



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 1999, 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

AIX, Domino, Domino Designer, IBM, iSeries, Lotus, Lotus Notes, Notes, OS/400, QuickPlace, Sametime, SecureWay, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. Microsoft and Windows 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

1 Team Workplace Administration Overview	1	Sample user directory settings for Sun ONE Directory Server and IBM Directory Server	29
Administration overview	1	Using nested groups	30
What's new in Team Workplace 6.5.1?	2	Access to the LDAP directory server	30
Tools for administering a Team Workplace server	4	Switching to another user directory	31
Server Settings in the administration place	6	Disconnecting from a user directory	32
NOTES.INI file settings	6	External group membership	32
Starting and stopping Team Workplace	6	Special characters supported for user and group names	40
Signing in as a Team Workplace administrator	7	3 Setting Up the Place Catalog	41
Additional documentation	8	The Place Catalog	41
2 Connecting to a User Directory	9	Setting up the Place Catalog	41
User directories	9	Place Catalog XML	44
Connecting to a user directory	10	How the Place Catalog works	46
Specifying a search base for group searches	13	Enabling DBCS members to use My Places	50
Mapping to the Team Workplace schema	14	Recovering if the Place Catalog server goes down	51
Specifying the format of distinguished names	15	4 Managing PlaceTypes	53
Allowing accented characters in user names (UNIX)	19	PlaceTypes	53
Translating LDAP names for offline installation	19	Creating a PlaceType	53
Example of translating names	23	Editing the server's PlaceType list	55
Customizing search filters	23	Refreshing PlaceTypes and places	55
Customizing the directory lookup user interface	27	Levels of refresh	57
		How basic refresh affects the elements in places	57
		How replace affects the elements in places	58
		Controlling whether the QPTool refresh command refreshes a place	60

Refreshing a PlaceType from the PlaceTypes view in the administration place	61
Signing a newly inherited scheduled PlaceBot in a place	62
Copying a PlaceType	62
Deleting a PlaceType	63
5 Administering Team Workplace Servers in a Cluster	65
Team Workplace servers in a cluster	65
Creating a cluster	67
Adding a Team Workplace server to a cluster	68
Configuring clustered servers for the Place Catalog	70
Removing a Team Workplace server from a cluster	72
6 Setting Up Security	75
Team Workplace authentication	75
Multi-server single sign-on authentication	76
Creating or editing Web SSO Configuration document	76
Completing single sign-on setup	78
Modifying user cache settings	80
Controlling access to the server	81
Specifying administrators of a Team Workplace server	81
Changing a local administrator password	83
Specifying who can create places on a server	84
Specifying super user access to a Team Workplace server	86
Expanded membership	88
Expanded membership groups	88
Setting up expanded membership	91

Changing the directory server or base distinguished name used for the expanded membership groups	94
Using expanded membership logging	96
Blocking specific protocols referenced in link URLs	96
Blocking HTML attachments that contain cross-site scripts	97
7 Customizing the My Places Feature	99
Customizing the My Places feature	99
display_columns setting	100
sort setting	101
results_per_page setting	101
exclude_by_membership setting	102
exclude_by_age setting	103
exclude_by_size setting	104
include_anonymous setting	105
place_links	105
place_ui setting	106
Using My Places URL parameters to configure My Places	107
8 Completing Other Server Configuration Tasks	111
Using the Server Settings room in the administration place	111
ActiveX controls	113
Setting up the Search Places feature	115
Configuring Search Places settings	117
Customizing Web page caching	119
Hiding the Sign In and Sign Out links	121
Configuring browser caching	121
Clearing Team Workplace files from the Internet Explorer cache	121
Preventing caching of Team Workplace pages on browsers	122

Enabling image caching in environments that don't use single sign-on	122	Archiving places	159
Disabling page compression	123	Renaming places	161
Displaying CGI variables in Team Workplace HTML source pages	123	Moving places to another server	161
Customizing user notifications settings	124	Removing places and PlaceTypes from the server	163
Using qpconfig.xml settings to configure notifications	124	Updating statistics in the Place Catalog	166
Configuring where Team Workplace routes replies to e-mail from places	126	Generating reports about places and servers	167
Specifying a footer that appears on all pages	126	Repairing places on the server	170
Enabling and disabling the UTF-8 Domino server setting	127	Cleaning up dead mail	172
Tracking the number of active Team Workplace users	128	Executing an XML API file	172
9 Using QPTool Commands	133	10 Troubleshooting	173
QPTool	133	Troubleshooting user directory problems	173
Adding external members to places	135	Can't add a name from the user directory	173
Changing user and group names in places	137	Names of external users and groups are missing or displayed as distinguished names	173
Changing the name hierarchy of names in places	140	Mapping dn to display_name causes problems	173
Updating external member information in places	141	Using the type-in method to add users from an external directory does not always work	174
Managing expanded membership	143	You cannot add new users with automatic lookup if more than one match is found	174
Resetting local user passwords	145	Cannot add two users with the same distinguished name as members	174
Removing members from places	146	Cannot create a place that has the same name as a user in the user directory	174
Sending newsletters to subscribers	148	Places do not show changes to user information made in user directory	175
Sending mail to managers and members of places	149	"OK with Anonymous access" shows rather than "OK with credentials" when saving user directory settings	175
Registering and unregistering places and servers on the server	151	User directory set to localhost or 127.0.0.1 causes server crash	175
Automating replica stub creation	153		
Refreshing places and PlaceTypes	156		
Locking and unlocking places on the server	158		

What's New notification doesn't work for users who access rooms through group membership	175	Users with flat names can't take places offline	180
Troubleshooting security problems	176	Users who install offline to Windows 2000 client are prompted for Web Application password	180
A second cn component in name is preventing user authentication	176	Offline not working for external users after changemember or changehierarchy commands used	180
A user can't sign into a place after a distinguished name change	176	Offline is not working for a super user	180
User can't sign in after name change in Domino Directory	176	Offline users can't use places and rooms accessed through group membership	181
In a third-party authentication environment, users with non-standard names are unable to authenticate	176	Offline authors or readers see synchronization errors	181
In a third-party authentication environment, users with multi-character delimiters in their names are unable to authenticate	177	Problem installing places offline on Windows	181
Users are rechallenged for credentials when publishing and lose their edits	177	Cannot install places with the same name from two different servers	181
If place member and super user have same name, the super user gets member access	177	Users who do not fill in offline passwords cannot install places offline	181
A user who is a member of a group is not getting the expected access	177	Offline users can't send e-mail from a place	181
Troubleshooting offline problems	178	Database authorization failures occur during Domain Catalog indexing when server is set up for Search Places and offline use	182
New rooms not installing to offline place during synchronization	178	Troubleshooting Sametime problems	182
Users are unable to sign in offline	178	Users can't schedule meetings from a place	182
User installing offline using SunONE Portal Server is prompted to reauthenticate	178	Sametime is not working for local users	182
Users can't install places offline in a Netegrity SiteMinder environment	179	Online awareness not working for users whose names contain accented characters	183
Users see ERROR 500 message when installing offline	179	External users with flat names cannot join online meetings that they publish	183
A PlaceBot does not run offline	180		
Offline users can't edit their member profiles when Sametime is enabled and the place name begins with "QuickPlace"	180	Appendix A Team Workplace notes.ini Settings	185
		Web page cache settings	185

Offline settings	185
Logging settings	186
Other settings	188
Index	191

Chapter 1

Team Workplace Administration Overview

This chapter describes the new administration features in this release of IBM® Lotus® Team Workplace (QuickPlace®), the tools you use to administer a Team Workplace server, how to stop and start a Team Workplace server, and where to find additional Team Workplace documentation.

Administration overview

Team Workplace is a self-service Web tool for team collaboration. Use Team Workplace to publish, share, and track all information relevant to a project. Teams can use Team Workplace to store resources (such as files, discussions, and schedules) related to a project in a common place where everyone can access the latest information.

This document is intended for Team Workplace administrators, and it describes the administration features in Team Workplace 6.5.1.

Administering a Team Workplace server involves the following tasks:

- Connecting to a user directory to simplify the registration and management of members in places
- Setting up a Place Catalog, a central database that collects information about places and Team Workplace servers
- Creating and managing PlaceTypes, places that are used as models for new places
- Setting up client authentication and access to the server
- Customizing the My Places feature that provides links to places of which users are members
- Administering Team Workplace servers in a cluster
- Configuring a variety of server-wide settings using the administration place or settings in a qpconfig.xml file
- Completing a variety of tasks using QPTool commands

Note You configure the underlying Team Workplace mail routing through IBM® Lotus® Domino®. For more information on configuring mail routing with Domino, see Domino Administrator Help.

New method for retrieving system images

Team Workplace 6.5.1 takes advantage of Domino's HTTP-accessible data directories by accessing system images from the file system. In previous releases system images were accessed from the resources.nsf database. As a result of this change, pages that use system images heavily, for example the Edit Page, load much more quickly than in previous releases. For backward compatibility, system images are stored in resources.nsf as well as in the file system.

Page compression

Team Workplace 6.5.1 compresses the HTML and text content in pages it transmits to clients if the browser supports compression. The compression reduces the size of HTML transmissions to 30% or less of the uncompressed size, with the result that users can open large pages more quickly than in previous releases. Only HTML and text content is compressed, not images or attachments.

Because problems can occur with page compression with Internet Explorer 5.5, the Team Workplace server does not use page compression for Internet Explorer 5.5 or lower.

Page compression is enabled by default, but you can disable it using the new qpconfig.xml setting page_compression. For more information, see the chapter "Completing Other Server Configuration Tasks."

New security features

Team Workplace 6.5.1 provides new security features that allow you to block specific protocols referenced in link URLs and to block imports of files that contain cross-site scripts. For more information, see the chapter "Setting Up Security."

New My Places settings

There are two new settings available for configuring My Places in the qpconfig.xml file. Use the new place_links setting to control whether Team Workplace opens a place accessed through My Places in the current browser window or in a new browser window. Use the new show_in_main_place attribute of the place_ui setting to open the My Places list in the page a user is currently signed into rather than in the Quickplace/quickplace main place.

New setting for disabling browser page caching

As a security measure, you can use the new qpconfig.xml setting browser_caches_place_content to prevent Team Workplace from caching on the browser pages that contain data. This setting is effective on all supported browsers. For more information, see the chapter "Completing Other Server Configuration Tasks."

New troubleshooting chapter

This book now contains a chapter called “Troubleshooting ” that describes and suggests solutions to problems you may encounter administering a Team Workplace server.

New notes.ini appendix

This book now contains an appendix called “Team Workplace notes.ini settings ” that summarizes the notes.ini settings used as part of Team Workplace server administration.

Tools for administering a Team Workplace server

You use the following tools to administer a Team Workplace server:

- QPTool commands
- qpconfig.xml file
- Server Settings in the administration place
- notes.ini file settings

In addition to these tools you also use tools available in Domino, for example, to configure mail routing and to set up single-sign on authentication.

QPTool commands

You use QPTool commands to complete many administrative tasks, for example, locking and unlocking places, changing user names, and registering places.

For a description of all the commands available, see the chapter “Using QPTool Commands. ”

qpconfig.xml file

You can specify many Team Workplace server configuration settings by creating a file called qpconfig.xml and using XML to specify the desired settings in the file. A Team Workplace server comes with a sample template file called qpconfig_sample.xml, which is installed in the server data directory. The file includes all of the settings you can specify in the qpconfig.xml file, descriptions of the settings, the default values, and sample values.

To customize a setting described in qpconfig_sample.xml, create a file called qpconfig.xml as described in the following procedure. If you do not create a qpconfig.xml file, the Team Workplace server uses all the default settings.

Additional documentation

In addition to this book, also see the following documentation, available on the Web at <http://www.lotus.com/ldd/doc>.

- The *Team Workplace Installation Guide* describes how to install Team Workplace, how to set up a server so that users can take places offline, how to set up Team Workplace to work with Sametime, and how to upgrade your existing servers.
- The *Team Workplace Developer's Guide* describes how to customize a place, how to use Placebots, and how to use XML to perform actions in Team Workplace.
- The *Team Workplace Release Notes* lists the Team Workplace system requirements and known problems.
- The book *Installing and Managing Team Workplace for iSeries* describes how to install and configure Team Workplace on iSeries servers.
- The Domino Administrator Help describes all the tasks involved with administering a Domino server.
- The *Domino Release Notes* list Domino system requirements and known problems.

In addition to the documentation listed above, the Help that comes with Team Workplace describes end-user features. To access the Help, from any place, click the Help button.

Chapter 2

Connecting to a User Directory

This chapter describes how to connect the Team Workplace server to an external LDAP directory and how to configure the Team Workplace server to work with the directory.

User directories

A place can have local users or external users. Local users have contact and authentication information stored in the membership database (Contacts1.nsf) of the place. Managers of the place can create users, change the users' access levels, and delete users. Local users can access only the place where their membership information is contained.

The contact and authentication information for external users is stored in a user directory on a separate server. When an external user is made a member of a place, a copy of their contact information is stored in the membership database of the place, but their authentication information is stored only in the user directory. These users can be added or removed as members of a place without their information in the user directory being affected.

You can connect the Team Workplace server to a user directory on an LDAP server so that place managers can add users from that directory as members of the place. If a place member's name or other information such as e-mail address changes in the directory, you can use QPTool commands to automatically update places to reflect the change. For example, if John Smith is a user in the directory and is registered as a member of places, if you change John's e-mail address in the user directory, you can use the QPTool `updatemember` command to update his e-mail address in places.

Note Distinguished names of users and groups in the user directory should be unique. If there are two distinguished names in the directory that are the same, only one of the names can be added to a place as a member. If two distinguished names are identical, add a middle initial or other distinguishing character to one of the names to make each name unique.

Connecting to a user directory

User directories store information about users in an enterprise, for example, user names, group names, and e-mail addresses. There are many advantages to connecting to a user directory:

- User information can be managed in one location — the directory — instead of in each place.
- Place managers can select new place members from the directory without entering any information for them. (When new local place members are added, the manager must enter their name, password, and e-mail address.)
- Place managers can select groups listed in the directory as new place members rather than creating each group member as a new place member.
- A user can be a member of many places and access any one of them with the same user name and password. This is possible because the user's user name and password are stored in one place — the directory — and Team Workplace authenticates them against the directory. Users who are local members of many places could have different user names and passwords in each place.
- Users can use single sign-on authentication to sign on to one place, and then access other places they are a member of without re-entering their user name and password.

A Team Workplace server can connect to a user directory on any server configured to use the Lightweight Directory Access Protocol (LDAP) version 3, including a Domino server that runs the LDAP service or any other LDAP directory server. LDAP is a standard way for Internet servers to present directory information. A Team Workplace server can connect to only one user directory at a time.

Upgrading from a Domino Directory configuration

If you are upgrading from QuickPlace 2.0.8 or 2.0.9, connecting to a Domino Directory through NRPC rather than LDAP is supported only during the upgrade to QuickPlace 6.5.1. See the following steps for information on switching directories.

For more information on upgrading, see the *Team Workplace Installation and Upgrade Guide*.

You can configure a Domino Directory server to use LDAP. For information on configuring LDAP on a Domino server, see Domino 6 Administrator Help.

5. Click User Directory.
6. Click Change Directory.
7. In the Type field, select “LDAP Server.”
8. In the Name field, enter the name of the server on which the user directory resides. For example, elvis.acme.com.
9. In the Port number field, enter the port number that the LDAP server uses to communicate with other servers, if necessary. The default is 389.
10. (Optional) Check “Check for SSL connection with LDAP user directory.” If you select this option and SSL is configured correctly on the Team Workplace server and the LDAP server, the Team Workplace server will initiate all requests to the LDAP user directory as SSL encrypted requests.
11. (Optional) In the Search base field specify a search base using the following Distinguished Name format: *ou=organizational_unit_name, o=organization_name*.

For example, if the organization is called Acme and you want LDAP searches to start at the highest level, you would enter *o=Acme*. If you want LDAP searches to start at a lower level in the organization hierarchy, also specify an organizational unit name. For example, to make sure that LDAP searches are confined to the organizational unit East in organization Acme, you would enter *ou=East, o=Acme*.

By default the Search base you specify applies to both user and group searches. However, you can use the *qpconfig.xml* file to specify a different search base for group searches.

For more information, see the topic “Specifying a search base for group searches.”
12. (Optional) Check “Narrow searches to the place name” to confine searches launched from a place to user directory names that include the name of that place.

For example, with this option checked, if a user does a directory search from a place called “Sales Support,” the search looks only for users who have “Sales Support” in their user names.
13. (Optional) If a user name and password are required to access directory information on the LDAP server, do the following:
 - a. Put a check mark next to “Check to use credentials specified below when searching the directory.”
 - b. Enter the user name, an LDAP distinguished name, for example *cn=admin,o=acme*.
 - c. Enter the password.


```
<server_settings>
  <user_directory>
    <ldap>
      <base_dn>
        <group>ou=groups,o=ibm</group>
      </base_dn>
    </ldap>
  </user_directory>
</server_settings>
```

For more information on creating and using the `qpconfig.xml` file, see the chapter “Team Workplace Administration Overview.”

Mapping to the Team Workplace schema

Users, groups, and all other objects in an LDAP directory are described by a variety of attributes. For example, the value for a user's first name is often stored as the *givenname* attribute and the last name as the *sn* (surname) attribute. Not all LDAP directories define attributes for users and groups in the same way. To display accurate information in the Team Workplace user interface about users and groups, such as names, phone numbers, and e-mail addresses, you might have to change some of the default attributes that Team Workplace assumes. For example, by default the Team Workplace server assumes an LDAP server uses the *sn* attribute to define a user's last name. However, if the LDAP server uses the *lastname* attribute instead, you must change the `qpconfig.xml` file so Team Workplace knows the correct attribute to display for the last name.

To configure which attributes the Team Workplace server retrieves from the LDAP directory to display information about users and groups, use the following `qpconfig.xml` settings. The values in bold are ones that you customize. The LDAP directory server must give the Team Workplace server access to the attributes you specify.

```

<server_settings>
  <user_directory>
    <ldap>
      <schema>
        <user>
          <object_class>objectClass</object_class>
          <object_class_value>person</object_class_value>
          <common_name>cn</common_name>
          <display_name>cn</display_name>
          <first_name>givenname</first_name>
          <last_name>sn</last_name>
          <email>mail</email>
          <phone>telephone</phone>
        </user>
        <group>
          <object_class_value>groupOfNames</object_class_value>
          <common_name>cn</common_name>
          <display_name>cn</display_name>
          <member>member</member>
        </group>
      </schema>
    </ldap>
  </user_directory>
</server_settings>

```

For more information, see the topic “Access to the LDAP directory server ” later in this chapter. For information on creating and specifying settings in the qpconfig.xml file, see the chapter “Team Workplace Administration Overview.”

Note Information about a member of a place added before a change in the schema mapping reflects the old mapping. To update the member information to reflect the new mapping, use the QPTool `updatemember` command, or edit the member's Member Profile in the place.

Note Mapping dn to the display name is not supported.

Specifying the format of distinguished names

The `dn_delimiter`, `dn_incoming_is_native`, and `secondary_cn_component` settings, which you specify in the `user_directory - ldap - schema` section of `qpconfig.xml`, are useful for resolving user authentication problems that specific distinguished name formats can cause.

For information on creating and specifying settings in the `qpconfig.xml` file, see the chapter “Team Workplace Administration Overview.”

dn_delimiter setting

By default, when Team Workplace adds an external user name as a member of a place, if the name contains a multi-character delimiter that includes a comma or semicolon, it replaces the comma or semicolon with a forward slash (/) and retains the additional delimiter character(s) in the name. The forward slash is used for compatibility with Domino name syntax. When some third-party authentication applications, such as Netegrity SiteMinder, pass these names to Team Workplace, they replace the entire multi-character delimiter with a forward slash (/). This naming inconsistency between the two applications causes authentication failures.

For example, if the name in a user directory is cn=john doe, ou=sales, o=acme (comma space delimiter), the name becomes cn=john doe/ou=sales/ o=acme in a place (slash space delimiter), but Netegrity SiteMinder passes the name cn=john doe/ou=sales/o=acme to Team Workplace (slash delimiter).

If you use a third-party authentication application and experience authentication failures due to this inconsistency in the handling of multi-character delimiters containing commas or semicolons, use the dn_delimiter setting in qpconfig.xml to specify that Team Workplace replace the entire multi-character delimiter with a forward slash, to be consistent with the authentication application. If the names of all the users in the directory use the same multi-character delimiter, specify that delimiter, terminated by the @ symbol. For example, if all names in the user directory contain the delimiter , (comma space) specify the following:

```
<server_settings>
  <user_directory>
    <ldap>
      <schema>
        <dn_delimiter>, @</dn_delimiter>
      </schema>
    </ldap>
  </user_directory>
</server_settings>
```

If names in the directory do not use the same delimiter, use the following `dn_delimiter` setting instead to enable Team Workplace to replace any single- or multi-delimiter character with a forward slash, if the delimiter conforms to LDAP RFC 3377.

```
<server_settings>
  <user_directory>
    <ldap>
      <schema>
        <dn_delimiter robust_compare="true"/>
      </schema>
    </ldap>
  </user_directory>
</server_settings>
```

Although you can use the `<dn_delimiter robust_compare="true"/>` setting if all names use the same delimiter, configuring the specific delimiter saves Team Workplace processing time.

robust_compare and the My Places feature

When a user accesses My Places from a server's main place (<http://servername/QuickPlace/quickplace>), Team Workplace has access to only the user's Domino-formatted name that the authentication application passes to it. However My Places requires the LDAP version of a user's name to use the Place Catalog to build a list of the user's places.

In an environment with multi-character delimiters, Team Workplace uses the `dn_delimiter` setting to convert the Domino formatted name it receives from the authentication application to the LDAP formatted name used in the Place Catalog. If `robust_compare` is used with the `dn_delimiter` setting, Team Workplace generates LDAP-formatted names that use single-comma (,) delimiters, regardless of the actual delimiter used in the names in the directory. Adding a new user as member of a place after you enable the `robust_compare` setting automatically creates the user's LDAP name in the Place Catalog with the single-comma delimiter. However, if the Place Catalog contains names of members created prior to use of `robust_compare` that do not use single-comma delimiters, you must change these delimiters to the single-comma delimiter. This is a one-time only change, which you can do using a Notes® agent.

dn_incoming_is_native setting

When a third-party authentication application such as Netegrity SiteMinder finds a distinguished name that contains components other than the `cn`, `ou`, and `o` components familiar to Domino, it sends the name to Team Workplace without adding the Domino-style forward slash delimiters. For example, if Netegrity SiteMinder finds the name `uid=sblake,o=acme` in the directory, it

passes that name to Team Workplace rather than uid=sblake/o=acme. Because Team Workplace uses the forward slash delimiters in the names in places, the naming inconsistency causes authentication failures. This problem is indicated if there are authentication failures and the Netegrity (or other application) log shows that the names pulled from the directory are in the same format as the ones sent to Team Workplace.

To correct the problem, use the following setting to indicate that Team Workplace should convert “ native” names to the Domino format:

```
<server_settings>
  <user_directory>
    <ldap>
      <schema>
        <dn_incoming_is_native enabled="true"/>
      </schema>
    </ldap>
  </user_directory>
</server_settings>
```

secondary_cn_component setting

When the second component of a distinguished user name in a user directory is cn, Team Workplace converts the component to ou by default. For example, if the distinguished name of a user in an external directory is uid=abrown,cn=users,dc=acme,dc=com, Team Workplace uses this name instead: uid=abrown,ou=users,dc=acme,dc=com (and the Domino-formatted version, uid=abrown/ou=users/dc=acme/dc=com). If you experience authentication failures because of this behavior, correct the problem by specifying the following setting to retain second cn components found in names:

```
<server_settings>
  <user_directory>
    <ldap>
      <schema>
        <secondary_cn_component enabled="true"/>
      </schema>
    </ldap>
  </user_directory>
</server_settings>
```

Note The secondary_cn_component setting is useful whether or not you use a third-party authentication application.

(.+) symbol means “one or more occurrences of any character.” In the preceding sample, this accounts for any value the “uid” and “c” components might have. You also use symbols to translate syntax that otherwise might be interpreted as a special character. For example, the \ symbol turns off the special meaning of the character which follows. Without this symbol in “o=ibm\com,” the dot (“.”) would be interpreted by its special character meaning, which is “match any single character.”

The “to” attribute specifies Domino components, using symbols to match values from the LDAP components and arrange them in a way Domino recognizes. For example, the symbol \1 means “whatever matched the first regular expression.” So, the CN component’s value will match the first regular expression (.+) found in the “from” attribute. In the same way, the symbol \2 means “whatever matched the second regular expression.” So, the OU value will be the explicitly stated “bluepages_” plus the second regular expression (.+), which in this case is the value of the country, or “c”, component. The O component is explicitly stated. You can have up to nine regular expressions in one rule.

You create rules for translating Domino names back to LDAP names within the <to_directory_name> element. Use the same symbols used in the <from_directory_name> element.

The preceding translation rules would result in the following example translations:

<i>LDAP directory name</i>	<i>Domino name</i>
uid=Joe User/c=us/ou=bluepages/o=ibm.com	CN=Joe User/OU=bluepages_us/O=ibm_com
uid=Nils Nilsen/c=dk/ou=bluepages/o=ibm.com	CN= Nils Nilsen/OU=bluepages_dk/O=ibm_com

Notice that the regular expressions accommodate the country, or “c,” code. There is no need to have a separate translation rule for each country code because they can be captured by a (.+) expression, and then inserted anywhere in the translated name with a \[number] expression.

Table of expressions

There are many symbols that can be used in regular expressions, but only a few are useful for the purpose of translating a non-conforming LDAP name to a Domino name. The following is a list of these symbols, with examples of their use as applied to matching a particular LDAP name. All of the examples shown here will match the LDAP user name “uid=Joe User/c=us/ou=People1/o=org.com.” The symbols described appear in bold in the examples:

<i>Symbol</i>	<i>Description</i>	<i>Example</i>
(.+)	One or more	uid=(+)/c=(+)/ou=bluepages/o=ibm\com

<i>Symbol</i>	<i>Description</i>	<i>Example</i>
	occurrences of any character.	
\1, \2, \3, etc.	Whatever matched the first regular expression, whatever matched the second, and so on. Up to 9 regular expressions may be used in one rule.	CN=\1/OU=bluepages_\2/O=ibm_com
\c	Turns off the meaning of any special character 'c'.	uid=Joe User/c=us/ou=People1/o=org\.com
.	Matches any single character.	uid=Joe User/c=us/ou=People./o=org
[...]	Matches any of the enclosed characters.	uid=Joe User/c=us/ou=People[123456789]/o=org
[^...]	Matches any character that is not enclosed.	uid=Joe User/c=us/ou=People[^2-9]/o=org
n-n	Matches any character in this range.	uid=Joe User/c=us/ou=People[0-9]/o=org[.]com
*	Matches any number (zero or more) of the preceding character or bracketed expression.	uid=Joe U.* /c=us/ou=People1/o=org\.com
+	Matches one or more of the preceding character or bracketed expression.	uid=Joe [A-Za-z]+ /c=us/ou=People1/o=org\.com
(regexp)	Delineates a regular expression so that it can be used in the replacement string (the "to" string in <translate>).	uid=Joe User/c=(.+)/ou=People1/o=org\.com

Example of translating names

The following settings provide an example of translating names that appear in the user directory as `cn=name,ou=People1,dc=acme,dc=com`.

```
<server_settings>
  <offline enabled="true">
    <name_translation enabled="true">
      <from_directory_name>
        <translate from="cn=(.+)/ou=People1/dc=acme/dc=com"
          to="CN=\1/OU=People1/O=acme_com" />
      </from_directory_name>
      <to_directory_name>
        <translate from="CN=(.+)/OU=People1/O=acme_com"
          to="cn=\1/ou=People1/dc=acme/dc=com" />
      </to_directory_name>
    </name_translation>
  </offline>
</server_settings>
```

Customizing search filters

You can use the `qpconfig.xml` file to customize the LDAP search filters that Team Workplace uses to:

- Search for external user names when authenticating users
- Search for external user names to include in places
- Search for external groups to include in places
- Search for the external groups of which an authenticated external user is a member

To configure search filters, add the following section from the `qpconfig_sample.xml` file to the `qpconfig.xml` file and then customize the settings. You must create `qpconfig.xml`, if you haven't already done so.

For more information on creating and using the `qpconfig.xml` file, see the chapter “Team Workplace Administration Overview.”

```

<server_settings>
  <user_directory>
    <ldap>
      <search_filters>
        <authentication><![CDATA[(I(cn={0})(uid={0})(shortname={0}))]]></authentication>
        <user_lookup><![CDATA[(&(objectclass=person)(sn={0})(givenname={1}))]]></user_lookup>
        <group_lookup><![CDATA[(&(objectclass=groupOfNames)(cn={0}))]]></group_lookup>
        <group_membership><![CDATA[(&(objectclass=groupOfNames)(member={0}))]]></group_membership>
      </search_filters>
    </ldap>
  </user_directory>
</server_settings>

```

For more information about LDAP search filters, see Domino Administrator Help.

Customizing the search filter to use for authentication

When Team Workplace cannot find the user name entered at login in the Contacts1.nsf database, it searches the LDAP user directory to get a distinguished name for login. Team Workplace issues the authentication filter shown in bold, which returns all matches for *cn=*username, *uid=*username and *shortname=*username.

```

<authentication>
<![CDATA[(I(cn={0})(uid={0})(shortname={0}))]]></authentication>

```

For the matches that result from the search, each distinguished name and password is passed to the user directory for verification. The first successful verification sets the current user to that distinguished name.

Edit this line to customize the search filter used for authentication. For example, to look for the name specified by the user first as a *cn* attribute value or a *mail* attribute value, change the line as follows:

```

<authentication><![CDATA[(| (cn={0})(mail={0})) ]></authentication>

```

Note that the zero (0) indicates that Team Workplace accepts only one name as input for authentication. You cannot specify another value and accept more than one name for input.

Customizing the search filter used to find users to add to places

The following information in bold shows the default search filter Team Workplace uses when place managers search for external user names to add to places:

```
<user_lookup><![CDATA  
[(&(objectclass=person)(sn={0})(givenname={1}))]]></user_lookup>
```

This filter indicates that when a user searches for the name of an external user, Team Workplace searches for the *objectclass* attribute value, person. It also indicates that it accepts two, comma-separated values from a user who is searching the directory for an external user. It searches for the first value specified as the value for the *sn* attribute, and the second value specified as the value for the *givenname* attribute. Edit this line to customize this search filter. For example, to search for the second specified name as a value for the *mail* attribute rather than the *givenname* attribute, change the line as follows:

```
<![CDATA[(&(objectclass=person)(sn={0})(mail={1}))]]>
```

If you customize the user search filter, you should also customize the hint the interface provides for searching and possibly other directory lookup user interface settings.

For more information, see the topic “Customizing the directory lookup user interface” later in this chapter.

Note that zero (0) and one (1) indicate the first and second, comma-separated input values, respectively. Team Workplace does not accept more than two input values from a user when searching for names to add to places.

Note When a user adds an external user name to a place, the user can type the name in the text area directly without clicking the Directory button and searching for the name. To find the specified name in this case, the user must specify a unique name in the directory. This unique name can be the distinguished name or another form of the name, for example, Smith or Smith, J. If the distinguished name is not specified, then the user lookup search filter described above is used to search for the name.

Customizing the search filter used to find group names to add to places

The following information in bold shows the default search filter a Team Workplace server uses when users search for external group names to add to places:

```
<group_lookup><![CDATA  
[(&(objectclass=groupOfNames)(cn={0}))]]></group_lookup>
```

This filter indicates that when a user searches for an external group, the Team Workplace server searches for the *objectclass* attribute value *groupOfNames*. It also indicates that the Team Workplace server accepts one name as input from a user and that it searches for the group name as the *cn* attribute value. Edit this line to customize the search filter. For example, to search for the *objectclass* value *groupOfUniqueNames* and search for the *grouptitle* attribute, change the line as follows:

```
<group_lookup><![CDATA  
[(&(objectclass=groupOfUniqueNames)(grouptitle={0}))]]></group_lookup  
>
```

The zero (0) indicates that Team Workplace accepts only one name as input for a group name. You cannot specify another value and accept more than one group name for input.

Customizing the search filter used to search for members of groups

After a Team Workplace server authenticates an external user, the Team Workplace server searches for all the external groups of which the user is a member. Then the Team Workplace server can determine the access the user has to places through group membership. The following information in bold shows the default search filter a Team Workplace server uses to search for the external groups of which an authenticated user is a member:

```
<group_membership>  
<![CDATA[(&(objectclass=groupOfNames)(member={0}))]]>  
</group_membership>
```

This filter indicates that the Team Workplace server searches the user directory for the *objectclass* attribute value *groupOfNames* and the *member* attribute value. Edit this line to customize the search filter. For example, to search for the *objectclass* attribute value *groupOfUniqueNames* and the *uniquemember* attribute value, change the line as follows:

```
<group_membership><![CDATA[(&(objectclass=groupOfUniqueNames)(un  
iquemember={0}))]]></group_membership>
```

The zero (0) indicates that Team Workplace accepts only one name as input for the group members. You cannot configure Team Workplace to accept more than one.

How the Exact Match search option affects search filters

When a user searches for an external user or group to add to a place, whether or not the user selects the Exact Match search option has an effect on the search filters that the Team Workplace server uses. For example, assume the Team Workplace server is configured to use the following search filter when users search for external users:

```
<user_lookup><![CDATA[(&(objectclass=person)(sn={0})(mail={1})] ]></user_lookup>
```

The following table describes the search filter that Team Workplace uses when a user searches for one value and for two comma-separated values, depending on the Exact Match setting.

<i>Exact Match setting</i>	<i>Search filter used when users searches for: smi</i>	<i>Search filter used when user searches for: smi, @acme</i>
Selected	sn=smi mail=*	sn=smi mail=@acme
Not selected	sn=smi* mail=*	sn=smi* mail=@acme*

Customizing the directory lookup user interface

Use the qpconfig.xml file to customize the user interface that users see when looking up users in the directory to add as place members. You can customize the search hint and also customize how the user interface displays the results of user searches. Add the following section from the qpconfig_sample.xml file to the qpconfig.xml file and then customize the values in bold.

```

<server_settings>
  <user_directory>
    <ldap>
      <member_lookup_ui>
        <column_name>
          <person>sn, givenname</person>
        </column_name>
        <column_disambiguate>
          <person>dn</person>
        </column_disambiguate>
      </member_lookup_ui>
      <search_ui_hint>
        <![CDATA[( enter <B>last name, first
          name</B>)]]>
      </search_ui_hint>
      <search_ui_index>sn</search_ui_index>
    </ldap>
  </user_directory>
</server_settings>

```

Note These customizations apply only to user lookups and not to group lookups.

Customizing the hint provided for user searches

To help users search for users in the directory, the search interface provides a hint indicating how to do the search. By default the hint is “enter last name, first name.” If you have customized the search filter Team Workplace uses when users search for external user names to add to a place, customize the search hint too, so users can search successfully.

For example, if you specify the following in the <search filters> section of qpconfig.xml:

```

<user_lookup><![CDATA[(&(objectclass=person)(sn={0})(mail={1}))]]></user_lookup>

```

you might then specify the following for in the <search_ui_hint> section:

```

<![CDATA[( enter <B>last name, email</B>)]]>

```

Note You can specify a maximum of 250 characters.

Customizing what the user interface shows as the result of user searches

By default, when a user searches a directory for external users, for the results Team Workplace displays values for the *sn* and *givenname* attributes in the first column, and the distinguished names in the second column. To display different attribute values, change the `member_lookup_ui` section in `qpconfig.xml`. To change the attributes in the first column, modify the `column_name` section. To change the attributes in the second column, modify the `column_disambiguate` section.

For example, to display the *sn* and *mail* attribute values in the first column, specify:

```
<person>sn, mail</person>
```

Any attributes you specify should be valid ones defined in the schema map.

For more information, see the topic “Mapping to the Team Workplace schema” earlier in this chapter.

You can also use the `<search_ui_index>` section to customize the attribute value that shows in the range field in the results box. By default the value for the *sn* attribute shows in the range.

Sample user directory settings for Sun ONE Directory Server and IBM Directory Server

The following `qpconfig.xml` customizations are recommended if your user directory is on a Sun ONE Directory Server (formerly iPlanet Directory Server) or IBM Directory Server (formerly SecureWay®). Changing LDAP settings not mentioned is optional.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<server_settings>
  <user_directory>
    <ldap>
      <schema>
        <group>
          <object_class_value>groupOfUniqueNames</object_class_value>
          <member>uniquemember</member>
        </group>
      </schema>
      <search_filters>
        <group_lookup><![CDATA[(&(objectclass=groupOfUniqueNames)(cn={0})
)]]></group_lookup>
        <group_membership><![CDATA[(&(objectclass=groupOfUniqueNames)(
uniquemember={0}))]]></group_membership>
      </search_filters>
    </ldap>
  </user_directory>
</server_settings>

```

Using nested groups

If a user directory has nested groups — groups within groups — that contain Team Workplace users, use the following notes.ini setting on the Team Workplace server to allow searches of the nested groups:

1. QuickPlaceNestedGroupLimit=*value*

where *value* represents the number of levels of groups the server can search. By default the level is 1, meaning that the server doesn't search nested groups. Note that in Release 2.0.x the default was 8 levels. Note that searching nested groups can have a negative effect on performance.

2. Enter the following command at the server console to restart the server so the change takes effect:

```
restart server
```

Access to the LDAP directory server

To use a particular LDAP attribute in the schema map, the Team Workplace server must have access to it. If Team Workplace connects to the directory anonymously (that is, without supplying credentials in the User Directory section of the Team Workplace server), the LDAP directory server must permit anonymous reading of the attributes to all users. If Domino is your

Group membership: security features

The following table describes the extent to which security features support external group membership.

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Who can create places on the server	Specify which users or groups can create places on the server. Only explicit members or members of group listed see the "Create a Place" link.	Yes
Who can administer the server	Specify which users or groups can administer the server. Only explicit members or members of group listed see "Server Settings" and "PlaceTypes" links when accessing the server.	Yes
Super User	Can designate a user or group from the directory as super user of all places on the server. This user is a manager of all places and can see all restricted pages.	Yes
Sign Out and Sign In	Sign out of a place or sign into a place as the same or another user. Sign Out also deletes all temporary files on the hard drive from the upload control.	Yes
Basic authentication	For places without Anonymous access for readers or authors, all users must sign in with name and password.	Yes

continued

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Multi-server session authentication	For places without Anonymous access for readers or authors, all users must sign in with name and password on custom login form found in domcfg.nsf. After they sign in, members can access other places and Domino servers for which they have access without re-entering their credentials.	Yes
Netegrity SiteMinder	Team Workplace can be configured to use Netegrity SiteMinder as the authentication scheme.	Yes
Current user link	Link to currently authenticated user in upper left.	Yes. See actual member, not group name. Link takes you to message saying no profile available.

Group membership: place membership

The following table describes the extent to which place membership features support external group membership.

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Page: restrict readers	Restrict readers of a published page.	Yes, group is available as reader, member of group can then read.
Page: add editors	Add editors to a published page.	Yes, group is available as editor, member of group can then edit, but other group members won't see checked out status.
Members view	List of all members of a place.	Yes. Members folder shows group name.
Member profile	Page showing member information and preferences for members and groups.	Yes. Contains common name for the group. There are no member profiles for members of the group unless they are also added explicitly to the place.

continued

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Local place groups	Aggregate existing members and groups in the place for use in room security.	Yes. Can add external groups to local place group. Individual members of the group are not available unless they have also been added explicitly to the place.
Calendar page authors	Calendar page authors show on page and in Calendar view.	Yes. Display_name as set in qpconfig.xml or common name as default.
Author column in folder	Folder displays author names for all pages.	Shows individual member's names, not group name. Display_name as set in qpconfig.xml or common name as default.
Username in page banner	Page displays author name.	Shows individual member's names, not group name. Display_name as set in qpconfig.xml or common name as default.
Forms: name pop-up	Field on a form to show members in place.	Yes. Display_name as set in qpconfig.xml or common name as default.
Form: page author	Page authors show on page and in folder views.	Shows individual member's names, not group name.
QPTool changemember	Can change a member in a place 1) from a local user to a user from the directory, 2) from one external directory user to another (name change), 3) from one external directory group to another.	Yes
QPTool changehierarchy	Can change external users and groups to a different hierarchy. For example, if your organization changes from ou=sales,o=org to ou=salesandmarketing,o=org, you can change the distinguished names for all members in a place.	Yes
QPTool removemember	Remove a member or a group from a place.	Yes

continued

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
PlaceType membership	When a place is created from a PlaceType, you can populate the new place with the membership from the PlaceType. Membership is never refreshed after the place is created.	Yes
Search by author	Search for all pages authored by a member.	No. Can search by individual author name, not by group name because the individual author name and not the group name is saved with the pages.
My Places	A list of all places on the server for which you are a member. Clicking the place name takes you to the place.	Yes

Group membership: notifications

The following table describes the extent to which notification features support external group membership.

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Place invitations	Send e-mail as new members with e-mail are added to the place.	Yes. Explodes the group and sends invitations to the members of the group telling them group has been added, sign in with username.
Notify: From field	The "From" field when notifying members of a page or view in a place.	Shows individual member's email address, not email address of group.
Notify: To, CC, BCC lists	When addressing a notification, you can use lists of all members in place to fill in To, CC and BCC fields.	Yes. Can choose group if has a valid email address or group can be exploded to choose individual members.
QPTool sendmail	Administrator of server can send mail to members of place(s)	Yes. Groups are exploded into mail for individual members of the group.

continued

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
What's new email	Summary e-mail about what has changed in the place. Individual preference for receiving what's new e-mail set on member profile. Default is to receive. Manager of place sets daily or weekly. QPtool newsletter command by administrator of server or server program document triggers the newsletter.	No. Members of a group do not have a member profile to set the preference.
Calendar subscriptions	Receive notification of new calendar events. Individual preference for receiving notification of calendar events set on member profile. Default is not to receive.	No. Members of a group do not have a member profile to set the preference.
Form: notification indicator	Notify members when a page is published with the form.	Yes. Groups are exploded into mail for individual members of the group.
Form workflow: editor-in-chief, approval cycle	Can send published page to an approver before making available to all members.	No. Groups not available as approver for workflow. Also not possible if member of a group is the originator of the workflow since there is no member profile and associated information (email).

Group membership: LDAP directory

The following table describes the extent to which LDAP directory features support external group membership.

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Schema mapping: display_name	By default, the display name used is cn. You can map this to another LDAP attribute in qpconfig.xml.	Yes
Schema mapping: common_name	By default, the common name used is cn. You can map this to another LDAP attribute (such as UID, for example) in qpconfig.xml.	Yes
DBCS usernames	Users and groups in an external directory can have names that use a double byte character set.	Yes
Customizing member lookup user interface	When searching for members from a directory to add to a place, you can customize the attributes shown in the results pages, the search index, and the search hint.	No. Once you select the Group radio button in the member lookup dialog, the customizations do not apply.
Search base for directory members and groups	Designate a point in the LDAP directory structure under which all users and groups are found.	Yes. Can use search base field on Server Settings, User Directory page or base_dn tag in qpconfig.xml if the search base for groups is different than search base for users.

Group membership: Sametime and offline use

The following table describes the extent to which Sametime and offline use features support external group membership.

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Sametime awareness	Online awareness state icon and associated menu for the current user, author online awareness state.	Yes, for members of the group.
Sametime chat (members online)	People Online window and chat functionality.	Yes, for chat. Groups or members of groups do not show up in the People Online window.
Sametime meetings	Ability to create and attend online meetings.	Yes
Work offline	Install and use place(s) offline. Take room(s) offline.	No. Members of a group cannot install places offline or take rooms offline.

Group membership: miscellaneous features

The following table describes the extent to which various miscellaneous features support external group membership.

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Place creation	Create a place with specified creator (initial manager)	No. Must use explicit member as creator.
Accessibility mode	Displays high-contrast theme and enhances keyboard and screen reader accessibility. Individual preference for accessibility mode set in member profile. Default is standard experience (no accessibility features).	No. Members of a group do not have a member profile to set the preference.
Tasks: Assignments	Assign tasks to members of the place.	Yes.

continued

<i>Feature</i>	<i>Description of feature</i>	<i>Membership through external group</i>
Place catalog	Collects information about all places in the service. A document is created in the place catalog when a place is created. Members are added to readers, authors, and managers fields. Membership operations (promote, demote, add, delete, name change) in the place are reflected in the place catalog document.	Yes

Special characters supported for user and group names

The following table summarizes the support for special characters in user and group names.

<i>Special character</i>	<i>Allowed for local users?</i>	<i>Allowed for local groups?</i>	<i>Allowed for external users and groups?</i>
@	Yes	No	No
<	No	No	No
>	No	No	No
&	No	No	No
:	No	No	No
;	No	No	No
^	No	No	Yes
, (comma)	No	No	No
=	No	No	Yes
(No	No	Yes
)	No	No	Yes
#	No	No	Yes
\	No	No	No
/	No	No	Yes
	No	No	No
*	No	No	No
+	No	No	Yes
“	No	No	No
' (apostrophe)	Yes	Yes	Yes

Chapter 3

Setting Up the Place Catalog

This chapter describes the Place Catalog and how to set it up.

The Place Catalog

The Place Catalog is a centralized database in which you collect information about all your places and Team Workplace servers.

The Place Catalog has two audiences: administrators and users. Administrators can use the QPTool report command or an XML interface to the Team Workplace Java™ XML API to access the Place Catalog to query information. Users access the Place Catalog indirectly, through features such as My Places, which allows them to see the places they belong to, and Search Places, which allows them to search in places across the enterprise.

For information on how to access the Place Catalog with the Team Workplace Java XML API, see the *Team Workplace Developer's Guide*. For more information on the QPTool report command, see the chapter “Using QPTool Commands.”

Setting up the Place Catalog

The Place Catalog feature is automatically enabled on all Team Workplace server installations. When you install a Team Workplace server, a local Place Catalog database (PlaceCatalog.nsf) is created. If you want to change Place Catalog settings or disable the Place Catalog, create a file called qpconfig.xml and copy into it the Place Catalog section from the file qpconfig_sample.xml. Then change settings.

For more information on creating a qpconfig.xml file, see the chapter “Team Workplace Administration Overview.”

For example, if your enterprise has several Team Workplace servers and you want more than one Team Workplace server to share a Place Catalog on a remote server, each Team Workplace server must have its own qpconfig.xml which specifies the server and file name of the Place Catalog. After you have set qpconfig.xml to point to the correct Place Catalog server, you can delete the local Place Catalog database on the Team Workplace server.

After you set up Place Catalog you must register any previously existing places.

You can set up one Place Catalog to service your enterprise, or set up several Place Catalogs to service different areas of your enterprise. It is recommended that an enterprise have a designated Place Catalog server (or servers) whose only purpose is to contain the Place Catalog. Each Place Catalog server should be part of a cluster with at least one failover server.

To set up a remote Place Catalog server shared by more than one server

1. Install a Team Workplace.
2. Make sure the server is accessible to other Team Workplace servers over Lotus Notes RPC (TCP/IP port 1352) and the HTTP protocols. This is set up by default.
3. In the ACL of the Place Catalog database, give access to Team Workplace servers and system administrators only. By default, the database has the following listed as Managers in the ACL: Team Workplace server, the system administrator, LocalDomainServers, and QuickPlaceAdministratorsSUGroup.
4. Open the Place Catalog database from the Domino Administrator client and create a full-text index. The Place Catalog database must be full-text indexed for the QPTool report command and the My Places feature to work. For more information on creating and updating full-text indexes, see Domino Administrator Help.

To configure Place Catalog qpconfig.xml settings

1. On each Team Workplace server that will communicate with the Place Catalog server, create a file called qpconfig.xml and save it as a text file.
2. Copy the following content to qpconfig.xml from qpconfig_sample.xml, replacing sample values with your own values. For descriptions of each XML tag, see the next topic “Place Catalog XML.”

For more information on copying from the sample file, see the chapter “Team Workplace Administration Overview.”

```
<?xml version="1.0" standalone="yes"?>
  <server_settings>
    <place_catalog enabled="true" log_level="0">
      <connection_pool size="8" />
      <place_catalog_servers>
        <server>

          <domino_server_name>
servername/enterprise</domino_server_name>
            <nsf_filename>PlaceCatalog.nsf</nsf_filename>
          </server>
        </place_catalog_servers>
      </place_catalog>
    </server_settings>
```

3. If the Team Workplace server is part of a cluster, set the appropriate values within the <cluster> node.

For more information on configuring a clustered Team Workplace server to work with the Place Catalog, see the chapter “Administering Team Workplace Servers in a Cluster.”

4. Restart the server.

To register existing places and servers with the Place Catalog

A Team Workplace server may already contain places that were created prior to configuring the Place Catalog, or that were added from a different server. In this case, the Place Catalog must be told of the existence of these places. This is done by using the QPTool register command.

Note Because the Place Catalog must uniquely identify a place by its name, two different places cannot have the same name. When upgrading an existing QuickPlace installation where two different places might have the same name on two different servers, the administrator must first resolve the conflict by unregistering one of the places, renaming its directory, and then registering the place with the new name. Registration is a Team Workplace feature that includes functionality from the previous utility Qpmove.

For more information on the QPTool register command, see the chapter “Using QPTool Commands.” For more information on upgrading to a Team Workplace 6.5.1 enterprise, see the *Team Workplace Installation and Upgrade Guide*.

Team Workplace servers also must be registered with the Place Catalog. You can do register servers either by creating a place on the server, which automatically creates a server entry in the Place Catalog, or by using the QPTool command “qptool register -server.”

Note If a server is registered in the Place Catalog and you change the port, protocol settings, or a URL prefix for the server, use “qptool unregister -server ” to unregister the server, then use “qptool register -server ” to register the server with the Place Catalog again so that place URLs are constructed correctly. Or update the appropriate fields in the server's PlaceServer document manually in the Place Catalog.

To populate the Catalog with entries for servers, and for places that existed before the Catalog was enabled, enter the following in the Domino server console:

<i>Server console command</i>	<i>Description</i>
load qptool register -server	Registers the server with the Place Catalog.
load qptool register -placecatalog -a	Registers existing places with the Place Catalog.

For more information on registering places and servers with QPTool commands, see the chapter “Using QPTool commands.”

Place Catalog XML

The following table describes each Place Catalog XML setting in the qpconfig.xml file.

Note For information on configuring the Place Catalog to work in a clustered server environment, see the chapter “Administering Team Workplace Servers in a Cluster.”

<i>Element or attribute</i>	<i>Description</i>
place_catalog enabled	The place_catalog section contains settings to enable the server to use a Place Catalog. Set the "enabled" attribute to "true" to tell the server to search for an existing Place Catalog. The default setting is enabled="true." To prevent the server from looking for a Place Catalog, change the enabled attribute to enabled="false" or remove the entire <place_catalog> section.
log_level	You can log operations related to the Place Catalog in the Domino server console as follows: Level 1 - Logs all Catalog database open and close operations Level 2 - Logs all server registration operations Level 3 - Logs all place registration operations Level 4 - Logs all member registration operations Each level also includes the information in the levels below it.
connection_pool size	For efficiency, the Team Workplace server creates a pool of connections to the Place Catalog that can be shared by the different requests on that Team Workplace server. This number should reflect the number of simultaneous requests that could result in a query or update to the Place Catalog. These types of requests include creation of places, the addition of or changes to place membership, and administration requests made by QPTool. You may want to start with a number representing a third of the maximum HTTP threads. For example, if the server uses 90 threads, then set this value to 30.
place_catalog_servers	This section lists all Place Catalog servers the local Team Workplace server will communicate with. Team Workplace supports only one Place Catalog server.
server	This section specifies settings for a particular Place Catalog server.

continued

<i>Element or attribute</i>	<i>Description</i>
domino_server_name	Specify in Domino format the name of the server hosting the Place Catalog, for example, server/organization.
nsf_filename	Specify the name of the Place Catalog database, for example, PlaceCatalog.nsf.

How the Place Catalog works

The Place Catalog contains data on the Team Workplace servers in your service, the places that live on those servers, and the members of those places. Each server and each place in your service has a separate entry in the Catalog. A Catalog entry is implemented as a Lotus Notes® document.

The following figure shows an example of a Catalog entry for a place titled “Place One.”

Place

PlaceName	place1
PlaceTitle	Place One
PlaceServerName	server1.acme.com
PlaceServerIsMaster	1
PlaceServerIsVirtual	0
PlaceSize (K)	2746
PlaceLastAccessed	04/10/2003 06:37 PM EDT
PlaceLastModified	04/10/2003 06:36 PM EDT
PlaceIsLocked	0
PlaceReaders	Anonymous
PlaceAuthors	CN=Administrators; CN=qp group
PlaceManagers	CN=Heather Nelson,0=Directory

The following figure shows a Catalog entry for a Team Workplace server called “server1.acme.com.”

PlaceServer

PlaceServerName	server1.acme.com
PlaceServerIsMaster	1
PlaceServerIsVirtual	0
PlaceServerClusterName	
PlaceServerAccessProtocol	http
PlaceServerAccessTCPPort	80
PlaceServerAccessURLPrefix	

How entries are updated

Some entries are created or updated in the Place Catalog in real time — the moment an event happens. Other entries are created or updated manually by a server task, or on a scheduled basis.

It is essential that certain data be sent in real time to avoid conflicts. For example, in a Team Workplace service there cannot be two places with the same name. The creation of a new place is an event that creates a new Catalog entry in real time. When a user creates a new place, Team Workplace first checks the Catalog for that name before creating a new entry. If it finds an existing place with that name, the user is prompted to choose a different name. If the creation of a place did not immediately create an entry, it would be possible for two users to create two places with the same name, which would cause a conflict when Team Workplace attempted to create entries for both in the Catalog. For this reason, a Place Catalog server that a Team Workplace server is configured to use must always be available. To increase availability of the Place Catalog, the Domino clustering feature can be used to make several Place Catalog servers available.

The following events create or update Place Catalog entries in real time:

<i>Event</i>	<i>Description</i>
A Team Workplace server is registered in, or unregistered from, the Team Workplace service.	A server becomes part of the service when <i>qptool register -server</i> command is issued, or when a place is created on the server. When a place is created, an entry for the server is immediately created in the Catalog if one does not already exist. Similarly, when <i>qptool unregister -server</i> is issued, the entry for the server is immediately removed from the Catalog.
Removal of a place from the service by <i>qptool unregister</i> .	The server's place entry is removed. If the place is part of a Team Workplace server cluster with a virtual server, the virtual server place entry is also removed. For more information on virtual servers in a cluster, see the chapter "Administering Team Workplace Servers in a Cluster."
Creation of a place from a browser or registration of a place by <i>qptool register</i> .	A new entry is created. The Place Catalog server must be running for users to create new places in the service. If the place is created on one server in a cluster, an entry for the virtual server is also created.
Creation of a place on a cluster server node by <i>qptool replicamaker</i> .	A place entry for that server cluster node is created.
Deletion of a place from a browser or by <i>qptool remove</i> .	The place's entry is deleted. Its name cannot be used for a new place until the QPTool remove — cleanup command has run, either automatically overnight, or manually by the administrator. In a cluster environment, this would have to be done on all cluster nodes.
Deletion of a place in a cluster server node by <i>qptool remove -cleanup</i> .	The place's entry for that server node is deleted from the catalog.
Creation of a member.	The new member is added to the place entry with the proper access level.
Deletion of a member.	The member is removed from the place entry.

continued

<i>Event</i>	<i>Description</i>
A change in member access.	The member moves to the field appropriate to their new access level.
A place is accessed.	The PlaceLastAccessed field is updated, which can take up to a minute.
Locking a place by <i>qptool lock</i> .	The PlacesLocked field of the Place Catalog entry is set to 1. If the place is in a cluster with a virtual server, the PlacesLocked field in the virtual server entry is also set to 1.
Unlocking a place by <i>qptool unlock</i> .	The PlacesLocked field of the Place Catalog entry is set to 0. If the place is in a cluster with a virtual server, the PlacesLocked field in the virtual server entry is also set to 0.

The following data can be updated using the QPTool placecatalog -push command or on a schedule on the Team Workplace server.

<i>Event</i>	<i>Description</i>
Place size.	The PlaceSize field is updated.
Dates and times the place was last modified.	The PlaceLastModified field is updated.

To update the PlaceSize and PlaceLastModified data on a particular place, enter the following commands from the server console:

<i>Server console command</i>	<i>Description</i>
<i>load qptool placecatalog -p placename(s) -push</i>	Updates size and last modified data for the place you specify. To specify more than one place, separate the placenames with spaces.
<i>load qptool placecatalog -a -push</i>	Updates size and last modified data for all places on the server.
<i>load qptool placecatalog -?</i>	Outputs quick help on the syntax of all the placecatalog arguments.
<i>load qptool placecatalog -i inputfilename -push</i>	Takes an XML file specifying the places to update. For more information on updating the Place Catalog with an XML input file, see the <i>Team Workplace Developer's Guide</i> .
<i>load qptool placecatalog -p placename(s) -o outputfilename -push</i>	Outputs the places that have been updated to a non-default output file. (The default file is qptool.placecatalog.xml in the server's program directory.)

Note This command cannot be used on a pre-6.5.1 place that has not been upgraded by qptool upgrade.

Or to update the the PlaceSize and PlaceLastModified fields at 2 AM, add the appropriate command line entry from the preceding table to the ServerTasksAt2= line in the server's notes.ini file. Or, if you want multiple servers in the Team Workplace/Domino domain to share the schedule, create a server program document in the Domino Directory of the Team Workplace domain. For more information on creating a server program document, see Domino Administrator Help.

For more information on QPTool commands, see the chapter “Using QPTool Commands.”

Synchronizing Place Catalog data in a cluster

In an enterprise with a Team Workplace server cluster, the QPTool placecatalog -update command can be run on the Place Catalog server to synchronize data between a place's entries on each physical server, and the place's virtual entry. For example, before QPTool placecatalog -update is run, the place's virtual entry contains the membership information, but the place's physical server entries do not. After QPTool placecatalog -update, both entries contain the same field values.

For more information on clusters, see the chapter “Administering Team Workplace Servers in a Cluster.”

Enabling DBCS members to use My Places

For double-byte character set (DBCS) users to use My Places:

- The users must be from an external user directory.
For more information on external user directories, see the chapter “Connecting to a User Directory.”
- The server must be configured for session-based (single sign-on) authentication. You configure session-based authentication through Domino.

For more information, see the chapter “Setting Up Security.”

Chapter 4

Managing PlaceTypes

This chapter describes how to create PlaceTypes to use as blueprints for creating places, order PlaceTypes in the list of PlaceTypes, refresh PlaceTypes, and copy and delete PlaceTypes.

PlaceTypes

As you set up a place to meet the needs of your team or organization, you may want to preserve your customizations for use in other places. For example, if a manager has created a theme that gives a particular place the look and feel of your corporate Web site, you may want to make that design available for the creation of other places in your organization.

You can preserve the design and content of a place by creating a PlaceType. A PlaceType is a blueprint from which users can create places. You can take a snapshot of a place and make it a PlaceType. Also, you can control the design and content of a child place by refreshing it with updates from the PlaceType.

Creating a PlaceType and making it available to users is a two-step process. A user with Manager access to a place customizes the place, allows it to be a PlaceType, and specifies which design elements will be preserved in the PlaceType. Then a server administrator must create the PlaceType on the server so it is available to users. For more information on customizing a place, allowing it to be a PlaceType, and determining which membership and design elements will be inherited from it, see the Help.

Creating a PlaceType

To create a PlaceType, do the following.

1. Sign in to the Team Workplace home page as an administrator.
2. Click PlaceTypes in the table of contents.
3. Click Create PlaceType.
4. Enter a name for the PlaceType. The name you enter here appears in the list of PlaceTypes a user sees when they create a place.

For example, a Team Workplace developer creates a new place called “Sales” and gives it the look and feel you want to appear in places created by the Sales team. The developer allows it to be a PlaceType, and you create a PlaceType from it called “Sales PlaceType.” To test it, you create a place called “Sales Test” from “Sales PlaceType.” If you want to change some design elements, you can ask the developer to change the elements in “Sales,” then refresh “Sales PlaceType,” then refresh “Sales Test.” “Sales PlaceType” inherits from “Sales,” and “Sales Test” inherits from “Sales PlaceType.”

The QPTool refresh command refreshes places and PlaceTypes. By default, QPTool refresh runs daily at 4 AM to refresh all child places (not including PlaceTypes) on the server. The place manager can control whether QPTool refreshes a place. To refresh a PlaceType, administrators can initiate the refresh command from the administration PlaceTypes room or use the traditional method for running QPTool commands.

Note When you refresh a place or PlaceType in a cluster, do the refresh on one server only and then let the changes replicate to the other servers.

For more information on the QPTool refresh command, see the chapter “Using QPTool Commands.”

Place membership

If the place manager allows it, membership of a place can be passed to a PlaceType when the PlaceType is created. That membership is then passed to new places created from the PlaceType. For example, if Annie was a member of “Sales” with Author access, she became an Author in “Sales PlaceType” and “Sales Test” when they were created.

However, changes to members and membership are not inherited when you refresh. For example, if the manager of “Sales” changes Annie’s access to Reader in “Sales,” when you refresh “Sales PlaceType” and “Sales Test,” Annie still has Author access in “Sales PlaceType” and “Sales Test.”

Caution When a new room is inherited, membership to the room is not inherited, but instead is determined by the room’s parent room in the place. For example, to continue the preceding example, assume that the manager of “Sales” adds a new room called “Finances” and gives only herself access to read sensitive information in it. When “Sales PlaceType” and then “Sales Test” are refreshed, “Sales Test” inherits the room “Finances” but all “Sales Test” members with Reader access or above can read “Finances” unless the “Sales Test” manager changes access.

Levels of refresh

There are two levels of refresh available for a place: basic refresh (the default level) or replace. With basic refresh, elements originating from a PlaceType but modified directly in a place are not affected by the refresh. For example, basic refresh does not affect changes a place manager makes to the Welcome page.

A replace occurs only when you use QPTool refresh command with the `-r` argument. Use replace with extreme caution because it causes all elements in a place that originated from a PlaceType to be updated, even elements modified directly in the place.

Neither basic refresh nor replace modifies elements that were created directly in a place rather than originating from a PlaceType.

Because changes to a PlaceType are never made directly in a PlaceType but instead can occur only through a refresh, it makes no difference which level of refresh you use to refresh PlaceTypes.

How basic refresh affects the elements in places

If you do a basic refresh of a child place with its PlaceType, and there are no changes in the PlaceType, the refresh causes no change in the child place. If there are changes in the PlaceType, the child place does not inherit an element change or deletion from the PlaceType if the element was also changed or deleted directly in the child place. The following tables describe this behavior in detail.

Elements modified in the PlaceType

The following table describes what happens as the result of a basic refresh of a place when elements have changed in its PlaceType.

<i>Element modified in PlaceType</i>	<i>Refresh effect on element in place if element not changed in place</i>	<i>Refresh effect on element in place if element changed in place</i>	<i>Refresh effect on element in place if element deleted in place</i>
Page	Updated	No change	No change
Folder	Updated	No change	No change
Room	Updated	No change	No change
Form	Updated	No change	No change
Field	Updated	No change	No change
Theme	Updated	No change	No change
PlaceBot	Updated	No change	No change
Room Setting	Updated	No change	No change
Aesthetic Settings	Updated	No change	No change
Member	No change	No change	No change
Local group	No change	No change	No change

Elements deleted in the PlaceType

The following table describes what happens as the result of a basic refresh of a place when elements have been deleted in its PlaceType.

<i>Element deleted in PlaceType</i>	<i>Refresh effect on element in place if element not changed in place</i>	<i>Refresh effect on element in place if element changed in place</i>	<i>Refresh effect on element in place if element deleted in place</i>
Page	Deleted	No change	No change
Folder	Deleted*	No change	No change
Room	Deleted**	No change	No change
Form	Deleted	No change	No change
Field	Deleted	No change	No change
Theme	Deleted	No change	No change
PlaceBot	Deleted	No change	No change
Room Setting	N/A	N/A	N/A
Aesthetic Settings	N/A	N/A	N/A
Member	No change	No change	No change
Local group	No change	No change	No change

*Folders that contain pages originating from a PlaceType but modified directly in the place, or that contain pages created in the place rather than originating from a PlaceType, are not deleted.

**Rooms that contain elements originating from a PlaceType but modified directly in the place, or that contain elements created in the place rather than originating from a PlaceType, are not deleted.

A task page in a place derived from a PlaceType lists [h_Managers] as editor

Note In a place that is derived from a PlaceType, all task pages display [h_Managers] in “Who can edit this task”. Since membership is not refreshed, members removed from the place will not be added back during refresh. The [h_Managers] entry ensures that managers of the place can edit the page if all other editors are removed from the place.

How replace affects the elements in places

If you replace a place with its PlaceType — using `qptool refresh -r` — changes made to elements directly in the place that originated in the PlaceType are lost. For this reason you should use `replace` with extreme caution. The following tables describe the behavior of a `replace` in detail.

Elements not changed in the PlaceType

The following table describes what happens as the result of a `replace` of a place when elements have not changed in its PlaceType

<i>Element not changed in PlaceType</i>	<i>Replace effect on element in place if element not changed in place</i>	<i>Replace effect on element in place if element changed in place</i>	<i>Replace effect on element in place if element deleted in place</i>
Page	No change	Replaced	Copied back
Folder	No change	Replaced	Copied back
Room	No change	Replaced	Copied back
Form	No change	Replaced	Copied back
Field	No change	Replaced	Copied back
Theme	No change	Replaced	Copied back
PlaceBot	No change	Replaced	Copied back
Room Setting	No change	Replaced	Copied back
Aesthetic Settings	No change	Replaced	Copied back
Member	No change	No change	No change
Local group	No change	No change	No change

Elements modified in the PlaceType

The following table describes what happens as the result of a replace of a place when elements have been modified in its PlaceType.

<i>Element modified in PlaceType</i>	<i>Replace effect on element in place if element not changed in place</i>	<i>Replace effect on element in place if element changed in place</i>	<i>Replace effect on element in place if element deleted in place</i>
Page	Updated	Replaced	Copied back
Folder	Updated	Replaced	Copied back
Room	Updated	Replaced	Copied back
Form	Updated	Replaced	Copied back
Field	Updated	Replaced	Copied back
Theme	Updated	Replaced	Copied back
PlaceBot	Updated	Replaced	Copied back
Room Setting	Updated	Replaced	Copied back
Aesthetic Settings	Updated	Replaced	Copied back
Member	No change	No change	No change
Local group	No change	No change	No change

Elements deleted in the PlaceType

The following table describes what happens as the result of a replace of a place when elements have been deleted in its PlaceType.

<i>Element deleted in PlaceType</i>	<i>Replace effect on element in place if element not changed in place</i>	<i>Replace effect on element in place if element changed in place</i>	<i>Replace effect on element in place if element deleted in place</i>
Page	Deleted	Deleted	No change
Folder	Deleted*	Deleted*	No change
Room	Deleted**	Deleted**	No change
Form	Deleted	Deleted	No change
Field	Deleted	Deleted	No change
Theme	Deleted	Deleted	No change
PlaceBot	Deleted	Deleted	No change
Room Setting	N/A	N/A	N/A
Aesthetic Settings	N/A	N/A	N/A
Member	No change	No change	No change
Local group	No change	No change	No change

*Folders that contain pages created directly in the place rather than originating from the PlaceType are not deleted.

**Rooms that contain any element created directly in the place rather than originating in the PlaceType are not deleted.

Controlling whether the QPTool refresh command refreshes a place

Place managers control whether the QPTool refresh command refreshes places created from a PlaceType. By default, the QPTool refresh command refreshes places. The QPTool refresh command runs on all places created from PlaceTypes daily at 4 AM, but administrators can also run it on specific places.

To specify whether the QPTool refresh command refreshes a place:

1. Open the place.
2. Click Customize in the table of contents.
3. Click Basic.
4. Click “Change Basics.”
5. In the Updates section, check “Receive updates” (default) to allow QPTool refresh to refresh the place. Remove the check mark to prevent QPTool refresh from running on this place.

Refreshing a PlaceType from the PlaceTypes view in the administration place

If a place used to create a PlaceType is modified, you can use the PlaceTypes room in the administration place to initiate the QPTool refresh command to do a basic refresh of the child PlaceType. If you use this method, at the same time you refresh you can modify the description that users see, the image, and the URL provided to users for more information.

1. Sign in to the Team Workplace home page as an administrator.
2. Click PlaceTypes in the table of contents.
3. Click the name of the PlaceType you want to refresh.
4. Click Edit.
5. Do one of the following:
 - To update the description and other information shown and also to refresh the PlaceType, click “Yes (default), copy changes and update the information below.”
 - To update the description and other information shown but not refresh the PlaceType, click “No, simply update the information below.”
6. (Optional) Change the description for the PlaceType.
7. (Optional) Change the image selection for the PlaceType.
8. (Optional) Change the URL information shown.
9. Click Next.

Choosing to refresh the PlaceType in Step 5 starts QPTool refresh in the background. If QPTool refresh is already running when you click Next, the PlaceType is not refreshed since only one instance of QPTool refresh can run at a time. Check the server console to determine whether a PlaceType has been refreshed.

You can also refresh a PlaceType by running the QPTool refresh command from the server console or command line. For more information, see the chapter “Using QPTool Commands.”

Signing a newly inherited scheduled PlaceBot in a place

When a place first inherits a new scheduled PlaceBot (agent), the place manager must sign the PlaceBot before it runs. This step is necessary only for a newly inherited scheduled PlaceBot:

1. Open the place.
2. Click Customize in the table of contents.
3. Click PlaceBots.
4. Select the PlaceBot and click Sign PlaceBot.

Copying a PlaceType

You can use operating system commands to copy a PlaceType from one Team Workplace server to another.

A PlaceType consists of a set of Notes database files (NSF files) in the AreaTypes subdirectory on the Team Workplace server. For example, if you create a PlaceType called Rapid Response, and your Domino and Team Workplace servers are installed in the c://lotus/domino directory, the NSF files for Rapid Response would be stored in the following location:

c:\Lotus\Domino\data\QuickPlace\AreaTypes\Rapid Response\

To copy a PlaceType from one Team Workplace server (server A) to another Team Workplace server (server B):

1. On server B, create a subdirectory for the PlaceType in x:\Lotus\Domino\data\QuickPlace\AreaTypes, where x is the drive on which Domino and Team Workplace are installed.
2. Copy the PlaceType files from server A to the subdirectory you created on server B.
3. If the PlaceType has PlaceBots, you must sign the agents in the database using the server ID of the current server, that is, server B. For more information on signing a database, see Domino Designer Help.
4. Use the following procedure to add the copied PlaceType to the list of PlaceTypes on server B.

To add copied PlaceTypes to the PlaceType list

If you copied PlaceType files to the Team Workplace server, you can add that new PlaceType to the list of PlaceTypes on the current server. You see the list of PlaceTypes when you sign in to the current server as the server administrator and click PlaceTypes in the table of contents. The new PlaceType is also available to Team Workplace creators until or unless you hide the name of the PlaceType.

To add a PlaceType copied from another server to the list of PlaceTypes on the current server, do the following:

1. Sign in to the Team Workplace home page as an administrator.
2. Click PlaceTypes in the table of contents.
3. Click Refresh List.

Deleting a PlaceType

When you follow the steps below or when you use the QPTool remove command without the -now argument, to mark a PlaceType for deletion on the current server, it is no longer available to users. However, the file and directory are not actually deleted until the QPTool remove -cleanup command runs on the server at 2 AM. You can remove the PlaceType immediately by running the QPTool remove -now command.

For more information on the remove command, see the chapter “Using QPTool Commands.”

Note You cannot delete the default PlaceType.

1. Sign in to the Team Workplace home page as an administrator.
2. Click PlaceTypes in the table of contents.
3. In the list of PlaceType names on the screen, click the name of the PlaceType you want to delete.
4. Click Delete.
5. In Team Workplace server cluster, do the following on each additional server in the cluster to remove the PlaceType from the PlaceTypes view of the administration place. This step is necessary because the administration place does not replicate in a cluster.
 - a. Sign in to the Team Workplace home page as an administrator.
 - b. Click PlaceTypes in the table of contents.
 - c. Click Refresh List.

Chapter 5

Administering Team Workplace Servers in a Cluster

This chapter describes how to set up Team Workplace servers in a clustered server environment.

Team Workplace servers in a cluster

A Domino cluster is a group of two to six servers that provides users with constant access to data, balances the workload between servers, improves server performance, and maintains performance when the size of your enterprise increases. The servers in a cluster contain replicas of databases that you want to be readily available to users at all times. If a user tries to access a database on a cluster server that is unavailable, Domino opens a replica of that database on a different cluster server, if a replica is available. Domino continuously synchronizes databases so that whichever replica a user opens, the information is always identical.

Clusters provide high availability of important databases, and clustered servers can redirect database open requests to other servers in the clusters, allowing users uninterrupted access to their databases. You can use clustering to provide high availability of a Team Workplace service, or group of servers. You can administer servers in a cluster by adding, removing, or upgrading them.

Using clustering to provide high availability of the Team Workplace service consists of setting up:

- Two or more servers to replicate the data.
- A solution to distribute HTTP requests to one or more of the servers in the cluster.

Domino Enterprise Server software is used to set up and manage the cluster. The servers in the cluster are sometimes referred to as cluster nodes. Team Workplace is installed on each of these nodes.

There are several solutions available for distributing HTTP traffic among a number of servers. The Team Workplace application requires that HTTP requests sent to one node are continuously sent to that node for a predetermined amount of time. This time period is sometimes known as “sticky time.”

Upgrading an existing Team Workplace server to provide high availability involves:

- Setting up a separate cluster of servers.
- Using QPTool commands to move the places to the newly set up cluster.

For more information on moving places, see the chapter “Using QPTool Commands.”

Administering and managing a Team Workplace server that is in a cluster is the same as administering and managing a server that is not clustered. With the exception of adjustments to the load balancing hardware and software, you make changes individually to each server by addressing the server directly by its hostname or Domino name when you use any of the following methods or tools:

- Using the browser to sign in to the server and visiting the Server Settings page, also known as the Team Workplace Administration Room.
- Using the Domino Administration Client to make changes, usually to the Domino Name and Address Book.
- Making changes using the file system such as modifying the notes.ini file or inspecting HTTP logs.

For information on upgrading a Team Workplace server in a cluster, see the book *Team Workplace Installation and Upgrade Guide*.

Planning capacity

Before you set up a Team Workplace cluster, you must first decide:

- How many concurrent users need to be supported.
- The type of clustering solution to be implemented.

These decisions determine how many servers of a given specification are required to support the user population for a given rate of Team Workplace usage.

Types of clustering solutions

The total number of servers required depends on the type of clustering solution.

The simplest clustering solution is failover to a “hot spare,” in which a primary server and a secondary server are clustered. The primary server handles user requests, and the secondary server is held in reserve in case the primary server fails or requires a scheduled stoppage. When the primary server is taken offline, user requests fail over to the hot spare until the primary server comes back online. In this type of cluster, the resources of the hot spare are not utilized while the primary server is active: the capacity of

the cluster is the capacity of the primary server. Therefore, if a given server specification supports 1,000 concurrent users, two such servers are required to support 1,000 users. If the hot spare is identical to the primary server, the capacity remains the same after the primary server fails over.

To make full use of all available servers, a load-balancing solution can be implemented. With load balancing, servers share the user load, and the maximum capacity of the cluster is approximately the sum of the capacities of the servers in the cluster. For example, a cluster of three servers that each support 1,000 users has approximately a maximum capacity of 3,000 concurrent users. However, if one server goes offline, the capacity of the cluster is reduced correspondingly (to 2,000 users in the example). Therefore, the average capacity of a load-balanced cluster is less than the maximum possible, and allowance should be made for server downtime so that response times do not significantly decrease when a single server becomes unavailable. Having more than two servers in a cluster provides greater flexibility and reliability because when a server is taken offline for scheduled maintenance, failover can still occur among the remaining available servers.

Creating a cluster

To create a cluster, you must have at least Author access, Delete Documents rights, and the ServerModifier and ServerCreator roles in the Domino Directory, and at least Author access in the Administration Requests database. If possible, use the administration server when creating a cluster. The administration server does not have to be part of the cluster.

Note If a server belongs to a different cluster, you do not have to remove the server from that cluster before you add it to the new cluster. The Cluster Administration Process removes the server from the original cluster and then adds it to the new cluster.

1. From the Domino Administrator, make sure the administration server or another server is current.
2. Click the Configuration tab.
3. Expand Server, and click All Server Documents.
4. In the Results pane, select the servers that you want to add to the cluster.
5. Click Add to Cluster.
6. When asked to choose the cluster you want to add the servers to, choose Create New Cluster, and then click OK.
7. Type the name of the new cluster, and click OK.
8. Choose Yes to add the servers to the cluster immediately, or choose No to submit a request to the administration process to add the servers to the cluster.

The following table describes the values you specify for the cluster setting.

<i>Attribute</i>	<i>Description</i>
virtual=" value "	The master server in a cluster acts as a user's entry point to places on other servers in the cluster. If you use the failover to a "hot-spare" clustering solution in which the master server is a physical Team Workplace server, specify virtual="false." If you use the load balancing clustering solution, in which the master server is an IP sprayer such as IBM Network Dispatcher that acts as a "virtual" server, specify virtual="true."
ssl=" value "	If SSL is enabled on the master server, specify ssl="true," otherwise specify ssl="false."
<port> number </port>	Specify the TCP port used to access Team Workplace requests by browsers, depending on whether SSL is enabled on the master server. The default port is 80 for non-SSL connections and 443 for SSL connections.
<hostname> name </hostname>	Specify the DNS hostname of the master server (for example, tw.acme.com).
<path_prefix> prefix </path_prefix>	Specify an optional path prefix used when creating URLs to the master server.

Place Catalog entries and clusters

There are two Team Workplace server cluster environment alternatives for storing Team Workplace server cluster data in the Place Catalog.

- If the cluster does not have a virtual server, data is maintained in separate entries in the Place Catalog for each physical server, and for each place on a physical server.
- If the cluster has a virtual server, each physical server and place has an entry. But there is also an entry for the virtual server that represents the combination of all physical servers. And there is an entry for each place in the cluster that represents all the replicas of the place in the cluster.

Chapter 6

Setting Up Security

This chapter describes the following topics related to Team Workplace security:

- Team Workplace authentication
- Setting up multi-server single sign-on authentication
- Modifying user cache settings
- Controlling access to the server
- Using expanded membership
- Blocking specific protocols referenced in link URLs
- Blocking HTML attachments that contain cross-site scripts

Team Workplace authentication

Team Workplace supports these types of authentication for Web browsers connecting to a Team Workplace server:

- Basic name-and-password authentication
- Multi-server single sign-on name-and-password authentication

Basic authentication is implemented by default. You can enable multi-server single sign-on so that Web users can log on once to a server and then automatically access any other server in the DNS domain enabled for single sign-on.

Note To use SSL to encrypt the data transferred between Web browsers and a Team Workplace server, enable SSL on the Domino Web server. For more information, see Domino Administrator Help.

Team Workplace supports custom authentication applications through the Domino Server API (DSAPI). This interface allows some third-party vendors to design a DLL to support authentication for access to Team Workplace databases.

Multi-server single sign-on authentication

Enable multi-server single sign-on authentication so that Web users can log in once to a Team Workplace server and automatically access any other Team Workplace servers in the DNS domain that are enabled for single sign-on without having to log in again.

To set up multi-server single sign-on authentication, you first create a Web SSO Configuration document for the domain. Then you complete single sign-on setup by modifying the notes.ini file, enabling multi-server session authentication, and adding a mapping form to the Domino Web Server Configuration database.

Keep the following points in mind about single sign-on authentication:

- Team Workplace does not support single-server sign-on authentication, but setting up multi-server sign-on authentication on a single server achieves a similar result.
- URLs issued to servers configured for single sign-on must specify the full DNS server name, not the host name or IP address. For browsers to be able to send cookies to a group of servers, the DNS domain must be included in the cookie, and the DNS domain in the cookie must match the server URL. This is why cookies cannot be used across TCP/IP domains.
- Clustered servers must have the full DNS server name in the host name field of the Web Site or Server document. This enables the Internet Cluster Manager (ICM) to redirect to cluster members using SSO. If the DNS server hostname is not there, ICM will redirect URLs to clustered Web servers with only the TCP/IP host name, by default, and will not be able to send the cookie because the DNS domain is not included in the URL.

Creating or editing Web SSO Configuration document

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

To set up multi-server single sign-on for a Team Workplace server, first create a Web SSO Configuration document, if there isn't one already. If there is already a Web SSO Configuration document, add the Domino server names of the Team Workplace servers to the document.

After you create or edit the Web SSO Configuration document, follow the steps in the topic “Completing single sign-on setup.”

7. 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 or people for whom the document is encrypted.

If you receive messages on the client indicating that a particular key was not found for encrypting the document, you might have to change your client's location document to point to a different mail or directory server that has all the public keys included in Server and Person documents.

8. Follow the steps in the topic, "Completing single sign-on setup."

To add names of Team Workplace servers to an existing Web SSO Configuration document

A Web SSO Configuration document may already exist for the domain. This might be the case, for example, if a Sametime server is also installed in the domain. In this case, follow these steps to add the Domino names of the Team Workplace servers to the existing Web SSO Configuration document.

1. Open the Domino Directory (names.nsf) of a Team Workplace server in the domain.
2. Select the Web - Web Configurations view.
3. Open the Web SSO Configuration document in edit mode.
4. In the "Domino Server Names field," add the Domino server name of each Team Workplace server in the domain that will participate in single sign-on; for example, server1/acme, server2/acme.
5. Close and save the document.
6. Follow the steps in the next topic, "Completing single sign-on setup."

Completing single sign-on setup

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

1. Add the following setting to the notes.ini file of each Team Workplace server that you will enable for single sign-on to prevent anonymous access to files in the html directory:
NoWebFileSystemACLs=1
2. Enable multi-server single sign-on authentication in the Server document for each Team Workplace server that you want to enable for single-sign on:
 - 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**.

Controlling access to the server

As an administrator of a Team Workplace server, you can do these access control tasks:

- Specify other users as administrators of the Team Workplace server.
- Change the password you use when you sign in as an administrator of the Team Workplace server.
- Specify who can create places on a Team Workplace server.
- Give an external user or group super user access to the Team Workplace server.

Specifying administrators of a Team Workplace server

You specify an administrator for a Team Workplace server when you set up the server. You can specify additional local users, external users, or external groups as administrators of a Team Workplace server. An administrator can do the following tasks:

- Configure Security settings in the Server Settings room to control who can administer the server and who can create places.
- Configure User Directory settings in the Server Settings room to set up server connections to a user directory.
- Configure Other Options in the Server Settings room to configure a variety of other server options.
- Create and delete places and PlaceTypes on the server.

Specifying local users as administrators

To specify a local user as an administrator:

1. Sign in to the Team Workplace home page as an administrator.
2. Click Server Settings in the table of contents.
3. Click Security in the table of contents.
4. If the Team Workplace server is not connected to a user directory, do the following:
 - a. Under “Who can administer this server,” click Add.
 - b. Specify the user name, password, and e-mail address for the administrator.
 - c. Click Next.

Removing the name of an external user from the list of users who can create places

To remove the name of an external user or group from the list of users who can create places:

1. Sign in to the Team Workplace home page as an administrator.
2. Click Server Settings in the table of contents.
3. Click Security in the table of contents.
4. Below “Who can create new places on this server?” click Remove.
5. Select the name to remove.
6. Click Next to remove the user from the list.

Allowing all users who have access to the server to create places

To allow any user who can access a Team Workplace server to create places on it:

1. Sign in to the Team Workplace home page as an administrator.
2. Click Server Settings in the table of contents.
3. Click Security in the table of contents.
4. Under “Who can create new places on this server?,” select “Anyone who can connect to the server.”

Specifying super user access to a Team Workplace server

Users granted super user access can enter every place and every room as managers. Members of places are unaware of super users. A user with super user access can also use the Server Settings room in the administration place to administer the server.

By default no super user is defined. You can't give super user access to a local user or a local group.

Note Offline functionality is not supported for a super user.

Specifying who has super user access from a browser

To specify who has super user access when accessing the server from a browser, use the `super_user` section of the `qpconfig.xml` file. You can specify only one name as a super user, either a user name or a group name.

For information on creating and using the `qpconfig.xml` file, see the chapter “Team Workplace Administration Overview.”

To configure a super user, specify the `super_user` setting as follows:

```
<server_settings>
  <super_user enabled="true">
    <dn>name</dn>
  </super_user>
</server_settings>
```

where *name* is the distinguished name of a user or group in the external user directory. The distinguished name must appear exactly as it does in the external directory. For example, if there are spaces after the component delimiters, there must be spaces in the super user entry as well.

To disable super user access from a browser, remove or comment out the `super_user` setting in `qpconfig.xml`.

Specifying who has super user access from a Notes client

To specify who has super user access when accessing the server from a Notes client, do the following:

1. Create a group called `QuickPlaceAdministratorsSUGroup` in the Domino Directory used by the Notes client.
2. Add as members the names to which you want to grant super user access.

You can specify two different names for super user access, one name for access from the browser set in `qpconfig.xml`, and another name for access from a Notes client specified using the `QuickPlaceAdministratorsSUGroup`.

If you want to give the same user or users super user access through the browser and Notes, and the Notes client Domino Directory is also the Team Workplace user directory, you can use the `QuickPlaceAdministratorsSUGroup` to manage both types of super user access. Create the `QuickPlaceAdministratorsSUGroup` as described above, and also specify `cn=QuickPlaceAdministratorsSUGroup` as the distinguished name for the `super_user` setting.

Super user access combined with explicit membership

If a user is a super user as well as an explicit member of a place, the access level the user has to the place depends on whether the place uses standard membership or expanded membership. If the place uses standard membership, the user gets the access assigned through the explicit membership. If the place uses expanded membership, the user gets super user access to the place.

For example, if a user with super user access is also a member of a place with Reader access and the place uses standard membership, the user has Reader access to the place. However, if the place uses expanded membership, the user has super user access to the place.

Expanded membership

Team Workplace by default lists the names of place members in the database access control lists (ACLs) of the rooms in a place. The combined names in an ACL cannot exceed 32K in size, which limits a place to approximately 300 to 900 members, depending on the length of the members' distinguished names. Expanded membership removes this limitation by generating groups in an LDAP directory to store the names of individual members, and then uses these groups, rather than the individual user names, in room ACLs. Currently expanded membership is certified for a maximum of 4000 external user members in a place.

Expanded membership pertains to individual external user place members and not to local or to external group place members.

Expanded membership groups

When a place uses expanded membership, Team Workplace creates room-specific access control groups in an LDAP directory specified through the `qpconfig.xml` file. The LDAP directory can be the same one that Team Workplace uses for other purposes, or a separate directory.

Team Workplace creates the following three groups in this LDAP directory for the main room (Main.nsf) of a place and adds them to the main room database ACL:

```
cn=h_Managers,ou=placename,base_dn
```

```
cn=h_Authors,ou=placename,base_dn
```

```
cn=h_Readers,ou=placename,base_dn
```

where

placename is the name of the place.

base_dn is a base distinguished name for the expanded membership groups that is configured through the `qpconfig.xml` file.

When an external user member is added to the place, Team Workplace adds the user's name to one of these groups, according to the access assigned to the user. For example, Team Workplace adds an external user member with Reader access to the place's "cn=h_Readers...." group.

If someone creates a subroom, Team Workplace creates the following groups in the directory, and adds the groups to the subroom ACL:

`cn=h_Managers,ou=uniquenumber,ou=placename,base_dn`

`cn=h_Authors,ou=uniquenumber,ou=placename,base_dn`

`cn=h_Readers,ou=uniquenumber,ou=placename,base_dn`

where

uniquenumber is the unique number XXXXXXXX in the room name “PageLibraryXXXXXXXX.nsf” that identifies the room.

placename is the name of the place that contains the room.

base_dn is the base distinguished name configured for the expanded membership groups.

Removing an external user member from a place removes the user’s name from the expanded membership groups associated with the place. Removing an external user member from a subroom, removes the user’s name from the appropriate Team Workplace group associated with the subroom. Removing a place or a subroom removes the expanded membership groups associated with the place or subroom.

Examples of expanded membership groups

Suppose a place named `salestrends` uses expanded membership and the base distinguished name specified in the `qpconfig.xml` file for the expanded membership groups is `ou=groups,o=teamworkplace`. If someone adds an external user member to `salestrends` with Author access, Team Workplace adds the user’s name to a group created in the LDAP directory called `cn=h_Authors,ou=salestrends,ou=groups,o=teamworkplace`. The group is included in `salestrends’ Main.nsf` room ACL.

Suppose someone creates a subroom named `PageLibrary85256CD200797D7B.nsf` within `salestrends` and adds an external user member to the subroom with Reader access. Then Team Workplace adds the user’s name to a group generated in the LDAP directory called `cn=h_Readers,ou=85256CD200797D7B,ou=salestrends,ou=groups,o=teamworkplace`. The group is included in the subroom ACL.

Access control in places that use expanded membership

Expanded membership uses group names in room ACLs rather than individual user names to control the access of individual external user members. As a result, the access given to an individual external user member no longer takes precedence over the access assigned to groups the user belongs to, or over super user access. The access control behavior for expanded membership differs from standard membership in the following ways:

- With expanded membership, an external user who is an explicit member of a place and who is also a super user has super user access to the place. With standard membership, the external user has the access the place assigns the user, not the super user access.
- With expanded membership, if an external user is an explicit member of a place (through a Team Workplace group) and also belongs to another group that is a member of the place, the user's access is the higher access of the two groups. With standard membership, the user has the access assigned to the individual user member.

User interface differences in places that use expanded membership

If you enable expanded membership for a place, users see the following changes:

- **Adding Members.** When users add members, they are no longer presented with a list of members with check boxes next to the member names. Instead, they click a Members button to display a Select Members dialog box from which they can search for the members to add.
- **Creating PlaceBots.** To create PlaceBots in a place, users must add a local user as a manager by selecting “Create new users specially for this place” in the Add Managers scene and then sign in as that manager.
- **Publishing Pages.** When users publish pages, the “Notify all members” option is not available.
- **Creating PlaceTypes.** Users cannot create a PlaceType from a place that uses expanded membership.

Important points about expanded membership

Keep these points in mind when using expanded membership:

- After you have set up places to use expanded membership, you cannot revert the places to standard membership.
- Do not disable expanded membership on the server if there are places that use it.
- If the directory server used for the expanded membership groups is the same one used for the Team Workplace user directory, specify a base distinguished name for the expanded membership groups that is outside the scope of the base distinguished name that Team Workplace uses for group lookups generally.
- Administrators should not modify the expanded membership groups.
- The LDAP directory that stores the expanded membership groups must allow write access.
- The user name and password that Team Workplace uses to manage the expanded membership groups (configured through Server Settings – User Directory) must have write access to the base distinguished name configured for the groups.
- Expanded membership is certified for 4000 external user members in a place.
- LDAP directory servers can limit the number of members allowed in groups.

Setting up expanded membership

Complete these steps to set up expanded membership:

1. Enable expanded membership on the server.
2. Configure the user name and password to use for connecting to the LDAP server that will store the expanded membership groups.
3. Enable places to use expanded membership.

Enabling expanded membership on the server

To enable expanded membership, use the `expanded_membership_model` settings in `qpconfig.xml`. The following sample setting values in bold are ones that you can customize to suit your needs.

You can enable expanded membership only if the Team Workplace server connects to a directory server over LDAP, and not if connects to a Domino Directory on a Domino server over NRPC.

```
<server_settings>
  <expanded_membership_model enabled="true">
    <ldap_server ssl="false">
      <port>389</port>
      <hostname>twgroups.acme.com</hostname>
      <base_dn>ou=teamworkplace,o=twgroups</base_dn>
    </ldap_server>
  </expanded_membership_model>
</server settings>
```

After you have modified and save the qpconfig.xml file, restart the HTTP task on the server. For more information on creating and using the qpconfig.xml file, see the chapter “Team Workplace Administration Overview.”

expanded_membership_model setting

To enable expanded membership, specify enabled= “true.” Note that after places are set up to use expanded membership you cannot revert them to the standard membership model.

To disable expanded membership specify “false,” or remove the expanded_membership_model section from the qpconfig.xml file. However, don’t disable expanded membership if there are any places that use it.

ldap_server – ssl setting

Specify “true” to use SSL encryption when connecting to the LDAP directory server that will store the expanded membership groups. Otherwise, specify “false.”

ldap_server – port setting

Specify the port number used by the LDAP directory server that will store the expanded membership groups. Typically an LDAP server uses port 389 for unencrypted connections and port 636 for SSL connections.

ldap_server – hostname setting

Specify the host name of the LDAP directory server that will store the expanded membership groups. The host name can be the same as the one for the Team Workplace user directory specified in the Team Workplace Server Settings room, or a different one. You must specify a host name even if it is the same as the Team Workplace user directory host name. The directory must allow write access.

ldap_server – base_dn setting

Specify the base distinguished name (directory node) under which Team Workplace will create the groups. The base distinguished name must

already exist in the directory — Team Workplace cannot create it. The components of the base distinguished name do not have to be o and ou.

Note Do not use “ou=qp” as part of the base distinguished name because qp is a reserved organizational unit in Team Workplace.

If the directory server that stores the expanded membership groups is the same one that Team Workplace uses for other purposes, specify a base distinguished name for the expanded membership groups that is outside the base specified on the server for group lookups generally. For example, if the base distinguished names specified for group lookups generally is ou=groups,o=acme, use a different base for the expanded membership groups, for example ou=teamworkplace,o=twgroups or ou=twgroups,o=acme. Using separate base distinguished names for the two types of groups optimizes performance by preventing unnecessary searches of all the expanded membership groups during the process of user authentication.

Configuring the name and password to use for connecting to the LDAP server that stores the expanded membership groups

If the directory allows anonymous write access to the base distinguished name (not a typical configuration), this step is unnecessary.

After you’ve enabled expanded membership through the qpconfig.xml file, configure a user name and password for the Team Workplace server to provide when connecting to the directory server that stores the expanded membership groups. The name and password must correspond to a valid user record in the directory, and the name must have write access to the base distinguished name in the directory used for the expanded membership groups.

To configure the name and password:

1. Sign in to the Quickplace/quickplace on the server as an administrator.
2. Click Server Settings in the table of contents.
3. Click User Directory in the table of contents.
4. Click Change Directory.
5. Under Expanded Membership Model:
 - Enter the user name in distinguished name format (for example, cn=qpadmin,o=acme)
 - Enter the password for the name.
6. Click Next.

Using expanded membership logging

By default, Team Workplace logs errors related to the use of expanded membership to the server console and Notes log. To help troubleshoot a problem related to expanded membership, use the notes.ini setting QuickPlaceMembershipModelLogging to increase the level of logging. Specify QuickPlaceMembershipModelLogging=1 to log slightly more detail than the default logging level, or specify QuickPlaceMembershipModelLogging=2 to do verbose logging. Because higher logging levels adversely affect server performance, specify QuickPlaceMembershipModelLogging=0 to remove the setting to revert to the default logging level when you are finished using these higher levels.

Blocking specific protocols referenced in link URLs

By default, Team Workplace publishes pages with links without considering the protocols specified in the link URLs. For tighter security, use the setting URLfield_protocol_filter in the <security> section of the qpconfig.xml file to prevent Team Workplace from publishing pages with URL links that reference specific protocols. The following table describes the attributes you can set.

<i>Attribute</i>	<i>Description</i>
enabled	When set to "true," prevents Team Workplace from publishing pages with link URLs that reference protocols designated as blocked.
allowed	When enabled is set to "true," specifies the protocols in URL links to allow.
blocked	When enabled is set to "true," specifies the protocols in URL links to block.

For example:

```
<server_settings>
  <security>
    <URLfield_protocol_filter enabled="true">
      <allowed>"http:","https:"</allowed>
      <blocked>"javascript:","View-source:","about:","file:","ftp:","news:","mailto:"<
        /blocked>
    </URLfield_protocol_filter>
  </security>
</server_settings>
```

Blocking HTML attachments that contain cross-site scripts

By default, Team Workplace users can import into pages HTML files that contain cross-site scripts. Cross-site scripts can run on other users' browsers. For tighter security, use the following setting in the qpconfig.xml file to prevent users from attaching HTML files that contain cross-site scripts:

```
<server_settings>
  <security>
    <XSS_ImportHTML enabled="false"/>
  </security>
</server_settings>
```

Chapter 7

Customizing the My Places Feature

This chapter describes how to customize the My Places feature.

Customizing the My Places feature

The My Places feature lets users registered in an external user directory see links to all the places of which they are members. Use the following settings in the `my_places` section of the `qpconfig.xml` file to customize a Team Workplace server's My Places configuration. The values in bold are sample values that you can modify to suit your needs.

```
<server_settings>
  <my_places>
    <display_columns>
      <column name="title" enabled="true" />
      <column name="last_modified" enabled="true" />
      <column name="size" enabled="true" />
    </display_columns>
    <sort order="ascending" />
    <results_per_page>10</results_per_page>
    <exclude_by_membership enabled="true">
      <dn>cn=AdminGroup,o=Acme</dn>
    </exclude_by_membership>
    <exclude_by_age enabled="false">
      <last_accessed older_than="30" younger_than="0" />
      <last_modified older_than="40" younger_than="0" />
    </exclude_by_age>
    <exclude_by_size enabled="true" over="100" under="2" />
    <include_anonymous enabled="false" />
    <place_links open_new_window="false" />
    <place_ui enabled="true" show_in_main_place="true">
      <url></url>
    </place_ui>
  </my_places>
</server_settings>
```

For more information on creating and specifying settings in the `qpconfig.xml` file, see the chapter “Team Workplace Administration Overview.”

The following table summarizes the `my_places` settings. For more detailed information on each setting, see the topics that follow.

<i>my_places setting</i>	<i>Description</i>
<code>display_columns</code>	Specifies which columns of place information My Places shows. You cannot hide the name column.
<code>sort</code>	Specifies whether My Places sorts places in ascending or descending order.
<code>results_per_page</code>	Specifies the maximum number of places shown in a page of results.
<code>exclude_by_membership</code>	Excludes specified distinguished names as a member. My Places does not list a place if a user is a member of the place only through the excluded names.
<code>exclude_by_age</code>	Excludes places last accessed or last modified before or after a specified number of days.
<code>exclude_by_size</code>	Excludes places that are larger or smaller than a specified size in megabytes.
<code>include_anonymous</code>	Includes places that users access anonymously.
<code>place_links</code>	Controls whether Team Workplace opens a place accessed through My Places in the current browser window or a new browser window.
<code>place_ui</code>	Enables and disables the My Places link. If enabled, also used to specify a URL of a custom portal application that substitutes for the My Places feature or to open the My Places list in the current page a user is signed into.

Note Users and administrators can override many of the My Places server settings on a one-time basis by adding parameters to the My Places URL.

For more information, see the topic “Using My Places URL parameters to configure My Places” later in this chapter.

display_columns setting

By default, My Places displays the following columns of information for a place: Name, Title, Last Modified date, and Size. Use the `display_columns` setting in the `my_places` section of `qpconfig.xml` to hide the Title, Last Modified, and/or Size column. For example, if long place titles cause the Title column to obscure the Size column, you can hide one of these columns. My Places always shows the Name column — you can't remove this column. You can't change the order in which the columns appear, and Name, Title, Last Modified, and Size are the only columns My Places can display.

The following table describes the values you can specify for the `display_columns` setting in `qpconfig.xml` to control the display of columns.

<i>Attribute</i>	<i>Description</i>
<code>column name="title" enabled="value"</code>	When <i>value</i> is true (the default) My Places shows the Title column. When <i>value</i> is false My Places hides the Title column.
<code>column name="last_modified" enabled="value"</code>	When <i>value</i> is true (the default) My Places shows the Last Modified column. When <i>value</i> is "false" My Places hides the Last Modified column.
<code>column name="size" enabled="value"</code>	When <i>value</i> is true (the default) My Places shows the Size column. When <i>value</i> is false My Places hides the Size column.

Note You can't specify different names for the columns.

For example, to hide the Last Modified and Size columns from My Places, specify the following for the `display_columns` setting:

```
<display_columns>
    <column name="title" enabled="true" />
    <column name="last_modified" enabled="false" />
    <column name="size" enabled="false" />
</display_columns>
```

sort setting

Use the `sort` setting in the `my_places` section of `qpconfig.xml` to specify whether My Places sorts places by name in ascending or descending alphabetical order. Specify the following, or omit the `sort` setting, to sort places alphabetically from lowest to highest (the default):

```
<sort order="ascending" />
```

Specify the following to sort places alphabetically from highest to lowest:

```
<sort order="descending" />
```

results_per_page setting

Use the `results_per_page` setting in the `my_places` section of `qpconfig.xml` to specify the maximum number of places My Places lists in a page of results. The maximum number of places displayed on a page by default is 20. For example, to allow My Places to display a maximum of 10 places in a page, specify the following for the `results_per_page` setting:

```
<results_per_page>10</results_per_page>
```

exclude_by_membership setting

Use the `exclude_by_membership` setting in the `my_places` section of `qpconfig.xml` to prevent My Places from listing places of which users are members only through a specified distinguished name or names. You can specify the name of a group or an individual user. The name must be from a user directory, except for the special case of the name `Anonymous` described below. Typically you use this feature to exclude places of which a user is a member only through a specified group.

If a user is a member of place through an excluded name as well as an unexcluded name, My Places continues to include the place in the user's list of places. For example, assume that you exclude the group `cn=Administrators,o=Acme`, which is member of a place named `salesresearch`. If the user `cn=John Doe,o=Acme` is a member of `salesresearch` only through his membership in the `cn=Administrators,o=Acme` group, My Places doesn't list `salesresearch` in John Doe's list of places. However if the individual name `cn=John Doe,o=Acme` is also a member of `salesresearch`, or if `cn=John Doe,o=Acme` is a member of an unexcluded group that is also a member of `salesresearch`, My Places lists `salesresearch` in John Doe's list of places.

The following table describes the values you specify for the `exclude_by_membership` setting.

<i>Attribute</i>	<i>Description</i>
<code>enabled="value"</code>	<code>enabled=true</code> enables exclusion by membership. <code>enabled=false</code> disables exclusion by membership (the default).
<code><dn>name</code>	The distinguished name of a member (typically a group) to exclude when <code>enabled=true</code> . To exclude additional names, include additional dn attributes. When specifying the attributes used the distinguished name, use the case that the directory uses. For example, if the directory uses lowercase <code>cn</code> rather than uppercase <code>CN</code> in the name, specify lowercase <code>cn</code> . You cannot specify a flat name. For example, you can specify <code>cn=admingroup,o=acme</code> , but not <code>cn=admingroup</code> .

For example, to exclude the group `cn=Administrators,o=Acme`, specify the following for the `exclude_by_membership` setting:

```
<exclude_by_membership enabled="true">
    <dn>cn=Administrators,o=Acme</dn>
</exclude_by_membership>
```

Excluding the name Anonymous

After a user signs in, My Places excludes the places that users access anonymously by default or if you use the setting `<include_anonymous enabled="false" />`. However, before a user signs in, My Places still shows the places users access anonymously. To also prevent users who haven't signed in from seeing the places they access anonymously, specify the name `Anonymous` in the `exclude_by_membership` setting:

```
<exclude_by_membership enabled="true">
    <dn>Anonymous</dn>
</exclude_by_membership>
```

exclude_by_age setting

By default, My Places ignores when places were last accessed or last modified when building My Places lists. Use the `exclude_by_age` setting in the `my_places` section of `qpconfig.xml` to exclude places from My Places based on when they were last accessed or last modified. The following table describes the values you specify for the `exclude_by_age` setting.

<i>Attribute</i>	<i>Description</i>
<code>enabled="value"</code>	When <code>enabled=true</code> My Places excludes places based on last accessed or last modified dates. When <code>enabled=false</code> My Places disables exclusion by last accessed or last modified dates (the default).
<code>last_accessed older_than="days"</code> <code>younger_than="days"</code>	When <code>enabled=true</code> , My Places excludes places that have not been accessed within the number of days specified by the <code>older_than</code> attribute, as well as places that have been accessed more recently than the number of days specified by the <code>younger_than</code> attribute. You can omit the <code>older_than</code> or <code>younger_than</code> attribute.
<code>last_modified older_than="days"</code> <code>younger_than="days"</code>	When <code>enabled=true</code> , My Places excludes places that have not been modified within the number of days specified by the <code>older_than</code> attribute, as well as places that have been modified more recently than the number of days specified for the <code>younger_than</code> attribute. You can omit the <code>older_than</code> or <code>younger_than</code> attribute.

For example, to list only places accessed or modified within the last 30 days, specify the following for the `exclude_by_age` setting:

```
<exclude_by_age enabled="true">
    <last_accessed older_than="30" />
    <last_modified older_than="30" />
</exclude_by_age>
```

To list only places accessed within the last 50 days and modified more than 3 days ago but within the last 30 days, specify the following:

```
<exclude_by_age enabled="true">
    <last_accessed older_than="50" />
    <last_modified older_than="30" younger_than="4" />
</exclude_by_age>
```

exclude_by_size setting

By default, My Places ignores the sizes of places when building My Places lists. Use the `exclude_by_size` setting in the `my_places` section of `qpconfig.xml` to exclude places from My Places lists based on their sizes. The following table describes the values you specify for the `exclude_by_size` setting.

<i>Attribute</i>	<i>Description</i>
<code>enabled="value"</code>	When <code>enabled=true</code> My Places excludes places based on size. When <code>enabled=false</code> My Places disables exclusion of places by size (the default).
<code>over="size" under="size"</code>	When <code>enabled=true</code> My Places excludes places larger than the size specified by the <code>over</code> attribute as well as places smaller than the size specified by the <code>under</code> attribute. Specify a size in MB (megabytes). You can omit one of the attributes.

For example, to list only places that are 100MB or greater, specify the following for the `exclude_by_size` setting:

```
<exclude_by_size enabled="true" under="100"/>
```

include_anonymous setting

My Places lists only places users access through individual or group membership by default, and not places that they access anonymously. Use the `include_anonymous` setting in the `my_places` section of `qpconfig.xml` to show places that users access anonymously, in addition to the places they access as members. Specify `enabled="true"` to allow My Places to show places that user access anonymously. Specify `enabled="false"` (the default) to exclude these places.

For example, to include places users access anonymously, specify:

```
<include_anonymous enabled="true" />
```

Tip By default or if you use the `<include_anonymous enabled="false" />` setting, after users sign in, My Places does not list the places users can access anonymously, but it does list these places before a user signs in. To prevent My Places from showing places users access anonymously before users sign in, specify the name `Anonymous` in the `exclude_by_membership` setting.

For more information, see the topic “`exclude_by_membership` setting” earlier in the chapter.

place_links

When a user clicks a place link in the My Places list, Team Workplace opens the place in the current browser window by default. Use the following setting to open a place accessed through My Places in a new browser window instead:

```
<place_links open_new_window="true"/>
```

place_ui setting

Use the `place_ui` setting to call a custom portal application to display users' lists of places when they click the My Places link. Also use the setting to open the My Places list in the page a user is currently signed into or to disable the My Places link in places. The following table describes the values you specify for the `place_ui` setting.

<i>Attribute</i>	<i>Description</i>
<code>enabled="value"</code>	When <code>enabled="true"</code> (the default), the My Places link shows in all places. When <code>enabled="false"</code> the My Places link is disabled in all places except the main place (QuickPlace/quickplace).
<code>show_in_main_place="value"</code>	When <code>enabled="true"</code> and <code>show_in_main_place="true"</code> (the default), the My Places list always opens in the Quickplace/quickplace main place. When <code>show_in_main_place="false,"</code> the My Places list opens in the current page of the place a user is signed into. Specifying "false" can negatively affect My Places performance if users use My Places to access many places, such as several hundred. Performance is affected because Team Workplace must cache a separate page for each place-specific My Places list, rather than cache just one page from the main place (Quickplace/quickplace).
<code>url</code>	To use a custom application to display users' places when they click the My Places link, for the <code>url</code> attribute, specify a valid URL for the application. The <code>url</code> attribute applies only if <code>enabled="true."</code> If you use the <code>url</code> attribute, Team Workplace ignores all other <code>my_places</code> settings in <code>qpconfig.xml</code> .

For example, to use a custom application to display places when user click the My Places link:

```
<place_ui enabled="true">
    <url>https://portal.abc.com/myplaces</url>
</place_ui>
```

Or to show the Team Workplace My Places list in the current page of the place a user is signed into:

```
<place_ui enabled="true" show_in_main_place="false">
</place_ui>
```

Using My Places URL parameters to configure My Places

You can specify settings for a one-time use of My Places by appending one or more parameters to the Team Workplace server's My Places URL. Most of these parameters correspond to and override the My Places settings on the server, either default server settings or custom server settings specified in the `my_places` section of `qpconfig.xml`.

One use for this feature is place maintenance. For example, administrators can mail users a My Places URL that appends a parameter that lists only places that exceed a specified size, and instruct the users to use the URL to determine which places to delete or reduce in size. Or administrators can mail a My Places URL with a parameter that lists inactive places that users should delete.

The My Places URL for a Team Workplace server is:

```
http://servername/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00E
F85256BB60054A7CB/?OpenDocument
```

The following table describes the My Places URL parameters.

For more information on the purpose of these parameters, see the previous topics that describe the corresponding `my_places` `qpconfig.xml` settings.

Note These parameters are case-sensitive.

<i>URL Parameter</i>	<i>Description</i>	<i>qpconfig.xml setting it overrides</i>
<code>Start=place number</code>	Specifies the place number in the place index at which My Places begins displaying places. The number of the first place in the index is 0. For example, if you specify 10, the first place listed in My Places is the 11th place down in the place index. My Places applies any sort and exclusion settings before applying the Start parameter.	None

continued

<i>URL Parameter</i>	<i>Description</i>	<i>qpconfig.xml setting it overrides</i>
Count= <i>number of places</i>	Specifies the maximum number of places to display per page. Note To display a list of all places which you can then, for example, print out, specify a number of places that you know exceeds the total number.	results_per_page
SortAscending	Sorts places by name in alphabetical order from lowest to highest.	sort
SortDescending	Sorts places by name in alphabetical order from highest to lowest.	sort
ExcludeByMembers= <i>dn;dn...</i>	Specifies one or more distinguished names to exclude as place members. Separate names with semicolons (;).	exclude_by_membership
DisplayColumns= <i>column name;columnname...</i>	Specifies which columns of place information My Places displays. You can specify Title, Last_Modified, and/or Size. Separate column names with semicolons (;). My Places displays only the specified column(s) and the Name column.	display_columns
ExcludeSizeOver= <i>size</i>	Excludes places that exceed the size specified in MB (megabytes.)	exclude_by_size over=" <i>size</i> "
ExcludeSizeUnder= <i>size</i>	Excludes places smaller than the size specified in MB.	exclude_by_size under=" <i>size</i> "
IncludeAnonymous	Includes places users access anonymously.	include_anonymous enabled="false"
ExcludeAnonymous	Excludes places users access anonymously.	include_anonymous enabled="true"
LastAccessedMaxAge= <i>days</i>	Excludes places not accessed within the number of days specified.	last_accessed older_than=" <i>days</i> "
LastAccessedMinAge= <i>days</i>	Excludes places accessed more recently than the number of days specified.	last_accessed younger_than=" <i>days</i> "

continued

<i>URL Parameter</i>	<i>Description</i>	<i>qpconfig.xml setting it overrides</i>
LastModifiedMaxAge= <i>days</i>	Excludes places not modified within the number of days specified.	last_modified_older_than=" <i>days</i> "
LastModifiedMinAge= <i>days</i>	Excludes places modified more recently than the number of days specified.	last_modified_younger_than=" <i>days</i> "

Adding parameters to the My Places URL

To create and use a modified My Places URL:

1. Click My Places and append the desired parameters to the My Places URL. Precede each parameter with an ampersand (&).
2. Press Enter to apply the parameters to the My Places list.
3. (Optional) Bookmark the URL.

Note The next time you click My Places in the Table of Contents, My Places reverts to the settings configured on the server.

Examples of adding parameters to the My Places URL

Following are examples of using parameters in the My Places URL.

Display eight places, starting at the eleventh place (the first place is numbered "0").

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&Start=10&Count=8
```

Display the default number of places per page, sorted by name in descending order. This setting overrides a <sort order="ascending" /> setting on the server.

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&SortDescending
```

Display places that the user is a member of explicitly, but excludes those of which the user is a member through membership in "AdminGroup1" or "AdminGroup2".

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&ExcludeByMembers=cn=AdminGroup1,o=Acme; cn=AdminGroup2,o=Acme
```

Display only places 5MB (megabytes) or less in size. Since no ExcludeSizeUnder parameter is specified, the default minimum size of 0 is used.

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&ExcludeSizeOver=5
```

Display only places modified in the past 5 to 30 days. Exclude places created or modified within the past 4 days, and also places modified more than 30 days ago.

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&LastModifiedMaxAge=30&LastModifiedMinAge=5
```

Display only places modified in the past 30 days. Exclude places modified more than 30 days ago.

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&LastModifiedMaxAge=30
```

Display places of which the user is explicitly or implicitly a member, plus all places the user accesses anonymously.

```
http://serverName/QuickPlace/quickplace/Main.nsf/h_Toc/22049553D70E00EF85256BB60054A7CB/?OpenDocument&IncludeAnonymous
```

Chapter 8

Completing Other Server Configuration Tasks

This chapter describes the following Team Workplace server configuration tasks not covered in other chapters:

- Using the Server Settings room in the administration place
- Setting up the Search Places feature
- Customizing Web page caching
- Hiding the Sign In and Sign Out links
- Configuring browser caching
- Disabling page compression
- Displaying CGI variables in Team Workplace HTML source pages
- Customizing user notifications settings
- Specifying a footer that appears on all pages
- Enabling and disabling the UTF-8 Domino server setting
- Tracking the number of active Team Workplace users

Using the Server Settings room in the administration place

Use the Server Settings room in the administration place on a Team Workplace server to:

- Control whether members can use ActiveX controls and Java applets
- Control whether managers of places on a server can run agents (PlaceBots) within the places they manage
- Restrict the size of file attachments members can add to pages
- Enable or disable Sametime services
- Enable or disable a Domino Offline Passthru Server
- Enable or disable an Alternate Offline Download URL
- Specify an e-mail URL prefix if users access the Team Workplace server through a gateway server
- Control whether members can subscribe to receive e-mails integrated with their calendars

The following table describes the features available when ActiveX is enabled compared to when it is disabled.

<i>Feature</i>	<i>ActiveX enabled</i>	<i>ActiveX disabled</i>
Drag-and-drop file import/export operations	Yes	No
File import operations done through file attachment dialog box	Yes	Yes but limited to one file per publishing cycle
Rendering of imported Microsoft Office files (Word, Excel, PowerPoint)	Yes	No
Rendering of imported HTML, JPEG, and GIF files	Yes	Yes
Drag-and-drop file attachment operations	Yes	No
File attachment operations done through the attachment dialog box	Yes	Yes but limited to one attachment per publishing cycle
Remove attachments from a page	Yes	Yes
Save attachments to the client file system	Yes	Yes
When opening attachments, load the attachments within their applications	Yes	Yes
Do round-trip edits of imported files	Yes	No

For information on how to enable ActiveX controls, see the previous topic.

Setting up the Search Places feature

A manager of a place enables or disables advanced search within a place. Team Workplace has two types of advanced search features: classic search and Search Places. Classic search is based on Domino search site and allows users to search for information within specific rooms or folders in a place or to search an entire place. The Search Places feature is based on Domino Domain Search and allows users to search all places they are a member of. Unlike classic search, Search Places requires a Domain Catalog server (a 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 information on enabling advanced search for a place, see the Help.

Before you set up the Search Places feature, note the following:

- The Search Places feature respects all access permissions on content, and so users must retain a single identity to be able to search across places. To search across places, authenticated users must be registered in an external user directory. Local users can search only within a place.
- If room access is controlled by a local group, even if the user has access through the local group, Search Places won't be able to find the document from the room. Restrict room access using groups from an external user directory.
- If the Team Workplace service consists of more than two Team Workplace servers, including the Domain Catalog server, to use the Search Places feature you must configure multi-server session-based authentication (single-sign on).

For more information, see the chapter “Setting Up Security.”

- To remove places when the Search Places feature is used, use the QPTool remove command with the -cleanup argument rather than with the -now argument. The QPTool remove command with -cleanup argument runs nightly and removes places when place information in the search index is cleared.

For more information, see the chapter “Using QP Tool Commands.”

- If you use Search Places, using only Team Workplace servers in a domain is the recommended configuration. However if a domain does include Domino servers that do not run Team Workplace along with Team Workplace servers, set up one Domain Catalog server for the Team Workplace servers and one Domain Catalog server for the Domino servers that do not run Team Workplace. Use this configuration to keep the domain index for Team Workplace searches separate from the one used for Notes searches of the domain.

The following table describes the search_places settings.

<i>Setting</i>	<i>Description</i>
enabled	<p>When set to true (default):</p> <ul style="list-style-type: none"> Enables users to see and use the All Places advanced search option on the server. Allows users to use Search Places on the Domain Catalog server. <p>When set to false:</p> <ul style="list-style-type: none"> Hides the All Places advanced search option on the server. Returns an error when Search Places requests are made to the Domain Catalog server.
anonymous	<p>When set to true allows anonymous users to search across places.</p> <p>When set to false (default) returns an error when anonymous users issue Search Places requests to the Domain Catalog server.</p> <p>If you allow anonymous users to search across places, and the manager of a particular place does not want to expose the contents of the place to anonymous users through the Search Places feature, the manager should make sure that anonymous access to the place is disabled, and limit the place membership to specified users and groups in the directory.</p> <p>If you allow anonymous access, make sure that anonymous users have the same access as the -Default- access in the ACL for CATALOG.NSF on the Domain Catalog server.</p>
SSL*	When set to true defines that SSL generates the URL for the domain catalog server (HTTPS). When set to false (default) defines that HTTP generates the URL.
port*	Defines the port used in the URL for the Domain Catalog server.
path_prefix*	Defines a path prefix for the URL for the Domain Catalog server.
hostname*	Specifies the hostname of the Domain Catalog server.
domino_server_name*	Specifies the Domino server name of the Domain Catalog server for example, ServerCatalog/Acme. Before removing places from this server, the server does a lookup to the Domain Catalog server to verify if the search index is cleared.

*Use these settings on any Team Workplace server that is not the Domain Catalog server. Do not use them on the Domain Catalog server.

Customizing Web page caching

Web page caching greatly improves the response time of the Team Workplace server. Without a cached copy of a Web page, the HTTP server must access the database upon every HTTP request, which results in a slower response time for the Team Workplace server. If a Web page is cached on the Team Workplace server, the server only has to pick up the page from the database one time, and then create a user-specific, cached copy of the page at that time. Upon subsequent requests for the page, the server retrieves and provides the cached copy, as long as it is still valid. If the server is brought down, the existing cache is maintained after the server is brought back up.

Certain actions cause the cache for a page to become invalid. Once a cached page is invalid, the next time the page is accessed it is re-cached. Following are some examples of how the entire cache or specific pages within the cache can become invalid:

- A change to the Team Workplace Server Settings, for example a change to the default maximum attachment size allowed, invalidates all places on the server (the entire cache).
- If the Place Catalog is enabled, a change in the Place Catalog database invalidates the entire cache.
- A change in `qpconfig.xml` invalidates the entire cache.
- A change to place membership — a member is added, modified, or deleted — invalidates the cache for all databases associated with that place — `main.nsf` and all the inner rooms. A change to inner room membership invalidates the cache for that particular room and its child rooms.
- A change in rooms — a room is created or deleted — invalidates the cache for all databases associated with that place.
- A page published in the Main room (`main.nsf`) invalidates the cache for all databases associated with that place.
- A page published in a parent room invalidates the cache for the parent room and the child rooms below it.
- A page published in a child room invalidates the cache for the child room and for any rooms below it. The cache for the parent room pages remain valid.
- A customization to a parent room, for example a theme change or a custom form, invalidates the cache for the parent room and the child rooms below it.

Web page cache settings

Team Workplace administrators can use notes.ini settings to change the following preferences for the server cache:

- Enable or disable caching
- Set the cache directory
- Set the cache size limit
- Set the time interval for cache cleaning
- Set the cache for anonymous users only
- Enable or disable logging

To enable the cache

Set “QuickPlaceWebCacheEnabled=1” in the notes.ini file.

To disable server caching, set “QuickPlaceWebCacheEnabled=0”

The server cache is enabled by default.

To set the cache directory

Set “QuickPlaceWebCacheDir= <full path>” in the notes.ini file.

If this variable is not set in the notes.ini file, then it is automatically set to the default directory: (<NOTESPROGRAM>\data\domino\quickplace\cache).

If a specified directory path is invalid, the server cache is disabled.

To set the cache size limit

Set “QuickPlaceWebCacheLimitInMB = <size in MB>” in the notes.ini file.

If this variable is not set in the notes.ini file or if the size given is not a positive number, then the variable is automatically set to the default size of 50MB.

To set the time interval for cache cleaning

Add “QuickPlaceWebCacheGCIntervalInMIN= <time interval in minutes>” to the notes.ini file.

If this variable is not set in the notes.ini file, or if the value given is not a positive number, then it is automatically set to the default value of 60 minutes.

To set the cache for anonymous users only

Add “QuickPlaceWebCacheUsers= Anonymous” to the notes.ini file.

The default value for this setting allows server caching for all users when the cache is enabled. Changing this setting disables caching for all other users.

To enable logging for the server cache

Set QuickPlaceWebCacheLogging = < log level> in the notes.ini file.

The logging setting has three levels: 1, 2, or 3, where 1 is the least detailed and 3 is the most detailed. Logging is written to log.nsf.

Hiding the Sign In and Sign Out links

After a user signs in to a place, Team Workplace displays the Sign In and Sign Out links in the Team Workplace user interface by default. You can configure Team Workplace to hide the Sign In and Sign Out links after a user signs in. You might want to hide the links if single sign-on is enabled on the server, or if Team Workplace is running on a public pedestal, for example, at a trade show. To hide the Sign In and Sign Out links, specify the following settings in the qpconfig.xml file:

```
<server settings>
  <authentication>
    <sign_out enabled="false"/>
    <sign_in enabled="false"/>
  </authentication>
</server settings>
```

Configuring browser caching

To control Team Workplace caching on browsers, complete any of the following tasks:

- For additional security, configure the server to clear the Team Workplace files from the browser cache on sign-out (Internet Explorer only)
- For additional security, configure the server to prevent caching of Team Workplace pages on browsers
- To improve performance, configure the server to cache images on browsers (only in environments that do not use single sign-on authentication)

Clearing Team Workplace files from the Internet Explorer cache

As a security measure, configure the server to clear the Team Workplace files (files from any URL that contains “/quickplace/”) from the browser cache when users click the Sign Out link from a place. This feature is supported for Internet Explorer only.

To clear the browser cache when a user signs out, add the following setting to the qpconfig.xml file:

```
<server settings>
  <authentication>
    <sign_out enabled="true"/>
    <clear_browser_cache enabled="true"/>
  </authentication>
</server settings>
```

The browser cache is cleared only if the Sign Out link is enabled, ActiveX controls are enabled in Team Workplace, and ActiveX is enabled on the browser. Internet Explorer enables ActiveX by default.

The Sign Out link is never available to anonymous users, and to users who access places in accessibility mode on a server that is not enabled for single sign-on. The Sign Out link is unavailable to all users if you configure the server to hide the Sign Out link as described previously. If the Sign Out link is unavailable for any of these reasons, you can configure the server to prevent caching of Team Workplace pages on browsers as described in the next topic.

Preventing caching of Team Workplace pages on browsers

Team Workplace caches pages on the browser by default. As a security measure, add the following setting to the qpconfig.xml file to prevent Team Workplace from caching pages that contain data.

```
<server settings>
  <browser_caches_place_content enabled="false">
</browser_caches_place_content>
</server settings>
```

Any Team Workplace pages containing data that users access after you have added this setting are not cached. Pages that do not contain user data continue to be cached for better performance. This feature is available for all supported browsers.

Enabling image caching in environments that don't use single sign-on

A Team Workplace server stores images from places in the resources.nsf database and in the Team Workplace file system. You can set up a server to cache the images in resources.nsf on the browser when users first access a place. Then when users access additional places, the cached images are used, which load more quickly than images loaded from the server. Image caching is supported only in Team Workplace environments that do not use single sign-on authentication.

To enable the display of CGI variables, use the following setting in the qpconfig.xml file on the server:

```
<server_settings>
  <cgi_variables enabled="true"/>
</server_settings>
```

For more information on creating and specifying settings in the qpconfig.xml file, see the chapter “Team Workplace Administration Overview.”

Customizing user notifications settings

Use qpconfig.xml settings to configure a variety of settings related to Team Workplace user notifications. For example use qpconfig.xml settings to specify the text displayed in the password prompt of place invitations or to specify whether notifications sent to groups show the members of the groups.

Use notes.ini settings to configure where Team Workplace sends replies to e-mail sent from places.

Note You configure the underlying Team Workplace mail routing through Domino. For more information, see Domino Administrator Help.

Using qpconfig.xml settings to configure notifications

Use the following section in qpconfig.xml file to specify a variety of settings for user notifications. Copy the following from qpconfig_sample.xml to qpconfig.xml, and customize the settings to suit your needs.

For information on creating the qpconfig.xml, see the chapter “Team Workplace Administration Overview.”

```

<server_settings>
  <notifications>
    <place_invitation>
      <password_message>Your intranet
password.</password_message>
    </place_invitation>
    <calendar>
      <client_types>
        <notes5 enabled="true"/>
        <msoutlook enabled="true"/>
      </client_types>
    </calendar>
    <recipient_rules>
      <expand_external_groups enabled="true"/>
      <allow_ambiguous_sendto enabled="false"/>
    </recipient_rules>
  </notifications>
</server_settings>

```

The following table describes these settings.

<i>Setting</i>	<i>Description</i>
password_message	Specifies the password prompt that appears in external users' invitations to visit places
notes5 enabled	When set to true (default), enables Lotus Notes 5 support for calendar notifications. When set to false, disables this support.
msoutlook enabled	When set to true (default), enables Microsoft Outlook support for calendar notifications using icalendar standards specified in RFC 2445. When set to false, disables this support.
expand_external_groups enabled	When set to true (default), when mail is addressed to an external group, the place expands the group and lists each member's e-mail address in the notification. When set to false, the notifications do not expand the group members. Instead the mail router is given the group names to resolve.
allow_ambiguous_sendto enabled	When set to true, allows users to send notifications to ambiguous names from an external directory and have the mail router resolve the names. When set to false (default), users can send notifications only to valid e-mail addresses.

Configuring where Team Workplace routes replies to e-mail from places

By default if a user replies to one of the following types of e-mail notifications, Team Workplace routes the reply to a database called DeadMailQP.nsf on the Team Workplace server:

- Notification sent by a place automatically, such as a “What's New” notification.
- Notification sent from a place by a user who has no specified e-mail address.

By default Team Workplace also routes all delivery failure notifications to DeadMailQP.nsf.

To instead route these types of replies as well as delivery failure notifications to the default mail location of the places from which the e-mails come, delete the following setting from the notes.ini file on the server:

```
h_UndelivMail
```

Or, to send these types of replies as well as delivery failure notifications to the default mail location of one specified place, modify these notes.ini settings:

```
h_UndelivMail=placename
```

```
$h_MailDomain=domainname
```

where *placename* is the name of the place to route the mail, and *domainname* is the fully qualified domain name of the server that hosts the place.

For example, specify:

```
replyplace@qpserver.acme.com
```

Specifying a footer that appears on all pages

You can specify an HTML footer of up to 255 characters in the server_messages section of qpconfig.xml to display HTML on the bottom of all pages on the Team Workplace server. For example you might specify a corporate logo, administrative message, or corporate disclaimer.

For more information on creating and specifying settings in the qpconfig.xml file, see the chapter “Team Workplace Administration Overview.”

For example, to display Acme Corporation in bold text in page footers, specify the following:

```
<server_settings>
  <server_messages>
    <footer>
      <![CDATA[<b>Acme Corporation</b>]]>
    </footer>
  </server_messages>
</server_settings>
```

To insert an image in the footer, put the image file in the data\domino\html directory and reference it in the footer setting as ``. Or put the image file in the data\domino\icons directory and reference it as ``.

For example, put the image file logo.gif in the data\domino\html directory and specify the following in qconfig.xml:

```
<server_settings>
  <server_messages>
    <footer>
      <![CDATA[]]>
    </footer>
  </server_messages>
</server_settings>
```

Enabling and disabling the UTF-8 Domino server setting

UTF-8 is an encoding format for Unicode. The Domino server document has a setting, "Use UTF-8 for Output," which changes the default character encoding of the Domino HTTP server to UTF-8. If the Team Workplace server is running with the GB-18030 code page, then this server setting must be set to Yes.

If the UTF-8 setting is not configured appropriately, your Domino server administrator must change the setting in Domino. For more information on changing the UTF-8 setting in Domino, see Domino Administrator Help.

Tracking the number of active Team Workplace users

To track the number of active users of a Team Workplace server, you use standard Domino Web server logging to log user access information to text files. Then you can use available tools to extract the names of each unique user. To retrieve the total number of active users in the Team Workplace service, you must set up each Team Workplace server in the service to generate log files.

When you set up the HTTP task to log user access information to text files, the HTTP task creates one log file a day that contains information about each user session with the Team Workplace server. The default name format for the log files is `access<date>.log`, where `<date>` is the date the log file is created in the format `MMDDYYYY`.

To set up logging of user access

To set up the HTTP task on a Team Workplace server to log user access information to text files, do the following:

1. Open the Server document for the Team Workplace server in the Domino Directory in edit mode.
2. Click the Internet Protocols - HTTP tab.
3. In the Log files field, selected Enabled.
4. In the "Directory for log files" field, specify an existing directory path for the log files. The HTTP task creates log files only if the specified directory path exists.
5. In the Access log field, specify the prefix for the log files. The default prefix is: `access`.
6. Click Save and Close.

For more information on Web server logging and other log settings in the Server document, see Domino Administrator Help.

To extract the names of Team Workplace users from log files on UNIX systems

There are many tools available to extract the names of users from the log files and to exclude irrelevant information. One of the simpler methods available is using native operating system commands. Following are some examples of using the `tr`, `grep`, and `sort` commands on a UNIX system to extract user names from log files.

Example of extracting names from one log file

The following commands translate the contents of the file, access03252002.log, to uppercase letters, extract only the lines that contain the character string “CN=”, eliminate any duplicate names, and write the resulting list to the file, uniquename.log.

```
tr “[:lower:]” “[:upper:]” < access03252002.log | grep “CN=” | sort -u
-k 3,3 > uniquename.log
```

Example of extracting names from multiple log files

The following commands process two log files, access03252002.log and access03262002.log, to produce the unique user list.

```
tr “[:lower:]” “[:upper:]” < access03252002.log | grep “CN=” | sort -u
-k 3,3 >> tempname.log
tr “[:lower:]” “[:upper:]” < access03262002.log | grep “CN=” | sort -u
-k 3,3 >> tempname.log
sort -u -k 3,3 < tempname.log > uniquename.log
```

The following Korn shell commands process all the log files generated by one server in the month of May to produce the unique user list.

```
for %f in (access05*.log) do tr “[:lower:]” “[:upper:]” < %f | grep “CN=”
| sort -u -k 3,3 >> tempname.log
for f in `ls -1 access05*log`
do
tr “[:lower:]” “[:upper:]” < %f | grep “CN=” | sort -u -k 3,3 >>
tempname.log
done
sort -u -k 3,3 tempname.log > uniquename.log
```

Example of extracting names from log files on multiple servers

To extract a list of active user names of a Team Workplace service that consists of multiple servers, you run the commands described in the examples above on each server, putting the output into a single network file that all servers can access. You then use that network file to generate the final output.

For example, if the Team Workplace service consists of two Team Workplace servers, X and Y, and the network file is n:\log\tempname.log, run Korn shell commands such as the following ones on each server:

On server Y run:

```
for %f in (access*.log) do tr "[:lower:]" "[:upper:]" < %f | grep "CN=" |  
sort -u -k 3,3 >> Y_tempname.log  
tr "[:lower:]" "[:upper:]" < %f | grep "CN=" | sort -u -k 3,3 >>  
Y_tempname.log  
sort -u -k 3,3 Y_tempname.log > n:\log\tempname.log
```

Then use the following command to sort and generate the final list of names:

```
sort -u -k 3,3 n:\log\tempname.log > uniquename.log
```

Chapter 9

Using QPTool Commands

This chapter describes how to complete various Team Workplace administration tasks using QPTool commands.

QPTool

QPTool is a server task that you run with arguments to do administrative tasks. You can use the QPTool command to complete the following tasks:

- Add external members to places
- Change user and group names in places
- Change the hierarchy of names in places
- Update external member information in places
- Manage expanded membership
- Reset local user passwords
- Remove members from places
- Send newsletters to subscribers
- Send mail to managers and members of places
- Register and unregister places and servers
- Automate replica stub creation
- Upgrade places and PlaceTypes
For information on upgrading places and PlaceTypes, see the *Team Workplace Installation and Upgrade Guide*.
- Refresh places and PlaceTypes
- Lock and unlock places
- Archive places
- Remove places or PlaceTypes
- Update statistics in the Place Catalog
- Generate reports about places and servers
- Repair places
- Clean up dead mail
- Execute an XML API file

Using QPTool commands in a cluster

When you run a QPTool command on a server in a cluster, Team Workplace applies the command only to the server on which you run it. The results of the command then replicate to the other servers in the cluster. For example, if you lock a place on one server in a cluster, the place is locked immediately only on that server. The place is locked on the other servers after replication replicates the lock property on the place's databases to the other servers.

The QPTool report command can gather information from all servers in a cluster. However, if the results of the report command are supplied as input to another qptool command, the other qptool command only acts immediately on the places on the server from which you issue the command.

Adding external members to places

You can use the QPTool addmember command to add a name from a user directory as a member of a place or places. When you use the addmember command rather than the Team Workplace user interface, you can add a member to multiple places at once. When you use the addmember command, you must use the -reader, -author, or -manager argument to specify the access the member has to the place's main room. Optionally, you can use the -allrooms argument to apply the member's main room access to all subrooms.

If you use the Team Workplace user interface to change an existing external member's access to the main room in a place, subrooms do not inherit the access change. To change an existing member's access to all rooms in a place, you can use the QPTool removemember command to delete the member from the place, and then use QPTool addmember with the -allrooms argument to add the member again with the new access.

Note You can't use the addmember command to add local members. You can't use addmember to add external members to the QuickPlace/quickplace.

The syntax for the addmember command is:

```
load qptool addmember arguments
```

The following table describes the supported arguments.

<i>Argument</i>	<i>Description</i>
-?	Prints help on the command.
-dn <i>name</i>	Specifies the name of an external user or group to add as a member. If the name contains at least one space, include quotation marks (" ") around it. Specify the name exactly as it is defined in the directory (including spaces), for example: "cn=Connor Jones,ou=Sales,o=Acme" Note Team Workplace does not look up the name in the user directory to verify the name you specify. Be sure the name you specify is valid.
-g	Indicates that a name specified for the -dn argument is the name of a group. You must use this argument to add an external group. If you use qptool addmember without the -g argument to add an external group as a member of a place, users who are members of the group can't access the place through the group membership, and the group may not show up in the user interface in some places.
-reader	Adds the specified name as a Reader of a place.
-author	Adds the specified name as an Author of a place.
-manager	Adds the specified name as a Manager of a place.
-allrooms	Applies the place access specified for the name to all rooms in a place. If you omit this argument, the name's specified access applies only to a place's main room.
-a	Adds the specified name as a member of all places on the server.
-p <i>place(s)</i>	Adds the specified name as a member of a specific place or space-separated list of places.
-i <i>inputfilename</i>	XML input file located in the server program directory that specifies the places in which to add an external member.
-o <i>outputfilename</i>	XML output file that logs the results of the command. By default the command logs results to qptool.addmember.xml in the server program directory.

The following table provides examples of the qptool addmember command.

<i>Task</i>	<i>Command</i>
Add the user cn=Connor Jones,ou=Sales,o=Acme as an Author of all rooms in Place1	load qptool addmember -dn "cn=Connor Jones,ou=Sales,o=Acme" -author -allrooms -p Place1
Add the group cn=Salesgroup,o=Acme as a Reader of the main room in all places	load qptool addmember -dn cn=Salesgroup,o=Acme -g -reader -a

Changing user and group names in places

Use the QPTool changemember command to change the name of a local user, external user, or external group in specified places. The original name is known as the source name and the name you change to is known as the target name.

Using changemember, you can do the following tasks:

- Change a user or group name to a new name — for example, change the name of a user who recently married so the user can continue to access a place using the new name. In this case, the target name is a new name.
- Change the name of a user or group to the name of another existing user or group — for example, change the name of a user who leaves the company to the name of a remaining user who assumes the original user's responsibilities. The access the target name has to places is the higher level of access between the source and target names. For example, if the source name is a manager of a place and the target name is a reader of the place, the target name becomes a manager of the place and has access to all pages previously accessible to the source and target names. The same access control principle applies to room access.
- Change the name of a local user to the name of an external user in a user directory — for example, to move from a pilot deployment that uses local users to a production deployment that uses a corporate directory.

You can make these combinations of name changes:

- Local user name to local user name
- Local user name to external user name
- External user name to external user name
- External group name to external group name

Note If an external user is not listed explicitly as a member of a place, but instead accesses the place through membership in an external group, the user's name is not listed as a member in the place's Contacts1.nsf database, but is included in security fields within the place. For example, if the user creates a page, the user's name is listed in the page's h_Authors field. If you use the changemember command to change the user's name in a place, the name is changed in these security fields and the user's access to the place continues.

You cannot make these combinations of name changes:

- External user name to local user name
- External group name to local user name
- External group name to external user name
- Local user name to external group name
- External user name to external group name

Note You can use the changemember command on a pre-6.5.1 place only if you have first used the qptool upgrade command to upgrade the place.

The syntax for the changemember command is:

```
load qptool changemember arguments
```

The following table describes the arguments. When a name specified as an argument contains spaces, include quotation marks (") around the name.

<i>Argument</i>	<i>Description</i>
-?	Prints help on the command.
-sourcedn <i>name</i>	Specifies the original distinguished name of an external user or external group exactly as the name is defined in the external directory, for example, "cn=Connor Jones, ou=Sales,o=Acme." Include any spaces in the name. Specify the letter case (uppercase or lowercase) correctly.
-sourceu <i>name</i>	Specifies the original name of a local user, for example, "Joe Smith."
-sourceg	Indicates that the specified source name is that of an external group.

continued

