawers” where portlets, such as Domino Application Portlet, store and retrieve a user’s credentials (for example, login details). Each slot holds one credential.

Domino Application Portlet uses the default segment only.

## Vault slot types

Domino Application Portlet uses the credential vault provided by WebSphere Portal in one of the following three ways:

- 1 A system slot stores system credentials so that they are shared among all users and portlets. User login is not required. The administrator sets the user name and password in a new slot (in the default segment) via the portal settings. To create the slot:
  - In WebSphere Portal 5.0, select Administration in the banner and then Access in the navigation tree. Click 'Add a vault slot'.
  - In WebSphere Portal 4.2, select the Portal Administration place and then Credential Vault under Security in the navigation tree. Click 'Add a vault slot'.
  - In WebSphere Portal 4.1, select Portal Administration from the drop-down in the banner and then Security. Select the Credential Vault tab. Click 'Add a vault slot'.

**Important** Ensure that 'Vault slot is shared' is checked. Whatever slot name is used to create the slot must be entered as 'Slot identifier' in the Domino Application Portlet configuration display.
- 2 A shared slot stores user credentials that are shared among all Domino Application Portlet instances for a given user. Users enter login information using the portlet’s Edit mode, accessed via the pencil icon. Credential changes in one portlet instance are reflected in all other portlet instances (where Shared Slot has been specified) for that user.
- 3 A portlet private slot stores user credentials that are not shared among portlets. Users enter their login information using the Domino Application Portlet Edit mode. The login details (credentials) relate to the current portlet instance only.

---

## Caching

The Domino Application Portlet can cache frequently used objects in one or more of the following ways:

- 1 **User and application** (most secure) Cached objects can be accessed only by the user who put them into the cache, and only while accessing the current database application (caching can be shared across multiple portlet instances).
- 2 **User** Cached objects are shared by all applications, but can be accessed only by the user who put them into the cache.
- 3 **Application** Cached objects can be accessed by any user, but only while using the application that put them into the cache.
- 4 **Shared** (least secure) Cached objects can be accessed by any user or application, regardless of which application or user put them into the cache.

After activating any of these caching methods you select the mime types of the objects to be cached from a list. If an object falls into more than one active caching category, Domino Application Portlet uses the most secure basis for caching (order as listed above).

For Shared caching only, you can enter one or more text strings: an object can be cached only if one of the strings is present in its URL. This helps you to limit shared caching to objects that are common to all users. For example, you might enter **/icons** to ensure that icons are put into the shared cache.

You can also limit the size and number of cached objects. Cache limits apply overall and not per caching category. For example, if you limit the number of cached objects to 100, the total number of objects cached across all of the four categories cannot be more than 100. When the cache is full and an a new item is cached, the new item replaces the item with the oldest access date.

## Objects and mime types

The following table lists the mime types that can be selected for caching.

<i>Mime type</i>	<i>Object</i>
image/jpeg	JPG image
image/pjpeg	
image/bitmap	BMP image
image/x-bitmap	
image/x-pcx	PCX image
image/pict	PICT image
image/x-pict	
image/gif	GIF image
image/tiff	TIFF image
image/x-tiff	
audio/mpeg	Media clip
audio/x-mpeg-3	
video/mpeg	
video/x-mpeg	
video/avi	
video/msvideo	
application/excel	Microsoft Excel®
application/x-excel	spreadsheet
application/x-msexcel	
application/vnd.ms-excel	
application/mspowerpoint	Microsoft Powerpoint®
application/vnd.ms-powerpoint	presentation
application/powerpoint	
application/x-mspowerpoint	
application/msword	Microsoft Word® file
audio/midi	MIDI sequence
audio/x-mid	
audio/x-midi	
audio/wav	Wave sound
audio/x-wav	
application/rtf	Microsoft Wordpad®
application/x-rtf	document
application/java	Java applets
application/java-byte-code	
application/x-java-class	
application/x-java-applet	
application/octet_stream	

---

## Transformation rules

Domino Application Portlet uses a parser to transform data flowing from the Domino server to the client browser so that it appears to be coming from the portal. The parser transforms references in the input text (URLs, SRCs and so on) according to a set of rules. Each rule comprises:

- An input expression that defines the text the rule is looking for.
- An output model that specifies how to transform text found by the input expression.
- A comment to explain what the rule does (optional).

The rules transform data in the Domino-to-client direction only. Each rule encrypts the original URL and appends it to the end of the transformed URL. Domino Application Portlet achieves the reverse transformation by taking the original URL from the end of the transformed URL.

You can use either (but not both) of the following for data transformation:

- 1 A regular expression parser.
- 2 A combination of an HTML parser and a JavaScript parser. When the HTML parser finds any JavaScript it passes it to the JavaScript parser. The HTML parser uses HTML rules; the JavaScript parser uses regular expression rules.

You specify both the parsing model and the rules themselves on the configuration display. The portlet uses the rules that are currently displayed on the Rules tab. To switch between the two options select Regular Expression or HTML as the Rule Type. Also on the configuration display you can export rules to, and import rules from, an XML file.

Whichever parsing model you use, the rules must conform to the appropriate syntax (regular expression or HTML). The following topics provide more information:

- Regular expression rules
- HTML rules

---

## Regular expression rules

Domino Application Portlet uses the Jakarta regular expression parsing engine. For an introduction to regular expressions you can refer to the RE class API in the Jakarta regular expression package at <http://jakarta.apache.org/regexp/apidocs/>. The following sections explain how to use regular expressions in Domino Application Portlet:

- Input expressions
- Output model
- Processing
- Tips
- Output functions

### Input expressions

The input expression defines what the rule is to look for when searching a string, and it is defined by a regular expression. For example, the following input expression:

```
Path_Info = '(.*?)'
```

searches the input string for all instances where the exact text **Path\_Info** = (case-sensitive, including the trailing space) is followed by something inside quotes. The matching operators used in the example are:

```
( Start a grouping of operators
. Match any character
* Zero or more times
? Use minimum (reluctant) matching
) End the grouping of operators
```

In the following string:

```
this is some text belonging to an input string Path_Info =
'http://myserver.ibm.com' this quoted 'word' is also part
of
the string
```

the text **Path\_Info** = 'http://myserver.ibm.com' is a match for the input expression.

**Note** The ? operator prevents either of the longer strings:

```
Path_Info = 'http://myserver.ibm.com' this quoted '
```

or

```
Path_Info = 'http://myserver.ibm.com' this quoted 'word'
```

from being returned as a match.

Searching according to a regular expression breaks every match up into blocks defined by parentheses. So in the given example the block returned for the first set (1) of parentheses is **http://myserver.ibm.com**. There is also a block defined as set zero (0) which is the entire match **Path\_Info = 'http://myserver.ibm.com'**.

To include any of the regular expression meta characters in the text part of an input expression you must precede them with a backslash (\). The meta characters are:

```
( [ { \ ^ $ | ) ? * + . ,
```

## Output model

The output model comprises simple text combined with output functions. For example:

```
Path_Info = '@transform_uri_abs(@param(1))'
```

is an output model. In it, @transform\_uri\_abs() and @param() are both output functions. So in the example above, the text **Path\_Info = 'http://myserver.ibm.co'** found in the input string is replaced by

```
Path_Info = 'some output from the output functions'
```

in the output. Note the use of more than one output function in the output model.

## Processing

The regular expression parser processes rules in the order in which they appear on the configuration display (the Rules tab). The process of transforming input text is as follows:

- 1 Start at the first character of the input text.
- 2 Look for a match by applying each rule in turn.
- 3 If a match is found, do not process further rules. Go to Step 5.
- 4 If no match is found move to the next character in the input text. Return to Step 2.

- 5 Transform the found text according to the output model for the rule. Move to the character in the input text that is immediately after the found text. Return to Step 2.

A consequence of this is that any given piece of text can be transformed only once, by the first rule that matches it. Where rules search for similar strings, the most specific rule should appear highest in the list on the configuration display, the least specific rule should appear lowest. For example:

- Both **SRC**="(.\*?)\.**gif**" and **SRC**="icon\_(.\*?)\.**gif**" would match the input string **SRC**="icon\_print.gif", but the second rule can only come into play if it precedes the first one in the rule list.
- Similarly, both **<A HREF=""** and **<A HREF="(.\*?)"** will match empty href URLs (the second rule will match full ones as well). The first rule must come higher in the list than the second one if it is to trap empty references.

## Tips

You can use rules to make the parser skip over parts of the text by finding matches and using an output format that re-inserts the original text into the string. For example, if an input regular expression is:

```
src="' \+ buildResourcesUrl
```

and the output model is:

```
@param(0)
```

any occurrences of the text **src="" + buildResourcesUrl** will remain unchanged in the output, provided the rule is higher up the list than any other rule that might lead to a match.

Regular expressions in Domino Application Portlet are not case-sensitive by default, but you can select case-sensitivity for the input expression of any rule. This only affects matching of the input: it does not affect the output. For example, a rule with the following input and output:

Input: **href="(.\*?)"**

Output: **href="@param(1)"**

matches **Href="Index.html"** but produces **href="Index.html"**. It matches any possible capitalization of HREF but always produces a lowercase output. In some instances this may not be desirable and a case-insensitive approach may be more appropriate. For example, XML tags and attribute names are case-sensitive and generally require regular expressions that preserve the case of their input. One way to preserve the case of matched text is to include it in a tagged expression, and refer to it in the output. An expression that preserves the case of HREF is:

Input: **(href)=“(.\*?)“**

Output: **@param(1)="@param(2)"**

Here, in the input, the HREF is matched block 1 and the link location is matched block 2. In the output, the matched block 1 text is output instead of a lowercase HREF.

If the name of your Domino server appears in some displays, for example under Address Book Location in a Teamroom database, you can suppress it by entering a suitable rule. For example, if your server was called **server.mycompany.com** you would use this input expression:

```
<font size="2">server\.mycompany\.com</font>
```

and a blank output model.

The default rules provided with Domino Application Portlet follow the exact HTML tag format produced by the Domino HTTP task. If you write your own HTML passthrough, or use JavaScript to write HTML pages, bear in mind:

- Text must match 100%. Therefore if your code contains extra spaces, matching will fail. The solution is to write your own rule which includes these extra spaces.
- If you have JavaScript that uses a variable name which is the same as an HTML reserved tag name, you must specify a new rule to handle the situation. Otherwise, HTML rules might apply and create an error.
- Be careful when using URLs obtained from JavaScript context (`window.location.pathname`, `window.location.href`, `window.location.host`, `document.location`). The current encoding will get as far as the database file name. Anything before that, however, will be encoded, and therefore you will not be able to parse the string for it.

---

## Output functions

Output functions take the text matched by the input expression, re-arrange it and replace it. The following functions are available in both the regular expression and HTML parsers:

- **@host()** or **@host** (HTML parser).  
This returns the name of the Domino machine, for example `dominoserver.ibm.com`.
- **@port()** or **@port** (HTML parser).  
This returns the port to use when connecting to the Domino machine, for example `80`.

- **@protocol()** or **@protocol** (HTML parser).  
This returns the protocol to use when connecting to the Domino machine, for example http or https.
- **@proxypath()** or **@proxypath** (HTML parser).  
This returns the path on the portlet server that is used to replace the link to the Domino server.
- **@transform\_uri\_abs(s)** (regular expression parser) where s is a string that is the URL to be transformed (s is generally obtained from @param) or **@transform\_uri\_abs** (HTML parser).  
Transforms any URL whose path is absolute (not relative), redirecting it to the Domino Application Portlet servlet on the portal server. It transforms URLs so that they begin with the servlet path and end with an encrypted and encoded string that references the original URL. Links such as **/path/db.nsf** are transformed, whereas references such as **relative/link/db.nsf** are not.
- **@transform\_uri\_all(s)** (regular expression parser) where s is a string that is the URL to be transformed (s is generally obtained from @param) or **@transform\_uri\_all** (HTML parser).  
Transforms any URL, even if its path is relative, redirecting it to the Domino Application Portlet servlet on the portal server. It transforms URLs so that they begin with the servlet path and end with an encrypted and encoded string that references the original URL.

The following functions are available only in the regular expression parser:

- **@param(n)** where n is an integer.  
This returns a string corresponding to the nth parenthesized expression in the input expression. The first parenthesized expression is 1, the second 2 and so on. The whole of the matched text is 0.  
If n is greater than the number of parenthesized expressions an error is logged and the whole of the matched text is returned. In other words the result is as for @param(0).
- **@parencount()**  
This returns the number of parenthesized expressions for this match to the input expression.

The following function is available only in the HTML parser:

- **@script** returns text processed by the JavaScript parser (which uses regular expressions).

---

## HTML rules

As an alternative to using only regular expression rules, you can use a combination of HTML rules (described here) to handle the HTML text and regular expression rules to handle JavaScript. When the HTML parser finds any JavaScript it passes it to the JavaScript parser.

The following sections explain how to use HTML rules in Domino Application Portlet:

- Input expressions
- Output model
- Processing
- Output functions

### Input expression

For HTML, the input expression is in three parts:

- 1 **Tag**, which specifies the HTML tag that the rule is to be applied to, for example **param**, **a** or **\*** (any tag).
- 2 **Input attribute**, which specifies the attribute that the rule is to be applied to, for example **src** or **href**.
- 3 **Input value**, which specifies the what the rule is to look for, for example **\*** specifies any value.

The only supported wildcard is **\***. It can be used on its own in any of the three input expression fields. For Input value only it may also be used at the end of a string.

### Output model

For HTML, the output model is in two parts:

- 1 **Output attribute**, which specifies the attribute name for the output. Often this is the same as the input attribute name, but it can be different.
- 2 **Output value**, which specifies the value for the output attribute. It comprises text optionally combined with a single output function. For example, **background-image:url(@transform\_uri\_all)**.

## Processing

The HTML parser processes rules as follows:

- Only one rule can be applied for a given Tag, Attribute and Input value combination.
- If more than one rule matches a given Tag, Attribute and Input value combination, the most specific rule will be applied. For example, if four rules are identical except for the following Input values:

Rule A Input value: **Text123**

Rule B Input value: **Text123\***

Rule C Input value: **Text\***

Rule D Input value: **\***

then Rule A is the most specific, Rule D the least specific. If the text being matched was **Text123** Rule A would be applied; if the text being matched was **Text123\_teststring** Rule B would be applied; if the text being matched was **Text\_teststring** Rule C would be applied; and if the text being matched was **teststring** Rule D would be applied.

- If rules are identical, except for their Output attribute and/or Output value, the one that appears first on the configuration display (the Rules tab) is used.

**Note** When parsing a URL in order to find database file names, the HTML parser changes the internal order of some of the tags. For example, notice below how **method="post"** changes position.

Before:

```
<form onsubmit="_getEditAppletData(); return true;"
method="post "
action="/discussi.nsf/8fe52a1d5de957318525663900486c63?Open
Form&Seq=1 "
enctype="multipart/form-data"
name="_MainTopic">
```

After:

```
<form onsubmit="_getEditAppletData(); return true;"
name="_MainTopic"
enctype="multipart/form-data"
action="/wps/PA_1_0_12D/rproxy/___PC_7_0_1IJ_PI_842884___/$$Z
GlzY3Vzcw==$$ .nsf/8fe52a1d5de957318525663900486c63?OpenForm
&Seq=1 "
method="post" >
```

---

## Troubleshooting

The following sections provide some guidance on resolving problems.

### Connectivity/setup problems

Here are some tips:

- Check your server's connectivity. Can your WebSphere Portal server see your Domino server?
- Check that the portlet is properly configured. In configuration mode (wrench icon) check that it is pointing to the correct Domino database. In edit mode (pencil icon) check and that the Authentication section contains the right user/password combination. Remember that this user must be defined in the Domino application ACL and in the Domino directory (including its internet password).
- Try restarting the portal server after installing the portlet and then reconfigure the portlet.
- Finally, if you get exception stack traces, review them to see where the problem might come from. You can save them to a text file document in order to study the problem.

### Debugging

To perform debugging tests, you should switch off caching. Click the wrench icon to access the Configuration display and go to the Caching section.

### Parsing

Domino Application Portlet is partly a rules-based application; it parses source HTML and JavaScript code and renders encrypted proxy-referenced code. The default configuration settings have been tested with four major standard Notes/Domino web applications (mail, resource reservations, teamroom and discussion). While testing your own application with Domino Application Portlet, you may experience some problems. Most of them are likely to stem from the way the HTML and JavaScript code is written. The following topics provide information about parsing:

- Transformation rules
- Regular expressions rules
- HTML rules

## Parsing JavaScript

If you are using the regular expression parser (as opposed to the HTML and JavaScript parsers) note that it applies rules to the entire file to be parsed, regardless of whether the content is HTML or JavaScript. So, if your JavaScript uses variable names that coincide with HTML reserved tag names, you must create separate rules to process the JavaScript variable names. Otherwise they may be processed by a rule designed to handle HTML.

If you are using the HTML and JavaScript parsers, the HTML parser first scans the input for HTML tags. If it identifies **<SCRIPT>** tags, or JavaScript within the HTML code, it sends these to be parsed by the JavaScript parser, using regular expression rules.

When a parser processes a URL that is subsequently used in JavaScript, remember that the URL will now contain encoded text as far as the **.nsf** file extension. For example, the following unencoded reference:

```
mail/jdoe.nsf
```

becomes something like this when parsed:

```
/wps/PA_1_0_1C2/rproxy/___PC_7_0_1IA_PI_625641___/$bWFpbC9rc  
2V3ZWxs$$$.nsf
```

If you use server paths stored in hidden fields, these should be processed by a separate rule, for example:

```
<input name="Path_Info" type="hidden" value="(.*?)">
```

With output model:

```
<input name="Path_Info" type="hidden"  
value="@proxysrcurl(@param(1))">
```

## What to do next if none of the above works

First of all, try to access your Domino application with your browser. If it displays properly, view the source code. Then go to the portal version and go to the same screen and view the source code. In general, you should view the source code of the screen whose action (button, link, whatever) is breaking, not of the resulting screen.

You can save both files and use a file compare utility to quickly see where the differences are. Try to compare the offending source code with your regular expressions and identify where the problem is. Write an additional rule following the instructions provided in this help system.

If you need to seek further assistance, please provide both the portal-generated source code and the browser-generated code in text files.



---

## Chapter 5

# Single Sign-on — Scenario for Using Non-Domino LDAP with Domino

This chapter provides configuration guidelines for the situation where an existing Domino Directory must coexist with the corporate (non-Domino) LDAP directory.

---

### Single sign-on — Scenario for using non-Domino LDAP with Domino

#### Description

In this scenario, the customer has an existing Domino environment that will be integrated into a Websphere Portal Server (WPS) environment. There are separate directories for both Domino and Websphere Portal:

- The Domino Directory contains information on all Domino users and groups, e.g. for mail, calendaring, Domino applications
- The corporate (non-Domino) LDAP directory contains information on all corporate users and groups; used for Portal user authentication. This directory exists on a non-Domino LDAP server, such as Active Directory, iPlanet, or IBM Directory Server.

Setting up a single sign-on (SSO) environment that includes this kind of Portal deployment with Lotus Collaborative products, such as Sametime and/or QuickPlace, is complex and difficulties can arise.

**Note** The solutions described here apply to Domino versions 6.0.2 and later, including Domino and Extended Products 6.5.1.

## Issues

The prevalent problem in making this scenario work is the “multiple-identity problem.” Multiple identity issues occur when the same user exists in both directories but has a different distinguished name (DN) in each one. WPS uses the underlying WebSphere Application Server (WAS) for authentication. WAS can only authenticate against a single user repository, so all Portal users must exist in a single master directory, typically LDAP. The Domino Directory, on the other hand, contains entries (Person Records) for every user that needs to take advantage of Domino server functionality, such as mail routing.

In this situation, a user — for example, John Smith — has a Domino distinguished name (DN) of John Smith/Boston/YourCo, but the corresponding entry in the LDAP directory has a distinguished name (DN) of uid=jsmith, ou=boston, dc=yourco, dc=com. When John Smith logs into the Portal server with his LDAP uid value, jsmith, the WAS server retrieves the full distinguished name (LDAP DN) from the LDAP directory and uses it to build the LTPA cookie. When Smith then accesses a WebSphere Portal page as an authenticated user where there are links to make names active for Sametime awareness, the Lotus Collaborative Components (LCC) of the WebSphere Portal collects his user information (LDAP common name, uid, and DN) from WebSphere Portal. LCC then attempts to initiate a Sametime Links connection with the Sametime server. In establishing this link the common name is supplied to Sametime to initialize and provide people awareness for him. When Smith accesses a WebSphere Portal page that contains a Notes portlet, the LTPA token that contains his LDAP DN is passed to the Domino server over HTTP. The Domino server then searches the Domino Directory for the LDAP DN where it will not be found. Although the LTPA token is accepted, the resulting SSO session is limited because of the unrecognized LDAP DN.

A plausible solution might be to enable Directory Assistance (DA) on the Domino server to include the LDAP server in the authentication path. When this is done, and the LTPA token that contains Smith’s LDAP DN is passed to the Domino server over HTTP, the Domino server now searches for the DN in the LDAP directory, where a match will be found and the user authenticated. However, the problem with versions of Domino prior to 6.0 is that Smith is authenticated by his LDAP DN - as cn=John Smith, ou=Boston, ou=users, dc=yourco, dc=com - but the entry for the same user in the Domino Directory is John Smith/Boston/YourCo. Domino does not automatically map the two entries. Consequently, everything that the user does in the Domino environment will be done as the LDAP identity - most likely not the desired outcome, as the following examples illustrate.

For example:

- When Smith sends mail, the From field contains the LDAP DN. He will be able to address and send mail, but if a recipient replies to the mail they will receive a 'name not found in directory' error because there is no Domino person document with the LDAP DN.
- When Smith creates documents in Domino databases the author metadata contains the LDAP DN. If a view is sorted on the Authors field, documents he creates through WebSphere Portal will sort in a different location than documents created through the Notes client, as well as those created when accessing the Domino application directly from a web browser.
- Smith will not have access to databases where his Domino identity is listed in the ACL, either explicitly or through Group membership. The same applies to documents where there are restrictions through either Reader or Author fields.

Consequently, the use of DA is not a solution to this problem for Domino R5.0.x and earlier servers.

However, starting with Domino 6.0, if Domino Directory Assistance is configured to include the LDAP directory that contains the user, then Directory Assistance can be used with some success. A new Directory Assistance option in Domino 6 titled "Attribute to be used as Notes Distinguished Name" maps user LDAP directory distinguished names to corresponding Notes distinguished names, and is used for client authentication or for database authorization. This feature allows organizations that need to migrate users from a Domino Directory to a remote LDAP directory to continue to use the users' original Notes distinguished names. It's also useful as a way to hide complex LDAP distinguished names from users.

This approach may require that the LDAP directory schema be changed in order to create a descriptive field name to be used for this function. (You can use an existing attribute in the LDAP directory provided the syntax type is DN.) Some customers may prohibit making such changes to the LDAP directory. If such changes are allowed, then customers can use the feature to map an LDAP attribute to the Domino DN. For example, the LDAP directory administrator may create an auxiliary object class in the LDAP directory which contains an attribute such as "NotesDN," which contains the name cn=John Smith, ou=Boston, o=YourCo. This is the LDAP format of the Domino user's name that is mapped by Domino back to John Smith/Boston/YourCo. The LDAP administrator would somehow have to populate that NotesDN field with the correct Domino name info for each user. The DA configuration allows this NotesDN field to be declared so that the LDAP name will automatically be mapped to the Domino DN.

For those customers using a Domino version prior to 6.0, or for those 6.0 users who cannot alter the corporate LDAP directory, the solution is to map the LDAP identity to the Domino identity manually. The FullName field (which usually appears in the directory template labeled “User Name”) of the Person document is a multi-value field and can contain as many variations of the user’s name as needed. (Note: the first value in this field is always the Domino distinguished name.) As a best practice, each entry should be unique in the Domino Directory. When a match is found against one of the entries in this field, Domino maps the identity to the first entry in the field for the purposes of authorization. This is normally the hierarchical version of the user’s name (e.g. John Smith/Boston/YourCo). To take advantage of this capability, the users’ LDAP DN is added after the second line of the FullName field in Domino format. If DA is enabled, then the administrator must ensure that any record found for the user can unambiguously be mapped to that user. If multiple records are found, the user’s email information is of great importance as the name mapping will not occur if records found do not all contain the same Internet email address information for the user (more about this below)

Manual user name mapping is typically done either by using a tool, such as IBM Tivoli Directory Integrator (ITDI), or by running agents within Domino to update person records. See step 3 in the section “Configuring the Domino environment,” below.

For more information about IBM Tivoli Directory Integrator, see the IBM Tivoli Directory Integrator Reference Guide.

### **Scenario workarounds**

Add LDAP form of user name to the Domino Directory Person record in one of the following ways:

- put user name in the Domino Directory manually
- use IBM Directory Integrator to synchronize LDAP user name with Domino Person record
- write a LotusScript agent to do the mapping

## **Roadmap — General configuration guidelines for this scenario**

### **A. Configuring the Domino environment**

1. Establish the LTPA relationship between Domino and Portal Server

For this approach to work the single sign-on LTPA relationship must be first established between the WebSphere Portal and Domino environments.

2. Configure Directory Assistance, if required.

Directory Assistance is disabled by default. If you are using DA to access multiple Domino Directories, or are otherwise enabling it, use the following guidelines:

For pre-Domino 6.0.2 servers - exclude the LDAP directory in the DA search path

Directory Assistance (DA) can interfere with effective authentication because, while it may facilitate a user match, the user name that will be used in the Domino environment is the LDAP identity. This causes a number of authentication problems, such as preventing the user from accessing Notes databases and from receiving replies to sent mail.

For Domino 6.0.2 servers and later — include the LDAP directory in the DA search path

If the LDAP name is included as a secondary value in the FullName field, then DA finds both Domino matches and LDAP matches:

- Get the Internet email address (value for Mail attribute) from each LDAP match whose DN matches exactly the name in the SSO token (i.e. the LDAP distinguished name). If there are multiple exact LDAP matches for the SSO token name, then double-check that the Internet email address is the same across these LDAP matches. (If for some reason the matches have different email addresses, then there is no good match. Review log.nsf if logging is turned on: Name ambiguity found during check of Internet email address.)
- For the matches we've already found from Domino, consider only those that have the same Internet email address as the one in the LDAP match. If multiple matches from Domino have the same Internet email address, double-check that these matches share the same Domino DN. (If for some reason the Domino matches have different DNs, then there is no good match. Review log.nsf if logging turned on: Name ambiguity found during check of Internet email address.)

3. Set up name mapping between the Domino and LDAP directories

In the Domino Directory, you will need to add at least one entry to the User Name field in each user's Person document.

- The first line of this **must** always be the full hierarchical Domino user name.
- The second entry should be the common name (cn) of the user in FirstName LastName format. These entries are set up by Domino when a user is registered and should be left as is. Additional entries, such as other forms of the common name, maiden name, and nick names, may exist and are allowed.

- After that, include the DN of the user's LDAP entry in Domino format ( / replacing commas). It should be noted that some LDAP directories use the uid for the RDN naming component, while others use the CN. For example, Active Directory uses a CN by default, while the IBM Directory Server uses the uid by default (a CN attribute exists, but the DN uses uid). Although we have used the naming components UID and CN in the example, below, the DN should work regardless of the RDN naming components used.
- In order for Sametime People Awareness to work, one LDAP value must match a value in the User Name field of the Domino Person document. If the user's LDAP uid value does not match the ShortName value in the Domino Directory, then the DN of the corresponding entry in the LDAP directory must also appear in the User Name field of the Person document. The same applies to other LDAP attributes, such as common name (cn). If you are using the cn as the RDN naming component in your LDAP directory, then the cn of the LDAP entry must be included in the User Name field in order to allow People Awareness to work

**Note** LDAP directory entries must always be secondary values in the User Name field. The first value must remain the hierarchical name of the Domino user.

#### Examples

<i>If the LDAP user entry looks like this:</i>	<i>And the Domino User Name field looks like this:</i>	<i>Add this to the User Name field for ST People Awareness:</i>
uid=jsmith, ou=Sales, o=Acme CN=John Smith	cn=Johnny Smith/ou=Sales/O=Acme Johnny Smith	uid=jsmith/ou=Sales/o=Acme
cn=John Smith, cn=users, dc=Acme, dc=com CN=John Smith	cn=Johnny Smith/ou=Sales/O=Acme Johnny Smith	cn=John Smith/cn=users/dc=Acme/dc=com

4. Synchronize user Internet passwords between Domino and LDAP directories

This is absolutely critical for full Domino integration with the WebSphere Portal. Since WebSphere Portal may pass username and password for some authentication transactions, you also need to synchronize the Internet password (the 'userPassword' attribute in LDAP) between the Domino and LDAP directories. There are still transactions that occur between the Domino server and WebSphere Portal that use the WebSphere Portal login credentials.

**Note** The efforts in steps 3 and 4 require ongoing maintenance. This can either be done manually, or with tools such as IBM Directory Integrator.

For more information about Websphere Portal Server, see the Portal Release Notes and InfoCenter.

For more information about Domino 6.5.1, see Domino Administration Help.

## **B. Configuring Sametime and/or QuickPlace**

Previously, Sametime and QuickPlace could be configured to use either the native Domino Directory (NRPC) or the Domino LDAP directory. However, recent versions of these products mandate the use of LDAP for new installations. In the case of upgrades, they still work with native Domino, but migrating from Domino to LDAP raises some conversion issues - namely, the conversion of existing QuickPlaces and Sametime Buddy lists to use the LDAP form of the user name. Specific information about these issues, and their solutions, are described below.

### **1. Sametime configuration**

- The Sametime server should be configured to authenticate against the native Domino Directory to allow People Awareness.
- For version 3.0, the Sametime documentation recommends that an LDAP directory be used. However, in a multiple directory environment configuring Sametime to use the native Domino directory provides for more flexible People Awareness. The specific example is the use of the NotesView portlet. If People Awareness is enabled for a column that contains the common name of a user, either directory (LDAP or native Domino) can be used. If the column contains the user's Domino DN, Sametime will not be able to determine online status if Sametime is using the LDAP directory.
- For version Domino 6.5.1, administrators have the option to use the Domino DN for instant messaging status lookup. Enabling this setting for users (either through user preferences or the Desktop policy) lets them display online awareness for names when the Sametime (IBM Lotus Instant Messaging) server is configured to look up Domino DNs (for example CN=John Smith/OU=Sales/O=Acme) instead of Note abbreviated hierarchical names (for example John Smith/Sales/Acme).
- Configure Directory Assistance on the Sametime Server. Unlike QuickPlace, which makes LDAP calls to the directory server, Sametime must use Directory Assistance when authenticating against LDAP. The Sametime server is the only server on which it should be configured. Although Sametime awareness will work, you will have the problems discussed earlier when authenticating to Domino applications running on the Sametime server.

- Buddy List conversion for LDAP authentication. If Sametime is configured to authenticate against the LDAP directory, then the ST Buddy Lists must be converted to use the Domino versions of the DN for the corresponding LDAP DNs. A tool for this purpose is being developed by ISSL. See resources for more information. If the tool is not used, this conversion must be done manually. Contact Lotus Support for a conversion tool (STBLConversion.exe) if necessary.

For more information about Sametime configuration, see the Sametime Administration Help.

## 2. QuickPlace configuration

### a. QuickPlace 2.08

- QuickPlace 2.08 should be configured to use the Domino Directory.
- When configuring the underlying Domino server for SSO, you must use a special version of the domcfg.nsf file which is available from [www.lotus.com/support](http://www.lotus.com/support). This file contains an updated default domain login document that performs some additional processing to maintain the LTPA cookie. If you use the default domcfg.nsf that is provided with Domino, the LTPA cookie will be overwritten when you access a QuickPlace, and when you return to WebSphere Portal you will need to log in again.

### b. QuickPlace 3.01

- QuickPlace 3.01 should be configured to access the same LDAP directory as the WebSphere Portal.
- If you are accessing an existing QuickPlace environment that has been migrated from an earlier version, this may be a problem. You may need to use the changemember command to update user names in the QuickPlaces to their LDAP versions. This allows users to maintain their current QuickPlace capabilities in the environment.
- If you have a requirement that you must use either the native Domino directory or Domino Directory through LDAP, then you will need to obtain a patch that supports the appropriate name mapping.

For more information about Quickplace configuration, see the QuickPlace Administration Help.

---

# Index

## A

- Administrators
  - summary of user names for pilot, 19
- Authentication (Domino)
  - in Domino Application Portlet, 96, 99
- Authentication (WebSphere Portal)
  - in Domino Application Portlet, 100
- Awareness
  - in Domino Web Access, 72
  - in Notes View portlet, 74
  - troubleshooting, 80

## B

- Bookmarks portlet
  - configuration, 65

## C

- Caching
  - in Domino Application Portlet, 96, 102
- Chat
  - in Domino Web Access, 72
  - in Notes View portlet, 74
  - in Team Workplace, 65
- Concrete portlets, 94
- Configuration
  - Domino Administrator, 45
  - Domino Document Manager, 38
  - Domino Web Access, 72
  - Domino Web Application Portlet, 94
  - Instant Messaging and Web Conferencing (Sametime), 46, 49
  - LDAP, 23, 26, 27
  - Notes/Domino and Extended Products Portlets, 63
  - single sign-on, 50, 52, 54, 56
  - Team Workplace, 30, 34, 65, 68
  - WebSphere Portal, 58

- Credential vault, 101

## D

- DIIOIP
  - turning on logging, 83
- Documentation
  - locations on Web, 20
- Domain Catalog server
  - described, 34
- Domino
  - installation, 21, 42
  - LDAP configuration, 23, 26, 27
- Domino Administrator software
  - configuration, 45
  - installation, 22
- Domino Application Portlet
  - authentication, 96, 99, 100
  - caching, 96, 102
  - configuration, 64, 94
  - exporting rules, 98
  - HTML rules, 110
  - importing rules, 98
  - installation on WebSphere Portal 5.0.2, 61
  - installation on WebSphere Portal v. 5.0 and earlier, 87, 89, 94
  - introduction, 87
  - output functions, 108
  - prerequisites, 89
  - regular expression rules, 105
  - rules, 97, 104, 105, 110
  - single sign-on (SSO), 100
  - system requirements, 89
  - transformation rules, 97, 104
  - troubleshooting, 112
- Domino authentication
  - in Domino Application Portlet, 99
- Domino Databases portlet
  - configuration, 74
- Domino Document Manager
  - configuration, 38
  - installation, 36
  - planning considerations, 13
- Domino Web Access
  - configuration, 72

- planning considerations, 13
- Domino Web Application Portlet.
  - See Domino Application Portlet
- Domino Workflow. See Lotus Workflow
- Domino.Doc. See Domino Document Manager
- DOMLOG.NSF, 82

## E

- e-meetings
  - in Team Workplace, 68
- Exporting rules
  - in Domino Application Portlet, 98

## F

- Failover, 11

## H

- HTML rules
  - in Domino Application Portlet, 110
- HTTP
  - turning on tracing, 82

## I

- Importing rules
  - in Domino Application Portlet, 98
- iNotes. See Domino Web Access
- Installation
  - Domino, 21, 42
  - Domino Administrator, 22
  - Domino Document Manager, 36
  - Domino Application Portlet on WebSphere Portal 5.0 and earlier, 89
  - Domino Application Portlet on WebSphere Portal 5.0.2, 61
  - Instant Messaging and Web Conferencing (Sametime), 43
  - Notes/Domino and Extended Products Portlets, 61

- overview, 17
- Team Workplace, 29
- WebSphere Portal, 20

Instant Messaging and Web Conferencing

- configuration, 46, 49, 56
- installation, 43
- LDAP and, 5
- planning considerations, 13

## L

LDAP

- configuration, 23, 26, 27
- installation, 21
- turning on tracing, 81

LDAP directory, 4, 7, 10, 115

LDAP searches, 6

Lotus Notes

- configuration, 45
- installation, 22

Lotus Notes Mail portlet

- configuration, 64

Lotus Workflow, described, 41

## M

My Contacts portlet

- configuration, 64

## N

Netegrity SiteMinder, 8

Notes View portlet

- configuration, 32, 74

Notes. See Lotus Notes

NOTES.INI settings

- iNotes\_WA\_SametimeServer, 14

Notes/Domino and Extended Products Portlets

- configuration, 63
- described, 59
- installation, 61
- LDAP and, 5

## O

Output functions

- in Domino Application Portlet, 108

Overview

- Domino and Extended Products and WebSphere Portal, 1
- LDAP configuration, 23

- pilot installation, 17
- planning, 2
- single sign-on configuration, 50

## P

People Finder portlet

- configuration, 64
- planning considerations, 14

Planning

- overview, 2

Portlets

- configuration, 63
- installation, 61

Prerequisites

- Domino Web Application Portlet, 89

## Q

QuickPlace. See Team Workplace

## R

Regular expression rules

- in Domino Application Portlet, 105

Rules

- in Domino Application Portlet, 97, 104, 105, 110

## S

Sametime

- configuration, 46, 49
- installation, 43
- LDAP and, 5
- planning considerations, 13
- single sign-on configuration, 56

Search Places, in

- Team Workplace, 34

Security

- in WebSphere Portal, 27
- planning, 10

Single sign-on, 115

- configuration, 50, 52, 54, 56

Single sign-on (SSO)

- in Domino Application Portlet, 100

SSO. See single sign-on

System requirements

- Domino Web Application Portlet, 89

## T

Team Spaces portlet

- configuration, 63

Team Workplace

- configuration, 30, 34, 52, 54, 65, 68
- installation, 29
- planning considerations, 12

Tivoli Access Manager, 8

Tracing

- HTTP, 82
- LDAP, 81

Transformation rules

- in Domino Application Portlet, 97, 104

Troubleshooting

- in Domino Application Portlet, 112
- known issues, 83
- overview, 75, 76
- strategy for, 78

## U

Upgrading, 14

User names

- in pilot, 19

## V

Vault slot types, 101

## W

Web Conferences portlet

- configuration, 63

Web conferencing

- in Team Workplace, 68

Web SSO configuration

- document, 53, 56

WebSphere Application Server

- single sign-on configuration, 52

WebSphere Portal, 115

- configuration, 27, 58
- installation, 20
- LDAP and, 4

WebSphere Portal authentication

- in Domino Application Portlet, 100