

TypingMaster Intra

LDAP / Active Directory Installation



Technical White Paper (2009-9)

CONTENTS

Contents	2
TypingMaster Intra LDAP / Active Directory White Paper	3
Background INFORMATION.....	3
Overall process.....	3
STEP 1 – INSTALLING TOMCAT 6.0 APPLICATION SERVER	3
STEP 2 - TYPINGMASTER INTRA WEB APPLICATION Installation.....	4
STEP 3- CONFIGURE TypingMaster Intra	4
STEP 4- CONFIGURE LDAP SUPPORT	5
Editing TOMCAT Server.xml file	5
Editing web.xml (OPTIONAL)	6
CREATING ACTIVE DIRECTORY DOMAIN USERS AND GROUPS.....	7
CONFIGURING TYPINGMASTER INTRA FOR LDAP.....	8
Restarting TOMCAT	8
Login to TYPINGMASTER with LDAP	9
TABLE 1 - LOGIN Trouble shooting.....	9
ADVANCED TROUBLESHOOTING FOR LDAP-ISSUES.....	10
OPEN LDAP Example (server.xml)	11

BACKGROUND INFORMATION

With Tomcat you can configure TypingMaster Intra to authenticate with Microsoft Active Directory via LDAP so you don't need to manage separate accounts in TypingMaster. There are two things that you'll get from Active Directory; authentication (is a username/password correct), and authorization (do they belong to a proper group).

This current LDAP implementation does not retrieve full user name from LDAP directory. If teacher wants the full user name (First name + Last name) to be shown in reports, administrator can configure TypingMaster to ask these details from the students during first login. Alternatively user account names can be used in TypingMaster reports.

This article describes step-by-step instructions to complete the LDAP capable TypingMaster Intra installation for enterprise level users. For small or mid-size schools it is usually a better choice to use integrated TypingMaster user accounts.

OVERALL PROCESS

To enable LDAP support, TypingMaster Intra needs to be installed into a separate TomCat Application Server and a few adjustments need to be done both to TomCat configuration files and TypingMaster Intra Configuration files.

For this reason some advanced technical skills are required to enable LDAP support.

STEP 1 – INSTALLING TOMCAT 6.0 APPLICATION SERVER

It is highly recommended to install a dedicated Tomcat 6.0 instance for TypingMaster Intra application.

1. Make sure you have Java 6 (Standard Edition) JRE or newer installed on your server
2. Download Tomcat version 6.0 from tomcat.apache.org
3. Choose Windows Service Installation if you are installing into Windows Server
4. Complete Typical Setup
5. Choose port 8080 and define (temporary) tomcat admin login details (e.g. admin, admin)

STEP 2 - TYPINGMASTER INTRA WEB APPLICATION INSTALLATION

1. Download TypingMaster Intra Web Application from: <http://download.typingmaster.com/java/tmintra.war> and store it e.g. to folder C:\temp\tmintra.war or similar
2. Install TypingMaster Intra Web Application to Tomcat 6:
 - Now when Tomcat is running, just open this web page from server console:
<http://localhost:8080/manager/html>
(Login with your Tomcat administrator user that was created during setup: admin, admin)
 - Scroll down to **Choose WAR file to deploy** section and choose a file **tmintra.war** (e.g. from C:\temp\tmintra.war)
 - Click DEPLOY button
 - TypingMaster (“tmintra”) appears on Application list now.

STEP 3- CONFIGURE TYPINGMASTER INTRA

- Go to this web address:
- <http://localhost:8080/tmintra>
- Decide if you would like to use external database e.g. Microsoft SQL Server. The default integrated SQL server is enough for 5.000 students but it is more complicated to backup than external server. **More information available in TypingMaster Intra Technology White Paper PDF file.**
- Create the primary administrator account for TypingMaster Intra. For easier access with LDAP, this account name should match your personal LDAP user name. You can also create multiple administrator accounts when you first login. Next choose default languages and define a valid SMTP mail server.
- After completing these 4 simple configuration pages TypingMaster Intra is up and running. Next step is to alter a few configuration files to enable LDAP.

STEP 4- CONFIGURE LDAP SUPPORT

The following **Server.XML** configuration file is mainly for Windows 2000/2003 Domain. You may need to contact your corporate LDAP administrator for additional details if your company is using another LDAP server environment.

EDITING TOMCAT SERVER.XML FILE

Please edit **server.xml** file with notepad text editor or similar from server console:

```
C:\Program Files\Apache Software Foundation\Tomcat 6\conf\server.xml
```

Update the server.xml file by adding there a new Realm block with your LDAP connection details like this:

```
<Realm className="org.apache.catalina.realm.JNDIRealm" debug="99"
connectionName="ldapuser" ← put here user name that can access ActiveDirectory
connectionPassword="xx" ← put here password for name that can access ActiveDirectory
connectionURL="ldap://ntserver:389" ← put here server name for Domain/ActiveDirectory
alternateURL="ldap://ntserver2:389" ← put here 2. server name for Domain/ActiveDirectory
userBase="dc=server,dc=typingmaster,dc=com" ← put here ActiveDirectory name in dc format
userSearch="(sAMAccountName={0})"
userSubtree="true"
roleBase="dc=server,dc=typingmaster,dc=com" ← put here ActiveDirectory name in dc format
roleName="cn"
roleSearch="(member={0})"
roleSubtree="true"
referrals="follow"
/>
```

Important: Please remember to comment out the original default REALM block like this:

```
<!-- <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
resourceName="UserDatabase"/> --!>
```

Tip: You can download the sample **server.xml** file (for Tomcat 6.0) from this link:

<http://download.TypingMaster.com/misc/tmintra-ldap-samples.zip>

EDITING WEB.XML (OPTIONAL)

Next step is editing application specific **web.xml** file with notepad text editor or similar from server console:

```
C:\Program Files\Apache Software Foundation\Tomcat 6\webapps\tmintra\WEB-INF\web.xml
```

The **web.xml** file already contains the following xml block in the end of file. You may want to edit a little or you can keep the existing default settings. Here you define the AD group (LDAP Role) where students belong to.

```
<auth-constraint>

  <!-- Roles that have access -->

  <role-name>typingmaster</role-name>          ← put here ActiveDirectory group name

</auth-constraint>

<login-config>

<auth-method>BASIC</auth-method>

<realm-name>Domain login</realm-name>         ← put here optional message shown during login

</login-config>

<security-role>

  <description>Domain login</description>

  <role-name>typingmaster</role-name>         ← put here ActiveDirectory group name

</security-role>
```

Domain User for LDAP communication

The sample Server.XML file above requires that you create one AD user called **ldapuser** (with sample password xxx) that simply has the access rights to browser the LDAP directory. This user does not require any other access rights to your network. Use **Administrative Tools / ActiveDirectory Users** from Windows Server 2003 Console to create this new user.

Group for TypingMaster Users

Create a new group to your LDAP directory with **Administrative Tools / ActiveDirectory Users**, by default this group is called **typingmaster**. You can change the group name if necessary. All ActiveDirectory users placed inside this group will have the access to TypingMaster Intra application. All other users will receive 403 Access Denied message.

Giving Access to whole *Domain Users* Group

Domain users group is the primary group for all users in AD. Unfortunately this membership is not visible to Tomcat via LDAP "memberOf" attribute. However, there is an easy workaround available as attribute "513" specifies the "domain users" in the LDAP server catalog. If you want to give access to all "Domain Users" without assigning them to any specific TypingMaster group first, please complete these additional steps:

Two additional steps are needed:

1. edit tomcat **server.xml** and replace the whole "roleSearch="(member={0})" row with this new row:

```
userRoleName="PrimaryGroupID"
```

2. Edit **web.xml** and replace two lines (typingmaster role-name entries) like this:

```
< role-name >513< /role-name >
```

AD Group for Tomcat Manager (optional)

When you enabled LDAP login to Tomcat, you cannot any more easily access Tomcat Manager tool running at <http://localhost:8080/manager/html> with the default admin, admin account created during setup.

If you like to allow logging to Tomcat Manager you need to specify Manager group to your AD. First step is to create a new group to your LDAP directory with **Administrative Tools / ActiveDirectory Users**, this group must be called **manager**. You can change the group name if necessary. All ActiveDirectory users placed inside this group will have the access to Tomcat Manager application where they can e.g. Stop and Restart TypingMaster Intra or add other apps.

CONFIGURING TYPINGMASTER INTRA FOR LDAP

By default LDAP in TypingMaster Intra is configured to allow normal logins (non-ldap logins). The program does not by default ask user details on the first login. If you wish to change these settings, edit the following file with notepad text editor or similar:

```
C:\Program Files\Apache Software Foundation\Tomcat 6\webapps\tmlntra\appdata\lms_settings.def
```

To ask user name and group information upon first login, set the line

```
ldap_askuserdetails=0  
to  
ldap_askuserdetails=1
```

If you wish for all users to log in through ldap change the line

```
ldap_only=0  
to  
ldap_only=1
```

When this setting is set all users will be directed to the ldap login automatically from the normal login page

NOTE: Before making this change make sure that you set or changed the TypingMaster Intra administrator's login id to match your Windows log in name. Alternatively, you can change the users you wish to be Administrators from the Users tab.

RESTARTING TOMCAT

Restart Tomcat with these commands from command prompt or use Tomcat SysTray icon to do it:

- net stop tomcat5
- net start tomcat5

LOGIN TO TYPINGMASTER WITH LDAP

Congratulations, all configuration tasks are now done and TypingMaster Intra should now support LDAP login.

- Now go to <http://localhost:8080/tmintra/ldaplogin>

Web browser will ask now for your Active Directory user name + password.

If you are not member of chosen group (role-name) you will get access denied message.

NOTE: If you have enabled the *ldap_only* setting, the following shorter URL will also work:

<http://localhost:8080/tmintra/>

TABLE 1 - LOGIN TROUBLE SHOOTING

Test 1: Login Dialog go to http://localhost:8080/tmintra/ldaplogin	Does your web browser ask for the user name with a dialog box?	No: Check the last row of "STDOUT.LOG" file for error messages, the file is located in the Tomcat/Logs folder. Correct the web.xml and server.xml files according to the error message. Yes: Go to Test 2
Test 2: Enter user name	What error you get when you enter a domain user name that belongs to group "typingmaster"	401: User name not found 403(Access denied): The entered user is not member of defined AD group "typingmaster"
If problem continues..		If you still cannot login, please see the TROUBLESHOOTING LDAP-ISSUES section on next page.

ADVANCED TROUBLESHOOTING FOR LDAP-ISSUES

If authentication does not work, please see the latest log entries from Tomcat/Logs folder (file name is **Catalina_log.timestamp.log**) and compare the error messages to sample ones below:

[LDAP: error code 49 - 80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 525, v893]

server.xml issue: you must define valid username with connectionName="" and connectionPassword="" parameters to get access to the LDAP Server/Windows Domain.

JNDIRealm[Catalina]: Connecting to URL ldap://tmserver1:389

Just a time-out may occur if the connectionPassword is wrong and no error is shown in log file. Remember to restart TomCat after you change the correct password to server.xml.

[LDAP: error code 1 - 00000000: LdapErr: DSID-0C090627, comment: In order to perform this operation a successful bind must be completed on the connection

server.xml issue: you must define valid username with connectionName="" and connectionPassword="" parameters to get access to the LDAP Server/Windows Domain.

[LDAP: error code 10 - 0000202B: RefErr: DSID-031006E0

server.xml issue: Please define all 3 dc values, such as userBase="dc=myserver,dc=typingmaster,dc=com"

JNDIRealm[Catalina]: base: dc=server,dc=typingmaster,dc=com filter: (sAMAccountName=test)

JNDIRealm[Catalina]: username not found

The entered user name ("test") was not found at all from LDAP directory.

JNDIRealm[Catalina]: Username XX successfully authenticated

JNDIRealm[Catalina]: getRoles(CN=x y,CN=Users,dc=server,dc=typingmaster,dc=com)

JNDIRealm[Catalina]: Searching role base 'dc=server,dc=typingmaster,dc=com' for attribute 'cn'

JNDIRealm[Catalina]: With filter expression 'member=CN=X Y,CN=Users,dc=server,dc=typingmaster,dc=com'

JNDIRealm[Catalina]: Returning 0 roles

The matching role cannot be found. Tomcat version may be too old to authenticate to LDAP properly.

Tips:

You can use e.g. JXplorer tool to browse and debug your LDAP configuration.

OPEN LDAP EXAMPLE (SERVER.XML)

Here is the advanced configuration example for Open LDAP.

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
  debug="99"
  connectionName="cn=Manager,dc=mycompany,dc=com"
  connectionPassword="secret"
  connectionURL="ldap://localhost:389"
  roleBase="ou=roles,dc=mycompany,dc=com"
  roleName="cn"
  roleSearch="(uniqueMember={0})"
  roleSubtree="false"
  userSearch="(uid={0})"
  userPassword="userPassword"
  userPattern="uid={0},ou=people,dc=mycompany,dc=com"
/>
```