

# WebMessenger®

## Mobile IM Server Administrator Guide



**callwave®**

[www.callwave.com](http://www.callwave.com)

[www.fuzemeeting.com](http://www.fuzemeeting.com)

Customer Care **1.800.844.4118** | [care-fuze@callwave.com](mailto:care-fuze@callwave.com)

Sales **1.866.470.1901** | [sales@callwave.com](mailto:sales@callwave.com)

### 3<sup>rd</sup> Party Software Notices

The WM Server includes the following open source third-party software:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>);
- Cryptographic software written by Eric Young (<eay@cryptsoft.com>)
- Software written by Tim Hudson (<tjh@cryptsoft.com>)
- OpenLDAP Library, licensed under The OpenLDAP Public License, Version 2.8. OpenLDAP is a registered trademark of the OpenLDAP Foundation
- Novel SDK (OpenLDAP implementation for Windows® with Novell Extensions), licensed under the Novell Developer License Agreement
- Apache Xerces XML Library: This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>), licensed under The Apache Software License, Version 1.1
- ACE™ Multiplatform Networking Library. ACE™ is copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright © 1993-2005, all rights reserved
- Oscar ICQ /AIM Protocol Implementation, licensed under the GNU Lesser General Public License, Version 2.1
- reSIProcate SIP Protocol Implementation. Copyright © 2000 Vovida Networks, Inc. All rights reserved.
- Expat Streaming Oriented XML Parser. Copyright © 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper. Copyright © 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.
- BOOST C++ Libraries, licensed under Boost Software License, Version 1.0
- PostgreSQL Database Access Client Library. Portions Copyright © 1996-2006, PostgreSQL Global Development Group Portions Copyright © 1994-1996 Regents of the University of California Full text of the 3rd party license agreements is placed in folder \Program Files\WebMessenger\WMP Server\Documents\copyright, created during the WM server installation.

Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of WebMessenger, Inc. WebMessenger may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from WebMessenger, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. WebMessenger and WebMessenger Mobile are registered trademarks of WebMessenger, Inc. All other trademarks are property of their respective owners.

Note that WM and WMP (WebMessenger Mobile Platform) may be used interchangeably throughout this document and within the User Interface.

© 2008 CallWave, Inc. All rights reserved.  
CallWave, FUZE and the FUZE logo are service marks of CallWave, Inc.  
All other trademarks or registered trademarks mentioned herein

# CONTENTS

<b>INTRODUCTION .....</b>	<b>4</b>
<b>SYSTEM REQUIREMENTS .....</b>	<b>5</b>
Hardware Configuration - Minimum.....	5
Hardware Configuration - Recommended.....	5
Software Requirements.....	5
Firewall Settings .....	5
Network Requirements for the Server Machine .....	5
<b>QUICK SETUP .....</b>	<b>7</b>
WM Mobile IM Server: Pre-Installation.....	7
WM Mobile IM Server: Installation.....	7
Install the WM Server .....	7
Uninstall the WM Server.....	10
WM Mobile IM Server: Post-Installation .....	10
Create New Users .....	10
Log In to Your Client.....	12
<b>ACTIVE DIRECTORY AUTHENTICATION.....</b>	<b>14</b>
Overview .....	14
Import Active Directory Users.....	15
Restart Services .....	17
Schedule User Updates.....	17
Reports.....	19
Configuration Files.....	20
Sections.....	22
<b>ADVANCED SETUP.....</b>	<b>24</b>
Microsoft SQL Server Installation.....	24
WM Server Manager .....	24
WM Server Event Log .....	25
Event Types.....	25
Event Definitions.....	25
WM Performance Counters.....	26
Gateways .....	28
Proxy Configuration .....	28
Work with TLS Protocol .....	28
Setup Auditors .....	28
AIM and ICQ Gateways Configuration .....	29
MSN Gateway Configuration .....	29
Yahoo! Gateway Configuration.....	29
Google Gateway Configuration .....	30
Jabber Gateway Configuration .....	30
MS OCS Gateway Configuration.....	30
MS LCS Gateway Configuration.....	31
Reuters Messaging Gateway Configuration .....	31
IBM Lotus Sametime Gateway Configuration.....	31
Verify Enterprise Gateway Configuration .....	32
IBM Lotus Sametime Interoperability.....	32
MS OCS 2007 Interoperability.....	32
MS LCS Interoperability.....	32
Reuters Messaging Server Interoperability .....	32
Active Directory .....	33
Section "Service Info" .....	33
Section "ADMAUTH".....	33
Section "LDAP".....	33
SSL Dispatcher Configuration.....	34
SSLDISPATCHER.INI .....	34
Internal Communication Ports.....	34
<b>WEB ADMINISTRATION .....</b>	<b>35</b>
Overview .....	35
Login.....	35
User Management.....	35
Add User.....	36
Edit User .....	37
View Buddy List .....	37
View Watcher.....	38
Property Management.....	39
Domain Management.....	39
<b>INDEX .....</b>	<b>40</b>

## INTRODUCTION

The WebMessenger Mobile (WM) Server enables information exchange across multiple networks and devices. It supports BlackBerry handhelds, Windows Mobile (PocketPC 2003, Windows Mobile 5.0 & 6.0 PPC/Smartphone), Symbian (S60 3rd edition), Palm handhelds, J2ME-based devices, and other wireless devices.

The WM Server can be deployed in very complex configurations, on multi-machine clusters and on several different operating systems. This setup guide is intentionally simplified in order to streamline the installation and the access to the available functionality on Windows Server OS.

**Estimated total WM Server installation time: two hours.**

---

**Note** *Please read this entire guide before starting the installation.*

## SYSTEM REQUIREMENTS

### Hardware Configuration - Minimum

*This configuration should be used for evaluation installations only.*

- 1 GHz Pentium III CPU/512 MB RAM
- 5 GB available HDD space
- 10 Mbps Network Adapter

### Hardware Configuration - Recommended

This configuration is suitable for enterprise customers with several thousand mobile users. For larger enterprise installations, please refer to our multi-machine/cluster deployment documentation.

- 2 GHz Pentium 4 CPU/2 GB RAM
- 60 GB available HDD space
- 100 Mbps Network Adapter

### Software Requirements

Before starting the installation, please make sure you have the following software available:

- WM Server software
- Windows Server 2003 (service pack 2 or later)
- For production installations: MS SQL Server (2000 or later) or Oracle (v8.0 or later) with latest service packs
- "Server" service must be enabled and running in order to install MSDE2000 - refer to the following MSDN KB article: <http://support.microsoft.com/kb/829386>

### Firewall Settings

Port 9000 is the default for client/server communication. This port can be changed in the **Dispatcher.ini** file. A port change requires a restart of the WM server and a change in the **Server Settings** on the client. It is necessary to open this port for inbound traffic if clients will connect from outside your corporate firewall.

The WM Server initiates outbound, bidirectional connections to third-party messenger servers (OCS, LCS, Sametime, Reuters, Jabber, etc.). The WM Server should have direct outbound connectivity (or through a transparent proxy) to third-party messaging servers.

GATEWAY	REQUIRED HOSTS/PORTS
<b>AOL</b>	login.oscar.aol.com 5190
<b>MSN</b>	messenger.hotmail.com 1863 nexus.passport.com 443
<b>Yahoo!</b>	scs.msg.yahoo.com 5050
<b>ICQ</b>	login.icq.com 5190
<b>Google Talk</b>	talk.google.com 443
<b>Jabber</b>	jabber.org 5222 jabber.com 5222
<b>Reuters Messaging</b>	sip.reuters.net 443 (transport: TLS/NTLM)

### Network Requirements for the Server Machine

Before starting the installation, please make sure you have the following network resources available:

- Static IP address
- Forward resolving, fully qualified DNS name

**Note**

If you do not have a fully qualified DNS name for your server, you can still access it by its IP address. If the WM server is accessed by IP address, the fully qualified DNS name in local "hosts" file should be set to that IP address (the "hosts" file is in the Windows installation folder; look for C:\WINNT\system32\drivers\etc\hosts or similar path).

**Setting the IP Address**

1. Forward resolving can be provided either by forward DNS server zone or by manual entry in the local hosts file (%SystemRoot%\system32\drivers\etc\hosts).

```
# Sample content of "hosts" file
# The second entry is the one you should enter manually
127.0.0.1      Localhost
10.0.0.3      machine.domain.com
```

Replace:

**10.0.0.3** with the server IP address

**machine** with the server machine name

**domain** with the domain that the server machine belongs to

2. Execute the command below on the server machine to check your DNS settings. It should return the IP of the server machine: **nslookup machine.domain.com**.

```
nslookup machine.domain.com
```

## QUICK SETUP

The WM Mobile IM Server Quick Setup has three parts:

- [Pre-Installation](#)
- [Installation](#)
- [Post-Installation](#)

### WM Mobile IM Server: Pre-Installation

1. Install Windows Server 2000 (or 2003) on a clean machine.
2. Apply the latest available Service Pack for the installed operating system.
3. Make sure the [network requirements for the server machine](#) have been satisfied.
4. If necessary, contact your network administrator for help. WM Server installations are also supported on VMWare and Virtual PC.

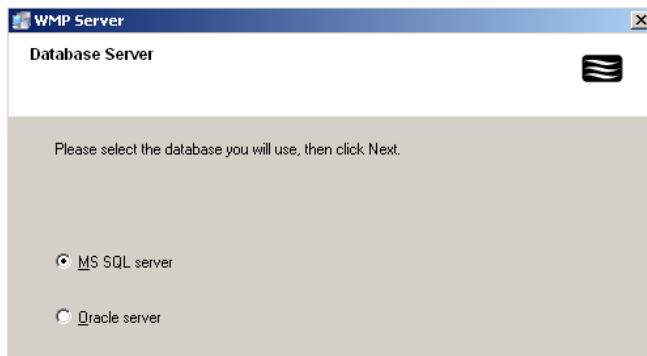
**Note** This server build can also run on Windows XP Professional Edition with the latest Service Pack. However, WebMessenger does not support this installation.

### WM Mobile IM Server: Installation

Start the WM server installation and follow the online instructions.

#### Install the WM Server

##### 1 Login and Select RDBMS



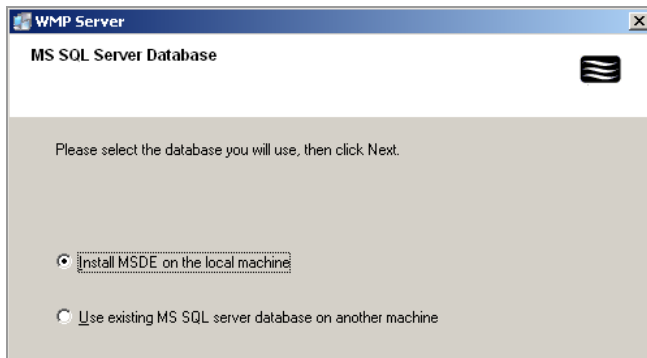
Log in to the server machine using an account with administrator privileges.

Start the WM Server installation.

Select the RDBMS you would like to use for this installation (**MS SQL server** or **Oracle server**).

**Note** When installing with Oracle server please contact WebMessenger Support for assistance.

##### 2 Choose Server DB Engine



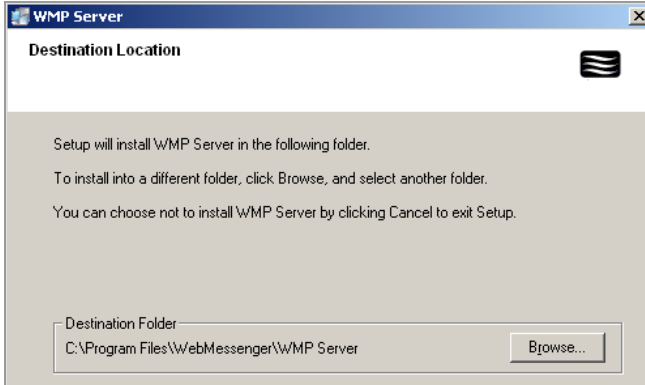
If you chose **MS SQL server** in the previous screen, you can install the MSDE engine on your machine (included in the WM server build for evaluation installations) or use an existing MS SQL Server on another machine.

If you choose **Install MSDE on the local machine** you will be prompted to reboot the machine after the MSDE installation and tuning are completed.

*You can decline the reboot and continue with the WM server installation and reboot afterwards.*

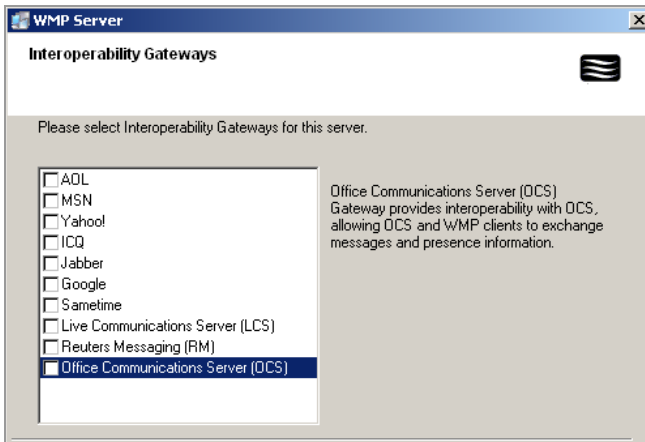
**Note** For production installations other than MSDE it is recommended to use Microsoft SQL Server 2000 or 2005 for better performance and reliability. If you decide to install MS SQL Server instead of MSDE, see [Advanced Setup](#).

### 3 Choose Destination Location



Either accept the default or browse to the desired location.

### 4 Choose Interoperability Gateway(s)



Select gateway(s) you want to install.

### 5 Configure Gateway(s)

For each gateway:

- Enter fully qualified DNS name or IP address.
- Enter listening port of the server or use the default.

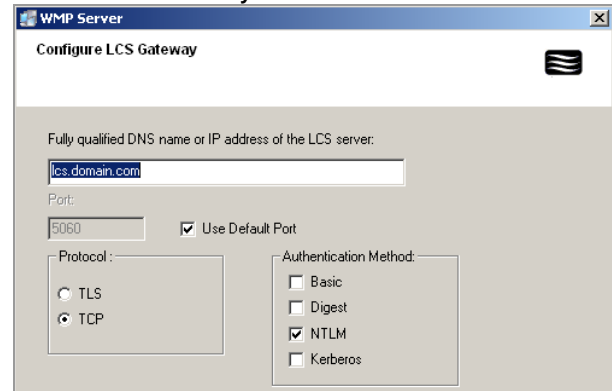
*This information can be changed later in the gateway configuration file.*

**Note** Contact your server administrator for the correct gateway settings.

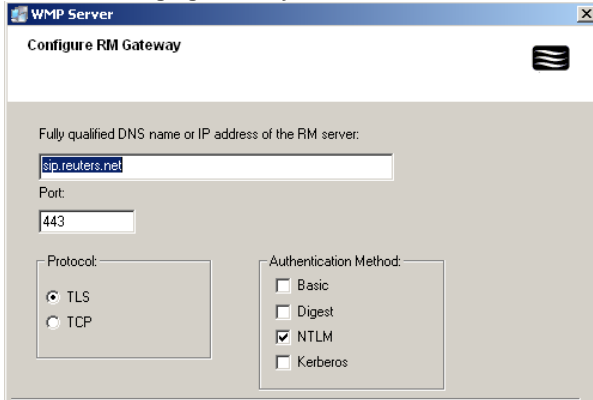
#### Lotus IBM Sametime Gateway



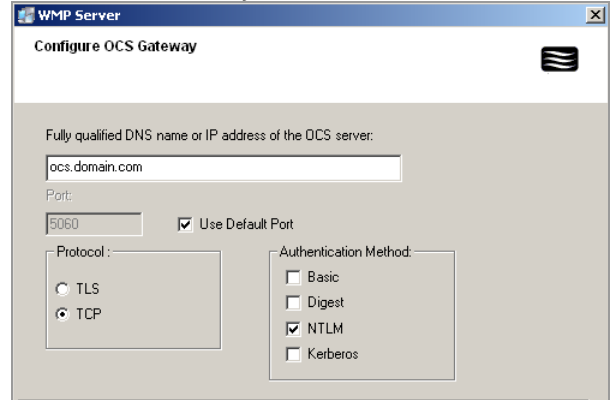
#### Microsoft LCS Gateway



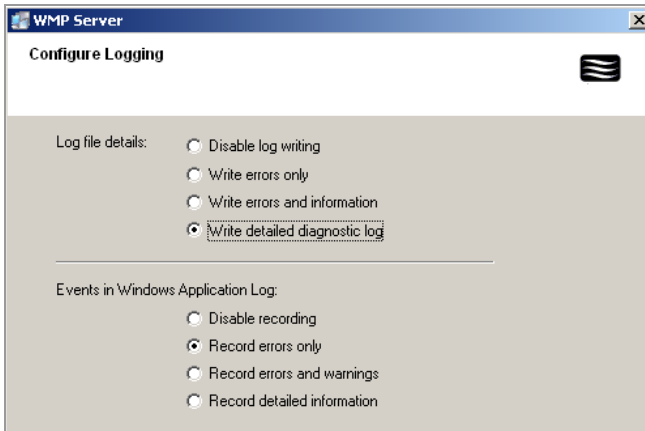
### Reuters Messaging Gateway



### Microsoft OCS Gateway



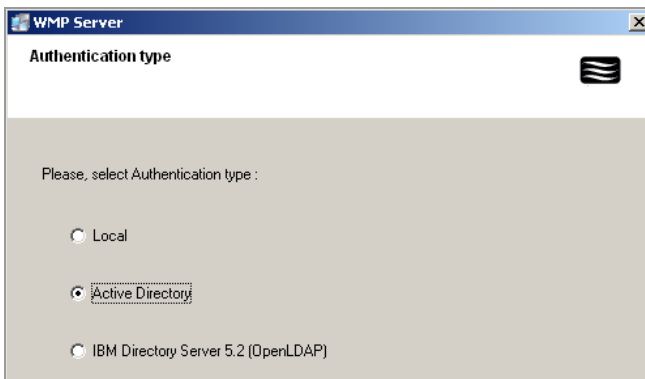
## 6 Configure Logging Settings



This screen allows you to specify the logging settings for the server. Events such as warning, errors and notices can be recorded in each service's log file, according to the chosen log level.

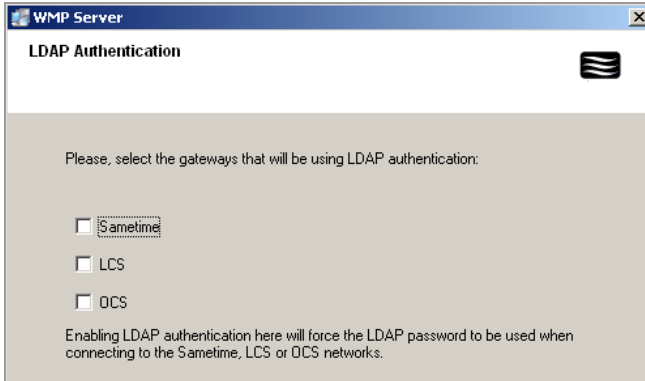
*Recommendation:*  
Keep defaults settings - detailed logs help our support team if you have any installation issues.

## 7 Select Authentication Type



Select the authentication type.

## 8 Select LDAP Authentication Gateways

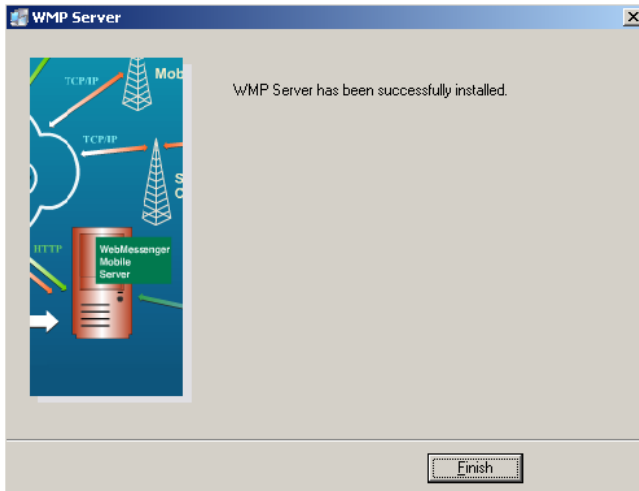


If you selected **Active Directory** authentication in the previous screen, you can select the enterprise gateways supporting this authentication.

When a gateway is selected for Active Directory authentication, the same Active Directory password will be used to login to the server and to log in the enterprise server (OCS, LCS or Sametime).

**Note** Do not select a gateway for Active Directory authentication if the Active Directory user passwords do not match the enterprise server account passwords.

## 9 Finish Installation



Click **Finish** to complete the installation. You may have to reboot.

### Uninstall the WM Server

1. From the Control Panel window, double-click **Add/Remove Programs**.
2. From the list of programs, select **WM Server** and click **Add/Remove**.
3. Click **OK** to confirm that you want to remove the application and all of its components.
4. From the Control Panel window remove MSDE and then delete all files from folder **C:\Program Files\Microsoft SQL Server**. This step is necessary only if you have installed MSDE.
5. From the Control Panel, uninstall the Java SDK.

## WM Mobile IM Server: Post-Installation

### Create New Users

The WM server creates a default predefined user with administrator privileges: **wmpadmin** with password **wmpadmin**. The purpose of this account is to act as a server administrator for the WM Server administration tools.

## 1 Add Users

Start the WM User Manager from program group **Programs/WebMessenger/WM Server**.

Click **Add** to create user, choose account type **Local**, and enter the user ID and the password.

## 2 Set IM Proxy Users

Set the IM networks proxy accounts for this user (MSN, AOL, ICQ, Yahoo!, Jabber, Google, Sametime, OCS, LCS, RM).

Each account consists of user ID in the particular network and password.

## 3 Exit WM User Manager

When you are ready, click **Exit** to close **WM User Manager**. Users can self-register and set their proxy accounts using the provided web registration page or through the mobile clients.

## 4 Self-Register

Registration	
<b>Username:</b>	<b>Password:</b>
<input style="width: 100%;" type="text" value="user name"/>	<input style="width: 100%;" type="password" value="*****"/>
	<b>Confirm Password:</b>
	<input style="width: 100%;" type="password" value="*****"/>
<b>First Name:</b>	<b>Last Name:</b>
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
<b>E-mail:</b>	
<input style="width: 100%;" type="text"/>	
<b>Company:</b>	<b>Phone number:</b>
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
aol <input checked="" type="checkbox"/>	
<b>Username:</b>	<b>Password:</b>
<input style="width: 100%;" type="text" value="your proxy account"/>	<input style="width: 100%;" type="password" value="*****"/>
msn <input checked="" type="checkbox"/>	
<b>Username:</b>	<b>Password:</b>
<input style="width: 100%;" type="text" value="your proxy account"/>	<input style="width: 100%;" type="password" value="*****"/>
yahoo <input checked="" type="checkbox"/>	
<b>Username:</b>	<b>Password:</b>
<input style="width: 100%;" type="text" value="your proxy account"/>	<input style="width: 100%;" type="password" value="*****"/>
icq <input checked="" type="checkbox"/>	
<b>Username:</b>	<b>Password:</b>
<input style="width: 100%;" type="text" value="your proxy account"/>	<input style="width: 100%;" type="password" value="*****"/>
<b>Fields indicated with * are required.</b>	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Open <https://machine.domain.com:1443/registration/index.jsp> (replace [machine.domain.com](https://machine.domain.com) with the correct address of your WM server machine).

Click **Registration** link and enter your information, then click **Submit**.

## Log In to Your Client

The following are instructions for configuring and logging in to the WebMessenger Mobile BlackBerry client.

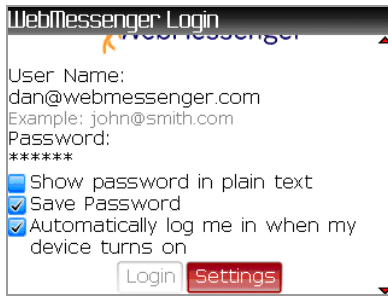
See the *WM Client User Guides* for configuring and logging in to other supported mobile devices.

## 1 Start WebMessenger



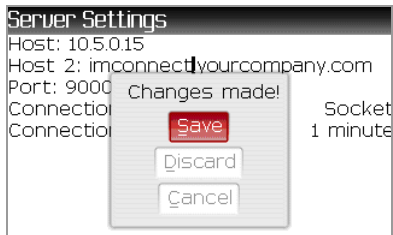
From the ribbon, select the WebMessenger icon and click the trackwheel.

## 2 Choose Settings



From **WM Login**, click the trackwheel, select **Settings** and click the trackwheel again.

## 3 Set Host Setting



Replace **10.5.0.15** with the IP address of your WM server address, click the trackwheel, select **Save** and click the trackwheel again.

## 4 Allow Connection

You may receive a prompt to allow the connection. Make sure you do so in order to be able to use the application.

*Please refer to the WM Client User Guides for instructions on how to populate your contact list and start using the WebMessenger Mobile client.*

# ACTIVE DIRECTORY AUTHENTICATION

The **Active Directory (AD) Authentication Manager** is used to configure the WebMessenger Server that authenticates the Active Directory user accounts.

## Overview

A user is considered successfully authenticated against the Active Directory server when the user:

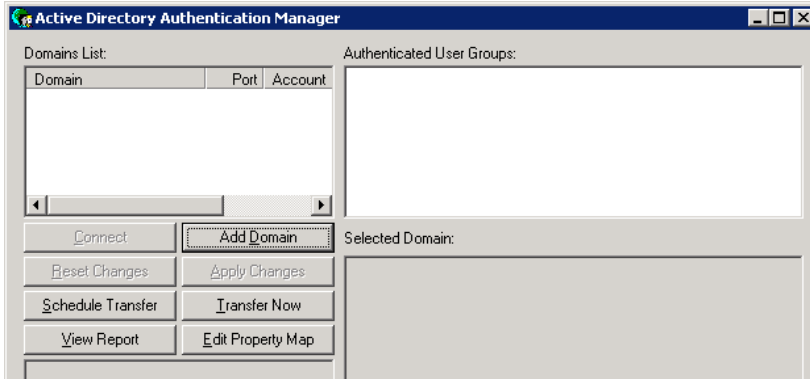
- is found on the Active Directory server
- has provided the same password as the one stored in the Active Directory server
- is a member of at least one allowed authentication group

It is a good practice to create one or more groups in Active Directory and to make all users that have rights to login to WebMessenger Server, members of these groups.

The LDAPAuthentication service uses standard Microsoft implementation of the LDAP protocol. It could authenticate users against more than one Active Directory server. Three login name formats are supported:

- NetBIOS style: **DOMAIN\user**
- DNS style: **<user@domain.com>**
- SIP URI: **<user@lcs.domain.com>**

## 1 Start the Active Directory Authentication Manager



Start > Programs >  
WebMessenger > AD  
Authentication Manager

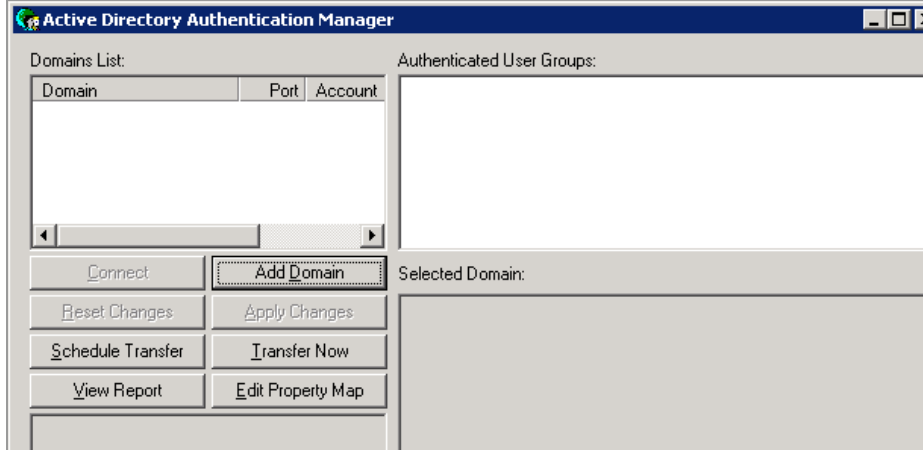
### AD AUTHENTICATION MANAGER OPTIONS

<b>Domain List</b>	Display a list of available domains to connect to for user authentication.
<b>Connect</b>	After selecting a domain from the list, click <b>Connect</b> to allow the <b>AD Authentication Manager</b> to connect to the domain and populate the <b>Selected Domain</b> list (bottom right window) with the domain groups.
<b>Add Domain</b>	Click to display the <b>Add Domain</b> dialog and enter information to create/add a new domain to the <b>Domain</b> List.
<b>Reset Changes</b>	Select to restore settings to the state prior to the last <b>Apply Changes</b> .
<b>Apply Changes</b>	Select to save all modifications.
<b>Schedule Transfer</b>	Select to configure a scheduled task for automatic execution of <b>AD Authentication Manager</b> for importing Active Directory users.
<b>Transfer Now</b>	Select to import users from the selected groups into the WM Server database.
<b>View Report</b>	Select to open saved reports. Every time <b>AD Authentication Manager</b> imports users into the WM database, it saves the import result in a report file in comma-separated format.
<b>Edit Property Map</b>	Select to map the Active Directory user properties to WM user properties.
<b>Authenticated User Groups</b>	Display a list of groups selected for authentication.
<b>Selected Domain</b>	After connecting to domain, list displays of available groups associated with the domain.

## Import Active Directory Users

To allow a user from Active Directory to have access to the WM Server, users must first be imported into the WM database.

### 1 Start AD Authentication Manager



Start > Programs > WebMessenger > AD Authentication Manager

Click **Add Domain** to display the **Add Domain** dialog.

### 2 Add Domain

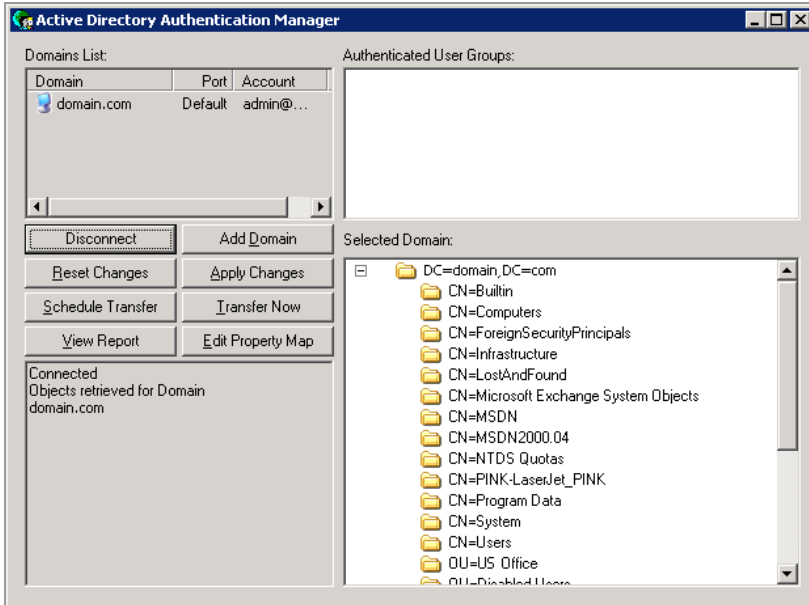
**Domain:** domain name where the active directory is located  
**Port:** communication port to access the active directory  
**Account:** administrator account name to access the directory (**administrator@domain.com**) - any account that can browse the Active Directory can be used  
**Password:** administrator account password

Click **OK** to add it to the **Domain** List.

### Edit Domain

To edit an existing domain, double-click the domain entry to open the **Edit Domain** dialog. To delete a domain, select a domain from the list and click **Delete**.

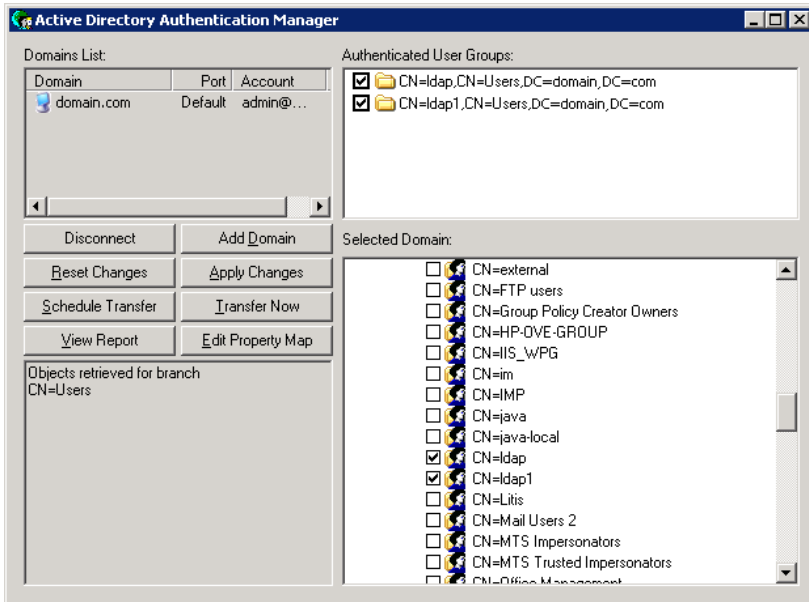
### 3 Connect to Domain



Select a domain from the list and click **Connect**.

The **AD Authentication Manager** will connect to the domain and populate the **Selected Domain** list (bottom right window) with the domain groups.

### 4 Choose Groups To Be Authenticated



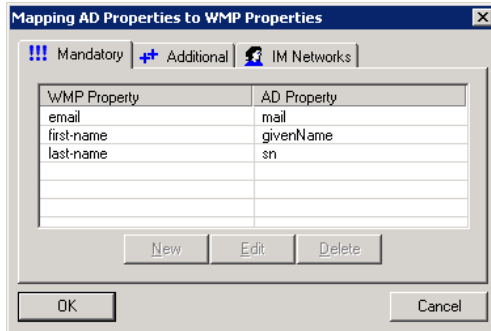
In the **Selected Domain** list, choose the groups to be authenticated by selecting the checkbox for each. The checked groups will appear in the **Authenticated User Groups** list (top right window).

To delete a group, select the group and click **Delete**.

To keep the group in the list but disable it for authentication, clear the checkbox.

Click **Edit Property Map** to display the **Mapping AD to WM** dialog.

## 5 Map Current Active Directory (Optional)



Map the AD properties with WM properties:

- **Mandatory:** main properties like email, first name, last name
- **Additional:** additional properties like cell phone, age, etc.
- **IM Networks:** proxy accounts for each authenticated user, if present in AD

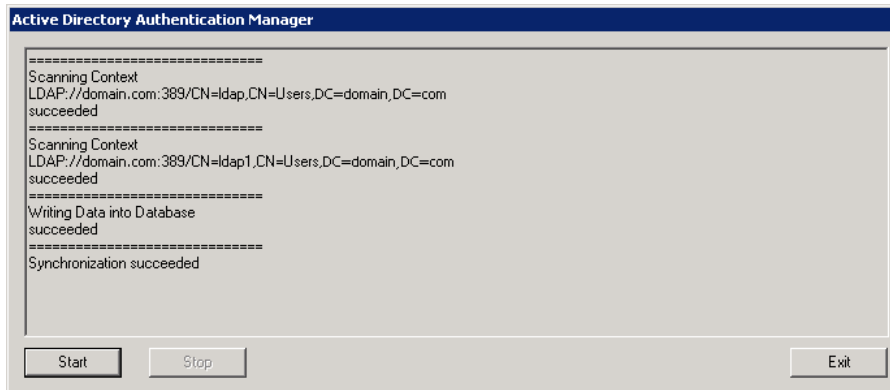
EXAMPLE: To create an LCS proxy account for a user, map Active Directory Exchange attribute **msRTCSIP-PrimaryUserAddress** to WebMessenger Server database property **LCS**.

When mapping is complete, click **OK**.

From **Active Directory Authentication Manager**, click **Apply Changes** to save all changes. **Reset Changes** will restore settings to the state prior to the last **Apply Changes**.

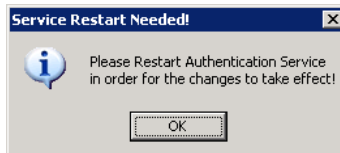
Click **Transfer Now** to import users, with their mapped properties, from the selected groups into the WM database.

**Note** Mapping is an optional step; it is not required for the Active Directory authentication to work.



Writing data to DB and synchronization will be confirmed.

### Restart Services

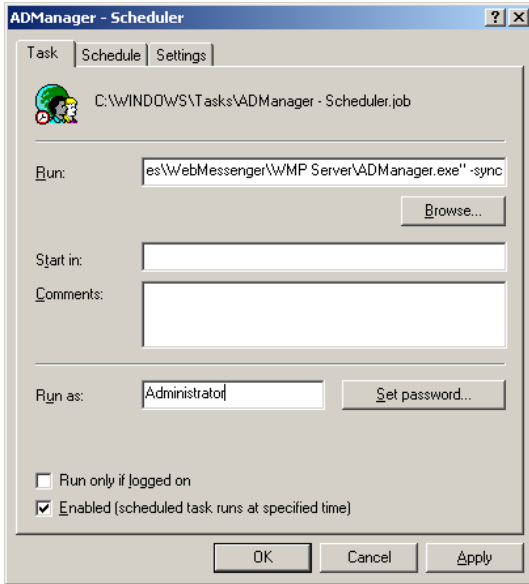


When changes have been made that require a restart of WebMessenger LDAP Authentication service, this message will display.

### Schedule User Updates

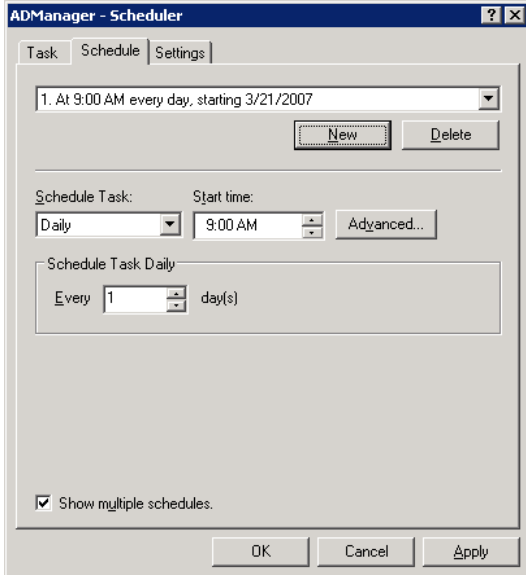
The **AD Authentication Manager** allows you to configure scheduled synchronization of WebMessenger Server to Active Directory in accordance with the **ADManager.ini** file.

## 1 Open ADManager Scheduler



Click **Schedule Task** to display the **ADManager – Scheduler** screen.

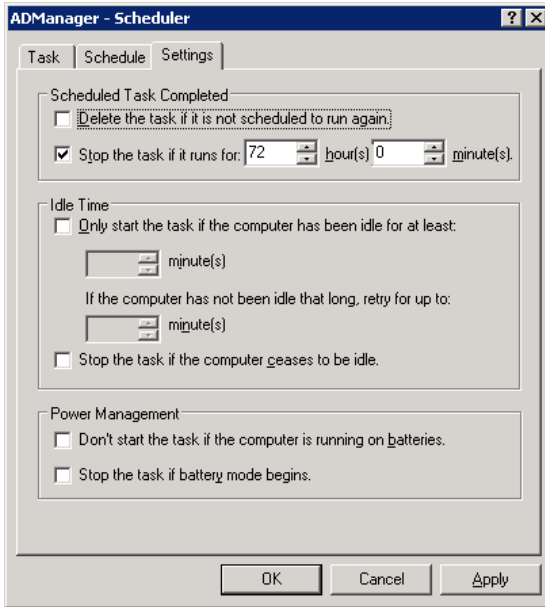
## 2 Create New Scheduled Task



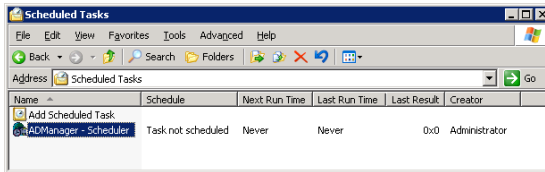
Select the **Schedule** tab and click **New** to create a new scheduled task.

Configure the task properties.

### 3 Schedule Limitations

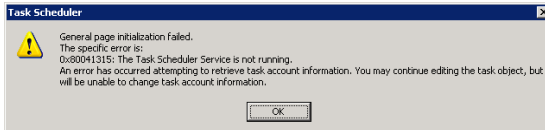


Select the **Settings** tab to set schedule limitations. Click **OK** to save the scheduled task and exit the **Scheduler** screen.



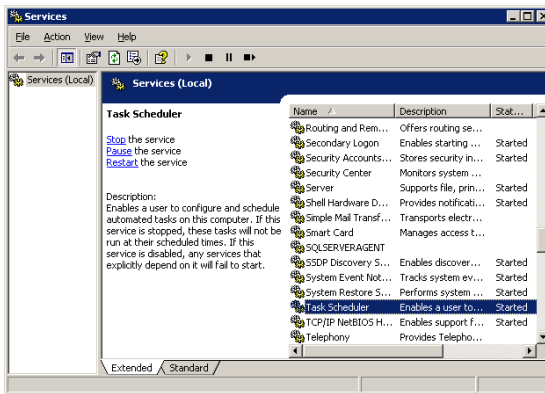
To verify that the task is properly scheduled, go to **Start > Settings > Control Panel > Scheduled Tasks**.

### Possible Warning Dialog



Possible issue:

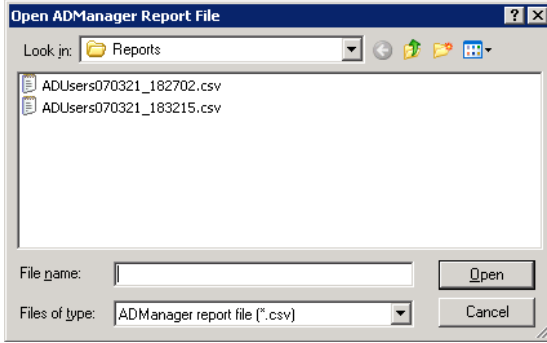
If Task Scheduler service is not running (Disabled or Stopped), this warning dialog will appear when you click **Schedule Transfer on Active Directory Authentication Manager**.



To resolve this issue go to **Services**, run Task Scheduler and make sure the Startup Type is set to **Automatic**.

## Reports

When AD Authentication Manager imports users into the WebMessenger Server database, it generates a report file in comma-separated (CSV) format stored in the **Reports** subfolder.



Click **View Report** to display the **Open AD Authentication Manager Report File** dialog and open a report associated with a CSV file extension application.

## Configuration Files

Active Directory (AD) Authentication Manager uses two configuration files – **ADManager.ini** and **LdapAuthentication.ini**. The AD Authentication Manager and the two configuration files are located in the WebMessenger Server installation folder. The **ADManager.ini** file is used to configure AD Authentication Manager itself. This is a “read only” file and can only be modified manually. The **LdapAuthentication.ini** file is a configuration file for the WebMessenger Server LDAPAuthentication Service. Although it is not recommended, this file can be modified manually.

Each time AD Authentication Manager starts, it reads these two **ini** files and the WM properties from the WebMessenger database as configured in the **LdapAuthentication.ini** file under the [Database] section. After modifications have been made and the Apply Changes or Transfer Now functions have been executed, the AD Authentication Manager saves the modifications under the [LDAP] section in the **LdapAuthentication.ini** file.

The format of the two files under the [LDAP] section is the same. In the following description, where name of the key ends with **X**, it has to be replaced with a digit, and if **X** is preceded with a **Y**, the two letters have to be replaced with a letter and a digit.

GENERIC KEY NAMES AND ACTUAL MEANING		
<b>PropMX</b>	becomes	PropM0, PropM1 ...
<b>NameY</b>	becomes	NameA, NameB ...
<b>PathYX</b>	becomes	PathA0, PathA1... PathB0, PathB1, ...

The keys with the same letter as suffix form a subsection of parameters related to one domain.

## ADManager.ini

KEY NAME	DESCRIPTION
<b>FirstIniFile</b>	[mandatory] File name of first target configuration file - the Tool will read database connection settings from this file and write [LDAP] section settings in it
<b>SecondIniFile</b>	[optional] File name of second target configuration file - the Tool will duplicate [LDAP] section
<b>UseDomainNTName</b>	Controls format of <b>&lt;user name&gt;</b> part in LCS/RM proxy accounts. <b>&lt;signin name&gt;;&lt;user name&gt;</b> <b>YES</b> – user name will be imported in format <b>domain\user</b> <b>NO</b> – user name will be imported in format <b>&lt;user@domain&gt;</b> Default value is <b>NO</b>
<b>ColumnSeparator</b>	Character used as column separator in the report file Possible values: “;”, “”, “ <b>TAB</b> ” or other Default value: “;”
<b>PropMX</b>	WM predefined mandatory property mapping parameter Format: WM property , AD attribute  EXAMPLE: PassA=TYGVOPAS

KEY NAME	DESCRIPTION
	<p>Currently pre-set mandatory mappings are:</p> <pre>PropM0=email,mail PropM1=first-name,givenName PropM2=last-name,sn</pre>
<b>PropEX</b>	<p>WM predefined additional properties mapping parameter Format: WM property , AD attribute</p> <p>EXAMPLE: PropE0=home-phone,homePhone</p>
<b>ProxyX</b>	<p>WM predefined IM Network properties mapping parameter Format: WM property , AD attribute</p> <p>EXAMPLE: Proxy0=LCS,msRTCSIP-PrimaryUserAddress</p>

**EXAMPLE**

```
[LDAP]
FirstIniFile=ldapauthentication.ini
SecondIniFile=authentication.ini
ColumnSeparator=,
PropM0=email,mail
PropM1=first-name,givenName
PropM2=last-name,sn
PropE0=home-phone,homePhone
PropE1=work-company,company
Proxy0=LCS,msRTCSIP-PrimaryUserAddress
PathB2=CN=group3,OU=Office,DC=domain2,DC=com
PropMB0=email,mail
PropMB1=first-name,givenName
PropMB2=last-name,sn
PropEB0=home-address,postalAddress
PropEB1=work-company,company
ProxyB0=LCS,msRTCSIP-PrimaryUserAddress
```

**LdapAuthentication.ini:**

KEY NAME	DESCRIPTION
<b>ServerY:</b>	<p>Domain name in DNS style of domain Y</p> <p>EXAMPLE: ServerA=domain.com</p>
<b>PortY:</b>	<p>Port, usually it is 389</p> <p>EXAMPLE: PortA=389</p>
<b>NameY:</b>	<p>Login account for domain Y</p> <p>EXAMPLE: NameA=administrator</p>
<b>PassY:</b>	<p>Account password in encrypted form</p> <p>EXAMPLE: PassA=TYGVOPAS</p>
<b>PathYX:</b>	<p>Distinguished name of a selected group</p> <p>EXAMPLE:</p>

KEY NAME	DESCRIPTION
	PathA0=CN=group1, CN=Users, DC=domain, DC=com PathA1=CN=group2, CN=Users, DC=domain, DC=com

**EXAMPLE**

```
[LDAP]
AccA=
NameA=administrator
PassA=GHDEETMNB
ServerA=domain1.com
PortA=389
PathA0=CN=group1, CN=Users, DC=domain, DC=com
PropMA0=email, mail
PropMA1=first-name, givenName
PropMA2=last-name, sn
PropEA0=home-address, homePostalAddress
PropEA1=home-phone, homePhone
ProxyA0=LCS, msRTCSIP-PrimaryUserAddress
ProxyA1=RM, msRTCSIP-PrimaryUserAddress
AccB=
NameB=admin
PassB=POTVBNMTR
ServerB=domain2.com
PortB=389
PathB0=CN=group1, CN=Users, DC=domain2, DC=com
PathB1=CN=group2, CN=Users, DC=domain2, DC=com
PathB2=CN=group3, OU=Office, DC=domain2, DC=com
PropMB0=email, mail
PropMB1=first-name, givenName
PropMB2=last-name, sn
PropEB0=home-address, postalAddress
PropEB1=work-company, company
ProxyB0=LCS, msRTCSIP-PrimaryUserAddress
```

**Sections**

**[ADMAUTH]**

<b>set_proxy_password_domains:</b>	<p>Comma-separated list of IM domain names, possible values:</p> <p><b>LCS</b> – force AD password for LCS proxy accounts  <b>Sametime</b> – force AD password for IBM Lotus Sametime proxy accounts</p>
------------------------------------	--

**[LDAP]**

This section contains parameters that LdapAuthentication service will use to connect to the Active Directory server. The **AD Authentication Manager** will fill in this section for you. For better control, some of the parameters are explained below. In the explanation, **X** at the end of a parameter name has to be replaced with letters **A, B, C ...** for each Active Directory server configuration.

<b>HostX:</b>	DNS name or IP address of the Active Directory domain controller If Active Directory server must be accessed by IP address, specify the IP address here and also configure PortX (or SSLPortX – when using SSL/TLS)
<b>SSLPortX:</b>	Port to use for SSL/TLS connection - use this setting when working with port 636, as it assumes SSL/TLS connection
<b>MethodX:</b>	<p>Bind (authentication) method to be used, possible values are:</p> <p><b>SIMPLE</b> – sends password in clean text  <b>NTLM</b> – default bind method  <b>GSSAPI</b> – negotiate with Active Directory server the best method available  <b>DIGEST-MD5</b> – If choosing this method, make sure it is supported by the Active Directory server (AD on 2003 server is) and AD is configured to store passwords by "reversible encryption"  <b>MSN</b> – Microsoft Network authentication  <b>DPA</b> – Normandy authentication (new MSN) authentication</p>

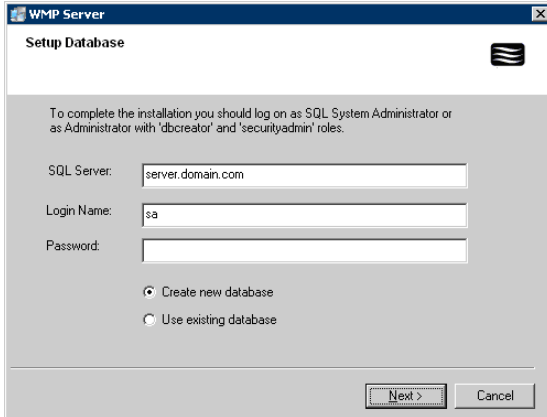
<b>FullName:</b>	Considered only when <b>SIMPLE</b> bind method is configured, user name will be in the form <b>user@domain.com</b>
------------------	--

## ADVANCED SETUP

### Microsoft SQL Server Installation

You can choose to use an existing MSSQL database server 2000 or 2005 instead of MSDE. Do the following when the MSSQL server is on the local machine:

#### Setup Database



Enter the hostname or IP address of an existing Microsoft SQL Server into field **SQL Server**.

Enter a login name (usually **sa**) and password with administrator privileges.

In the radio group below, choose one of the options:

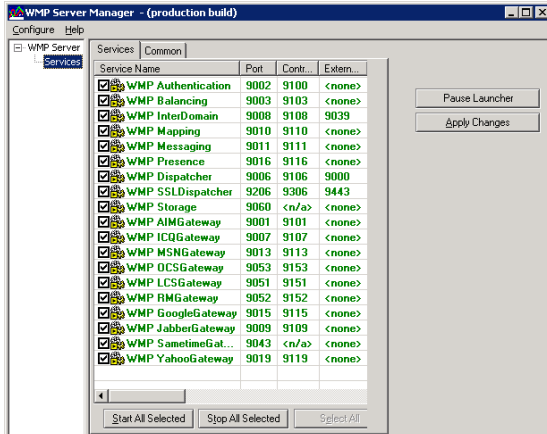
- **Create new database** – select this option if there is no existing database on the chosen MSSQL server
- **Use existing database** – select this option when you are upgrading an existing installation or when you want to reuse an existing database

When you do not have an MSSQL installation on the local machine, the setup prompts for MSDE installation. If you choose MSDE, it will be installed on the local machine (using the login **sa** and password **saPass**) and all other database setup steps will be done automatically.

**Note** *MSDE installation must be present in the directory MSDE2000A along with the server setup, in order for the setup to find it and install it automatically. When this condition is not met, the setup will prompt you to browse and select the setup.exe in the folder containing the MSDE.*

## WM Server Manager

### 1 Start/Stop Server Modules



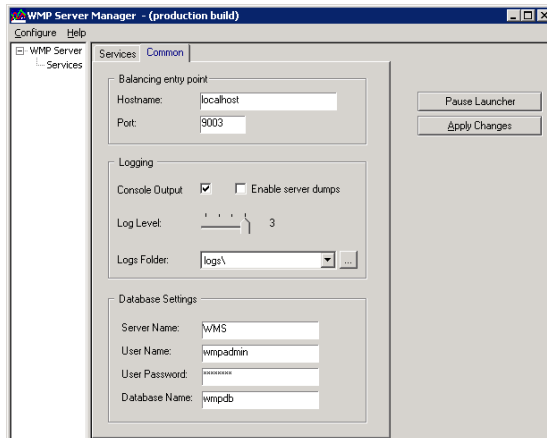
To Start/Stop/Restart a server module as service or as console application – right-click it with the mouse and select desired option from the context menu.

To disable temporarily a particular service from being automatically started by the Launcher service (the server watchdog service), uncheck the service checkbox in the **Launcher** list.

If you want to save the modifications, click **Apply Changes**.

You could also temporarily pause the **Launcher** by clicking **Pause Launcher** or **Pause** from **Launcher** Control Panel.

## 2 Control Settings



The **Common** tab provides control of each service's common settings (see **Service Info** section in the **ini** file).

- **Balancing entry point** – host name (or IP address) of the computer where WM Balancing service runs and listens
- **Logging** – whether to output logging details to the console window, minimal log level (ranging from 0: off to 3: full with debug) and the folder where the log files will be stored
- **Database Settings** – what provider will be used (MSSQL, PostgreSQL, etc.) and the needed settings to connect to the database – server host name, user account, password and database name

## WM Server Event Log

WM Server's services write events into the Windows Application Event Log. To enable it per WM service, put in [TRACKING] section of service configuration file **event log = <event type>**, where **<event type>** can be **0** - disabled, **1** – errors only, **2** – errors and warnings, **3** – errors, warnings and information events.

```
[TRACKING]
eventlog = 1
```

There are informational, warning and error events with the following specification for Type, Source, Category and custom defined event IDs. Source of events is WM Server, Category identifies WM Server's service.

### Event Types

- Information** – fires when WM service has been successfully started and when the WM server has recovered from failure
- Warning** – fires when the WM server can safely recover from a problematic situation
- Error** – fires when unrecoverable error occurs or when a recoverable error repeats 3 times in a row

### Event Definitions

WM SERVER SERVICES				
TYPE	SOURCE	CATEGORY	EVENT IDs	DESCRIPTION
Information	WM Server	Service name	13002	Service started
Information	WM Server	Service name	13003	Database connection established
Information	WM Server	Service name	13004	Service connection established
Warning	WM Server	Service name	14001	Service to service connection lost
Warning	WM Server	Service name	15001	Recoverable service failure
Error	WM Server	Service name	15002	Database connection lost - Resolve the problem and restart the WM server
Error	WM Server	Service name	15003	Repetitive service failure. 'Service name' failed N times for S seconds

LDAP ADMINISTRATION TOOL				
TYPE	SOURCE	CATEGORY	EVENT IDs	DESCRIPTION
Information	WM Server	LDAP Authentication Manager	13501	User synchronization successfully completed

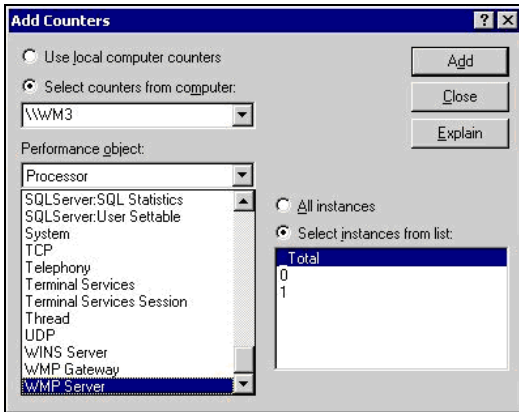
LDAP ADMINISTRATION TOOL				
TYPE	SOURCE	CATEGORY	EVENT IDs	DESCRIPTION
Information	WM Server	LDAP Authentication Manager	13501	User synchronization successfully completed
Information	WM Server	LDAP Authentication Manager	13502	User synchronization started
Information	WM Server	LDAP Authentication Manager	13503	User synchronization interrupted by the administrator
Information	WM Server	LDAP Authentication Manager	14501	LDAP information extraction failure
Warning	WM Server	LDAP Authentication Manager	14502	Database connection failure
Warning	WM Server	LDAP Authentication Manager	15501	LDAP information extraction failure
Error	WM Server	LDAP Authentication Manager	15502	Database connection failure
Error	WM Server	LDAP Authentication Manager	15504	Bad configuration settings

## WM Performance Counters

WM server exports two Performance objects – **WM Server** and **WM Gateway** each with its own list of performance counters like messages per second, presence packets per second, number of logged in users per gateway and so on. To enable performance counter per service and to be able to see it in Performance console - set counters to **on** in Performance section.

```
[PERFORMANCE]
counters = on
```

### 1 Open Performance Console



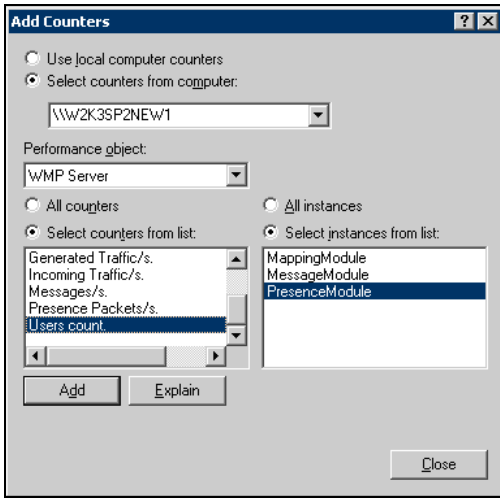
Use Microsoft's Performance console (**Perfmon.msc**) to view graphically represented counter data.

To open it, do one of the following:

Click **Start > Run >** type **perfmon >** click **OK**  
 OR  
 Use **Start Menu > Programs/Administrative Tools/Performance**

Select **System Monitor** from the left, then click **Add**.

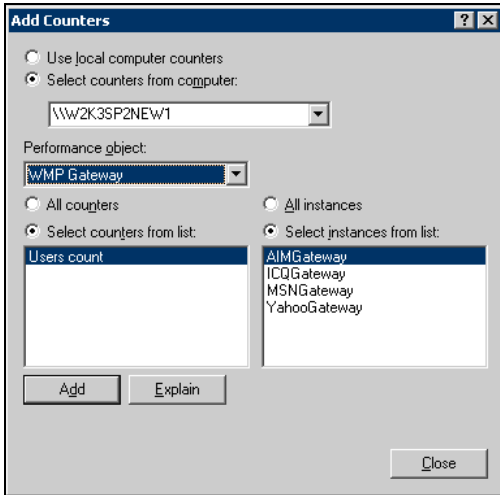
## 2 Add Counters



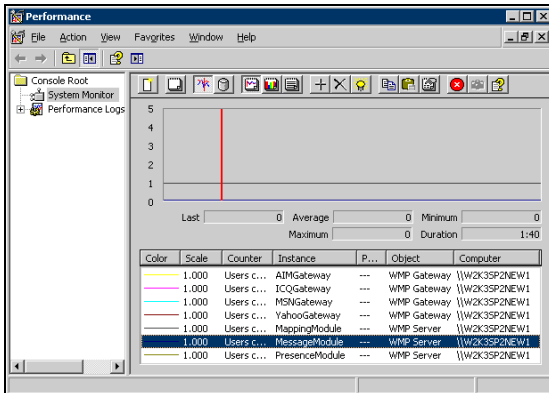
Go to **Performance object** combo box and select **WM Server** or **WM Gateway** object.

Select desired counters and instance of each counter.

Click **Add** to add counters in graph.



## 3 View Real Time Counter Values



You can see real time values of selected performance counters.

## Gateways

### Proxy Configuration

Currently the AIM, ICQ, MSN, Sametime, Yahoo!, Jabber and Google gateways could be configured to use HTTP/SOCKS proxy. You can take the configuration values from Internet Explorer's Internet (Proxy) Settings page.

```
#####
# SOCKS 4/5 support
[PROXY]
# 0 -- no proxy
# 1 -- HTTP proxy
# 4/5 -- SOCKS 4/5
type = 0
proxyaddress =
proxyport =
# leave blank if authorization is not used
username =
password =
# keep alive time in seconds
keepalive =
```

### Work with TLS Protocol

When OCS or LCS gateway is configured to use TLS protocol, there might be additional installation steps.

- If OCS/LCS server address is manually configured in gateway's configuration file, set server address with its FQDN name (not IP) in configuration parameter **serveraddress**: for OCS and/or **rtcserveraddress**: for LCS.
- If OCS/LCS server's certificate is signed from not-trusted Certificate Authority, follow this procedure:

To import the digital certificate for the OCS/LCS server's root CA into the Trusted Root Certification Authorities folder in the Local Computer certificate store:

1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. Click **File**, and then click **Add/Remove Snap-in**.
3. On the Standalone tab, click **Add**.
4. Select **Certificates**, then click **Add**. When prompted, select **Computer account**, and then click **Next**.
5. On the Select Computer page, select **Local computer** (the computer this console is running on), and then click **Finish**.
6. In MMC, expand **Certificates – Local Computer**, and then expand **Trusted Root Certification Authorities**.
7. In the details pane, right-click and point to **All tasks**, and then click **Import**.
8. On the first page of the Certificate Import Wizard, click **Next**.
9. In the File name dialog box, type the name and location of the file containing the root CA's digital certificate, and then click **Next**.
10. On the Certificate Store page, click **Place all certificates in the following store**, make sure that the Certificate store dialog box shows **Trusted Root Certification Authorities**, and then click **Next**.
11. On the final page of the wizard, click **Finish**.

### Setup Auditors

#### IM Logic Auditor

DNS Redirecton to IM Logic should be set up. No further actions are required.

#### FaceTime Auditor

Edit gateways configuration files and setup proxy settings to point to FaceTime proxy. Use proxy type 40 or 50 (SOCKS version 4 or 5 using FaceTime Auditor).

## AIM and ICQ Gateways Configuration

<b>External Network Server Hostname and Port</b>	<p>If AIM/ICQ server address is different than typical <b>login.oscar.aol.com : 5190 / login.icq.com : 5190</b>, you could enter actual addresses in parameters:</p> <pre>foreignserver = &lt;address&gt; foreignport = &lt;port&gt;</pre>
<b>Custom Status Message</b>	<p>To enable receiving of custom status messages from AIM/ICQ server enter <b>1</b> for value of parameter <b>getstatusmessage</b>:</p> <pre>getstatusmessage = 1</pre>
<b>Typing Notification</b>	<p>To enable receiving of typing notification enter value <b>on</b> for parameter <b>typingnotification</b>:</p> <pre>typingnotification = on</pre>

## MSN Gateway Configuration

<b>Proxy Settings</b>	<p>You can use HTTPS proxy for .NET Passport Authentication. Fill in parameters of [SSL Proxy] section with appropriate values.</p>
	<pre>##### # SSL Proxy -- the proxy must be able to connect to port 443 (https) [SSL Proxy] # 0 -- no proxy # 1 -- HTTP proxy # 4/5 -- SOCKS 4/5 type = 0 proxyaddress = proxyport = # leave blank if authorization is not used username = password =</pre>
<b>Typing Notification</b>	<p>To enable receiving of typing notification enter value <b>on</b> for parameter <b>typingnotification</b>:</p> <pre>typingnotification = on</pre>
<b>Email Notification</b>	<p>To enable receiving of notification for recently received emails – enter value <b>on</b> for parameter <b>newmailnotification</b>:</p> <pre>newmailnotification = on</pre>
<b>Informative Messages</b>	<p>To enable this feature – enter value <b>on</b> for parameter <b>infomsgs</b>:</p> <pre>infomsgs = off</pre>

## Yahoo! Gateway Configuration

<b>Typing Notification</b>	<p>To enable receiving of typing notification enter value <b>on</b> for parameter <b>typingnotification</b>:</p> <pre>typingnotification = on</pre>
----------------------------	---

<b>Email Notification</b>	To enable receiving of notification for recently received emails – enter value <b>on</b> for parameter <b>newmailnotification</b> :  <code>newmailnotification = on</code>
---------------------------	--

### Google Gateway Configuration

<b>Typing Notification</b>	To enable receiving of typing notification enter value <b>on</b> for parameter <b>typingnotification</b> :  <code>typingnotification = on</code>
----------------------------	--

### Jabber Gateway Configuration

<b>Allow Domain List</b>	Specify one or more (separated by semi-colons “;”) domains in the <b>allowdomainlist</b> key: Only proxy accounts from these domains are allowed to use the gateway.  <code>allowdomainlist = jabber.org;jabber.com</code>
<b>Typing Notification</b>	To enable receiving of typing notification enter value <b>on</b> of parameter <b>typingnotification</b> :  <code>typingnotification = on</code>

### MS OCS Gateway Configuration

OCSGateway.ini file specific parameters. See [Service Info](#).

<b>serveraddress</b>	DNS name or IP address of a Office Communications Server 2007 (OCS)
<b>serverport</b>	OCS Server listening port
<b>transport</b>	transport/security
<b>getstatusmessage</b>	Enables OCS specific statuses like: “Do not Disturb”, “Be Right Back”, “Inactive”, “Busy (Inactive)” and others to be received as custom status message
<b>utf8</b>	'utf8 = on' enables utf8 encoding of contact's first and last name as well as names of the groups from user's contact list. Default value is off.
<b>accept_timeout</b>	Accept invitation timeout: seconds the gateway will wait before accepting IM invitation. Value type of this key is an integer, in the range 0-10, with 0 being the default one, if value is not specified. This parameter configures a period of time which OCS gateway will wait before accepting incoming instant messaging invitation. It allows a user logged simultaneously in OCS from WM mobile client and from Microsoft Office Communicator 2007 to accept invitation and start IM conversation on his desktop machine before accepting this message from WM mobile client.
<b>showblockeduser</b>	Enables showing status of the blocked user: <b>0</b> - shows as custom "Blocked" status, <b>1</b> - shows real status of the blocked user
Recommended values:	
<b>serveraddress</b>	<OCS server DNS name/IP address>
<b>serverport</b>	5060
<b>transport</b>	TCP/NTLM
<b>getstatusmessage</b>	1

### Automatic OCS Server Discovery

The automatic server discovery mode enabled when server connection parameters 'serveraddress', 'serverport' and 'transport' are missing, commented out, or empty in the gateway configuration file. For this case, a proper SRV record in DNS has to be set. The OCS gateway searches for next DNS records in order they are listed:

```
_sipinternaltls._tcp.<sip domain>
_sipinternal._tcp.<sip domain>
_sip._tls.<sip domain>
_sip._tcp.<sip domain>
```

Here <sip domain> refers to the host portion of the SIP URIs assigned to users. The OCS gateway does strict domain name matching between the domain in the SIP URI and the SRV record. For more information on how to configure DNS for automatic sign-in, see "Microsoft® Office Communications Server 2007 Planning Guide" document.

When TLS protocol is configured special requirements are needed. See [Work with TLS Protocol](#).

<b>MS LCS Gateway Configuration</b>	
LCSGateway.ini file specific parameters. See <a href="#">Service Info</a> .	
<b>rtcserveraddress:</b>	DNS name or IP address of a Live Communications Server 2003/2005 (LCS)
<b>rtcserverport:</b>	LCS Server listening port
<b>transport:</b>	transport / security
Recommended values:	
<b>rtcserveraddress:</b>	<LCS server DNS name/IP address>
<b>rtcserverport:</b>	5060
<b>transport:</b>	TCP/NTLM

When TLS protocol is configured special requirements are needed. See [Work with TLS Protocol](#).

<b>Reuters Messaging Gateway Configuration</b>	
RMGateway.ini file specific parameters. See <a href="#">Service Info</a> .	
<b>rtcserveraddress:</b>	DNS name or IP address of a Reuters Server
<b>rtcserverport:</b>	Reuters Server listening port
<b>transport:</b>	transport / security
<b>rtcserveraddress:</b>	sip.reuters.net
<b>rtcserverport:</b>	443
<b>transport:</b>	TLS/NTLM

**Note** On Windows 2000 Server only, either LCS or RM gateway can be working at the same time on one machine.

<b>IBM Lotus Sametime Gateway Configuration</b>	
<b>BuddyListSync:</b>	Used to synchronize the contact list. Possible values are <b>on/off</b> .  <b>on</b> – all buddies are stored on the Sametime server and can be retrieved on next login <b>off</b> – contact list is not stored and the buddies displayed in client are lost on the next login  <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; width: fit-content;">                     [Service Info]                      BuddyListSync = on                 </div>

## Verify Enterprise Gateway Configuration

When you log in on your mobile client it issues a command to the server to connect the corporate and public Instant Messaging (IM) servers that you have specified for this account. The WM server logs you in on these IM servers on your behalf, using the proxy account (user name and password) that you have specified for each IM network. The procedure explained below is for IBM Lotus Sametime, but can be used for the rest of the IM networks that have been installed with your server. Following this procedure the administrator can verify that the IM gateways that the WM server has are operating correctly.

### IBM Lotus Sametime Interoperability

Testing Sametime server interoperability:

1. If you are using Active Directory authentication – see [Active Directory Authentication Manager](#) to enable Active Directory authentication.
2. Go to the WM server registration page and log in with your account (if using Active Directory) or create new account (if you are using local authentication). Check the Sametime network checkbox and specify user name and password for your Sametime proxy account.
3. Install WM mobile client on your device. Set correct server address and port. Log in with your new account.
4. Log in to the Sametime server using a native Sametime client, with account different from the one you have set as proxy account. Add the "proxy user" you have assigned to your WM account as a buddy in your native Sametime client.
5. The status of the buddy in native Sametime client (the "proxy user") should change from offline to online. This proves that you have running WM server with working Sametime server interoperability.

### MS OCS 2007 Interoperability

If your OCS account has different sign-in name and user name, for example:

Sign-in name = **signinname@company.com**  
User name = **name@company.com**

Specify your OCS proxy account in this format: **<signinname@company.com;name@company.com>**

### Testing OCS Server Interoperability

Follow the procedure explained in the section for [Sametime](#) above. Use native OCS client for the test.

### MS LCS Interoperability

If your LCS account has different sign-in name and user name, for example:

Sign-in name = **signinname@company.com**  
User name = **name@company.com**

Specify your LCS proxy account in this format: **<signinname@company.com;name@company.com>**

### Testing LCS Server Interoperability

Follow the procedure explained in the section for [Sametime](#) above. Use native LCS client for the test.

### Reuters Messaging Server Interoperability

If your RM account has different sign-in name and user name, for example:

Sign-in name = **name.company.com@reuters.net**  
User name = **name@company.com**

Specify your RM proxy account in this format: **name.company.com@reuters.net;name@company.com**

### Testing Reuters Server Interoperability

Follow the procedure explained in the section for [Sametime](#) above. Use native Reuters client for the test.

## Active Directory

A user is considered successfully authenticated against Active Directory server when:

- it is found on server
- has the same password as one stored on server
- it is a member of at least one "allowed" group, if such is configured

It is a good practice to create one or more groups in LDAP Directory and to make all users with rights to login in WM Server members of these groups. By enabling or disabling groups in **LdapAuthentication.ini** you may control which user could login to WM Server and which not.

LdapAuthentication service uses standard Microsoft implementation of LDAP protocol. It could authenticate users against more than one LDAP server. It supports three kinds of login names:

- NetBIOS style - **DOMAIN\user**
- DNS style - **user@domain.com**
- SIP URI - **user@lcs.domain.com**

### Section "Service Info"

LdapAuthentication.ini file specific parameters

<b>tasklist</b>	ADMAUTH
<b>service_name</b>	ldapauthentication

### Section "ADMAUTH"

<b>stage</b>	4*
<b>dllname</b>	ADMAuth.dll*
<b>account_type</b>	<b>1</b> – create an account <b>0</b> – do not create**
<b>account_creation</b>	Comma-separated list of IM domain names ***

\*this is not an option

\*\*this parameter controls creation of WM account when successfully authenticated to Directory user does not present in WM database. If **account\_creation = 1** a user with login name and password2 will be created.

\*\*\*passwords of all proxy accounts from IM domains that are enumerated in a list will be updated with password of logged in user. Spaces are not allowed in list.

### Section "LDAP"

This section contains parameters that LdapAuthentication service will use to connect to LDAP Server. For Active Directory you have to use LDAP Authentication Manager tool which will fill it in automatically (see the tool's documentation). Additional parameters are explained below. In the explanation **X** at the end of parameter name has to be replaced with letters A, B, C ... for each Active Directory server configuration.

<b>HostX</b>	DNS name or IP address of the Active Directory domain controller If configured, together with PortX/SSLPortX could be used when connection to Directory goes through tunnel.
<b>SSLPortX</b>	Port to use for SSL/TLS connection
<b>MethodX</b>	Bind (authentication) method to be used, possible values are: <ul style="list-style-type: none"> <li>• <b>SIMPLE</b> - sends password in clean text</li> <li>• <b>NTLM</b> - default bind method</li> <li>• <b>GSSAPI</b> - ldap library will negotiate with AD server for the best appropriate method - usually library chooses <b>GSS-SPNEGO</b> method that uses Kerberos v5</li> <li>• <b>DIGEST-MD5</b> - to be used AD server has to support it (AD on 2003 Server does) and AD has to be configured to store passwords by "reversible encryption" *</li> <li>• <b>MSN</b> - Microsoft Network authentication</li> <li>• <b>DPA</b> – Normandy authentication (new MSN) authentication</li> </ul>

<b>FullName</b>	Taken in account only when <b>SIMPLE</b> bind method is configured. User name passed to ldap library will be in form <b>user@domain</b> , (user principal name) not <b>user</b> (SAM account name).
-----------------	---

\*By default AD Server keeps user password in one-way hash. **DIGEST-MD5** bind method server has to store user password by "reversible encryption," to be possible to compare stored password with one come from client. This could be set for entire domain in bit flag attribute **pwdProperties** of object **domainDNS** or for a user in attribute **userAccountControl** (flag **reversiblepwd = on**) for **user** object.

\*\*If there isn't any group configured, but after successful bind, the ADMAuth task will consider that user is authenticated.

\*\*\*When user uses its SIP URI, the ADMAuth task will bind to Active Directory by NameX & PassX configured in **ini** file. If they are omitted, task will use credentials of logged in Windows user, or will bind as anonymous user if **SIMPLE** bind method was configured.

## SSL Dispatcher Configuration

WM clients support secure socket connections via SSL, but for this functionality to work the SSL Dispatcher service must be configured and running. This section describes how to configure this service.

In the default installation, there is an executable and a configuration file, named **SSLDispatcher** and **SSLDispatcher.ini**, respectively.

### SSLDispatcher.ini

Preconfigured settings are OK to be used with the default certificate. If you wish to generate your own certificate, modify the "security" section in the **ini** file:

```
[security]
cert = default.cert
key = default.key
```

You need to specify your own certificate file (**.cert**) and private key file (**.key**), which is used by **SSLDispatcher**. These files must be in the Privacy Enhanced Mail (PEM) format.

The Privacy Enhanced Mail (PEM) format is now much more liberally used as a key format, and can contain private keys (RSA and DSA), public keys (RSA and DSA), and x509 certificates. It stores data in a Base64-encoded DER format, surrounded by ASCII headers, so it is suitable for text-mode transfers between systems. You can use the publicly available **openssl** command-line tool to generate a new key pair/certificate.

After making the changes, restart the service to apply them. Both files must be accessible to the service, and ideally should be located in the same directory as the executable and the configuration file.

## Internal Communication Ports

WM Server components may communicate with each other using TCP/IP protocol on the ports listed below. These ports should be enabled for TCP traffic within the WM server machine boundaries and between WM servers in WM cluster:

```
25, 443, 1533, 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009, 9010, 9011, 9012, 9013, 9015, 9016, 9019,
9039, 9043, 9044, 9050, 9051, 9052, 9060, 9101, 9102, 9103, 9105, 9106, 9107, 9108, 9109, 9110, 9111, 9112, 9113,
9116, 9119, 9120, 9121, 9122, 9143, 9150, 9201, 9202, 9300, 9998, 9999, 9443
```

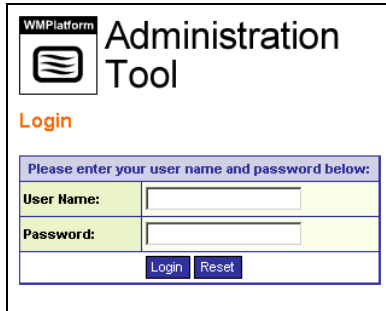
## WEB ADMINISTRATION

### Overview

The **Web Administration** tool allows you to observe the server statistics, manage services and users. The main links are:

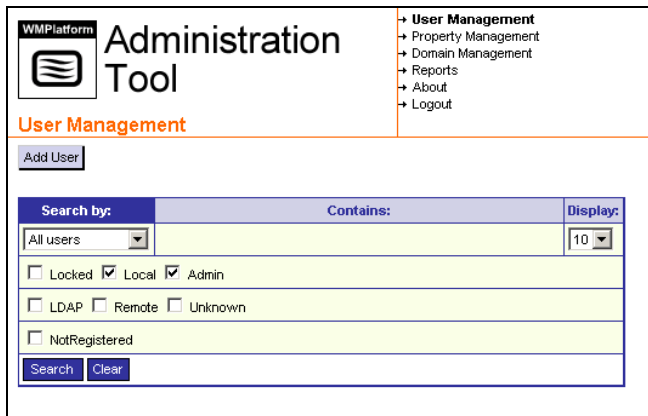
1. User Management
2. Property Management
3. Domain Management
4. Logout

### Login





Log in through **https://SERVERNAME:1443/admin/**, where **SERVERNAME** lookS like **www.company.com**.

### User Management





Do a user search, add a user and modify its properties from **User Management**.


 **Locked** - Temporarily locked local account (login not allowed)


 **Local** - User in the local database

 **Admin** - System administrator

 **LDAP** - Imported from Active Directory and authenticated through LDAP


 **Remote** - Buddies from external networks

 **Unknown** - Buddies from external networks (no activity so far)

 **Not Registered** - Newly created user accounts, which are not activated

Search for different type of users by selecting the proper user type (local, sip, ldap, etc.).

## Add User

 <b>Administration Tool</b>		<ul style="list-style-type: none"> <li>→ <b>User Management</b></li> <li>→ Property Management</li> <li>→ Domain Management</li> <li>→ Reports</li> <li>→ About</li> <li>→ Logout</li> </ul>
<b>User Management: Add User</b>		
<a href="#">Back to User Management</a>		
Property	Value	
User name	<input type="text"/> *	
Password	<input type="text"/> *	
Confirm Password	<input type="text"/> *	
First Name	<input type="text"/>	
Last Name	<input type="text"/>	
E-mail	<input type="text"/>	
Company	<input type="text"/>	
Phone Number	<input type="text"/>	
Fields indicated with * are required.		
<input type="checkbox"/> aol		
User name	<input type="text"/>	
Password	<input type="text"/>	
<input type="button" value="Register User"/> <input type="button" value="Clear"/>		

From **User Management** you can add a new user.

The mandatory parameters:

**Username**  
**Password**  
**Confirm Password**  
**First Name**  
**Last Name**  
**E-mail**  
**Company**  
**Phone Number**

## Edit User

Property	Value
email	Gordon@mail.net
first-name	John
last-name	Gordon
online-status	offline
work-phone	555-555-5555

Here you can modify an existing user.

You can:


- remove user from the server
- change user details
- remove property from user account
- view buddy filter for user
- view watcher: users watched on user properties
- view buddylist: full user buddy list
- change user ID and/or pass
- change account status

## View Buddy List

Name	Domain	Nick	Group	X
colin	WMP	Colin Davis	Friends	<input type="checkbox"/>
jay	WMP	Jay Horowitz	Friends	<input type="checkbox"/>
j.gordon	yahoo	J Gordon	Friends	<input type="checkbox"/>
jh1000	yahoo	Jay Horowitz	Friends	<input type="checkbox"/>

Here you can see the buddy list of the user.

## View Watcher



# Administration Tool

- **User Management**
- Property Management
- Domain Management
- Reports
- About
- Logout

User Management: View Watchers

[Back to Edit User](#)

20 watcher(s) for john's properties.

Name	Nick	Property
Colin Davis	Colin	online-status
Colin Davis	Colin	first-name
Colin Davis	Colin	last-name
Colin Davis	Colin	email
Colin Davis	Colin	work-phone
Colin Davis	Colin	reg-date
Jay Horowitz	Horowitz	online-status
Jay Horowitz	Horowitz	first-name
Jay Horowitz	Horowitz	last-name
Jay Horowitz	Horowitz	email
Jay Horowitz	Horowitz	work-phone
Jay Horowitz	Horowitz	reg-date
Mike Donovan	Donovan	online-status
Mike Donovan	Donovan	first-name
Mike Donovan	Donovan	last-name
Mike Donovan	Donovan	email
Mike Donovan	Donovan	work-phone
Mike Donovan	Donovan	reg-date
Tony Anderson	Tony	online-status
Travis Smith	Smith	online-status

Here you can see the watchers list of the user:

## Property Management

New Property Name	Description	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Create"/>
Property name	Description	Action
online-status	<input type="text"/>	<input type="button" value="Update"/>
first-name	<input type="text"/>	<input type="button" value="Update"/>
last-name	<input type="text"/>	<input type="button" value="Update"/>
nick-name	<input type="text"/>	<input type="button" value="Update"/>
email	<input type="text"/>	<input type="button" value="Update"/>
homepage	<input type="text"/>	<input type="button" value="Update"/>
gender	<input type="text"/>	<input type="button" value="Update"/>
age	<input type="text"/>	<input type="button" value="Update"/>
home-phone	<input type="text"/>	<input type="button" value="Update"/>
cellular	<input type="text"/>	<input type="button" value="Update"/>
home-address	<input type="text"/>	<input type="button" value="Update"/>
work-company	<input type="text"/>	<input type="button" value="Update"/>
work-jobtitle	<input type="text"/>	<input type="button" value="Update"/>
work-address	<input type="text"/>	<input type="button" value="Update"/>
work-phone	<input type="text"/>	<input type="button" value="Update"/>
work-fax	<input type="text"/>	<input type="button" value="Update"/>
work-homepage	<input type="text"/>	<input type="button" value="Update"/>
reg-date	<input type="text"/>	<input type="button" value="Update"/>
device-class	<input type="text"/>	<input type="button" value="Update"/>
pin-number	<input type="text"/>	<input type="button" value="Update"/>
activation-date	<input type="text"/>	<input type="button" value="Update"/>
image-url	<input type="text"/>	<input type="button" value="Update"/>
share-bl	<input type="text"/>	<input type="button" value="Update"/>
incl-share-bl	<input type="text"/>	<input type="button" value="Update"/>
alertrules	<input type="text"/>	<input type="button" value="Update"/>

The **Property Manager** allows you to extend existing properties with new ones.

You can create or put/update description of properties accessible from the user properties list (see **add property** from list in user account).

## Domain Management

New Domain Name	Address	Port	Requires Proxy Account	Sho Regis
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
Domain	Address	Port	Requires Proxy Account	Sho Regis
yahoo	wms.company.com	9001	<input checked="" type="checkbox"/>	<input type="text"/>
msn	wms.company.com	9013	<input checked="" type="checkbox"/>	<input type="text"/>
yahoo	wms.company.com	9019	<input checked="" type="checkbox"/>	<input type="text"/>
icq	wms.company.com	9007	<input checked="" type="checkbox"/>	<input type="text"/>
jabber	wms.company.com	9009	<input checked="" type="checkbox"/>	<input type="text"/>
google	wms.company.com	9015	<input checked="" type="checkbox"/>	<input type="text"/>
sametime	wms.company.com	9043	<input checked="" type="checkbox"/>	<input type="text"/>
ics	wms.company.com	9051	<input checked="" type="checkbox"/>	<input type="text"/>
pcs	wms.company.com	9053	<input checked="" type="checkbox"/>	<input type="text"/>
fm	wms.company.com	9052	<input checked="" type="checkbox"/>	<input type="text"/>

Open **Web Administration**. Go to **Domain Management**.

Add fully qualified Domain Name of the server where the gateways are run in **Address** field.

All other data should look exactly as shown on the screenshot.

Wait a couple of minutes for the changes to take an effect.

## INDEX

AD Authentication Manager	
screen options.....	14
AIM	
proxy configuration.....	28
AIM/ICQ	
Gateway configuration parameters .....	29
AOL	
IM Networks Proxy Accounts .....	11
required hosts/ports .....	5
BlackBerry client	
configuring .....	12
logging in.....	12
dialogs	
Active Directory Authentication Manager .....	15
Add Counters .....	26, 27
Add Domain .....	15
Add Proxy Users .....	11
Add User .....	11
ADManager Scheduler .....	19
Authentication type .....	9
Configure LCS Gateway .....	8
Configure Logging.....	9
Configure OCS Gateway.....	9
Configure RM Gateway.....	9
Configure Sametime Gateway .....	8
Database Server .....	7
Destination Location .....	8
Edit Domain .....	15
Interoperability Gateways.....	8
LDAP Authentication.....	10
Mapping AD Properties to WMP Properties ..	17
MS SQL Server Database.....	7
Open ADManager Report File.....	20
Performance .....	27
Registration.....	12
Scheduled Tasks .....	19
Service Restart Needed.....	17
Services .....	19
Task Scheduler .....	19
WMP Server.....	24
WMP Server Manager .....	24, 25
DNS settings	
checking.....	6
firewall settings .....	5
default port (9000).....	5
Dispatcher.ini file.....	5
required gateway hosts .....	5
required gateway ports .....	5
forward resolving.....	6
Google	
Gateway configuration parameters .....	30
IM Networks Proxy Accounts .....	11
proxy configuration.....	28
required hosts/ports .....	5
IBM Lotus Sametime	
Server interoperability .....	32
ICQ	
IM Networks Proxy Accounts .....	11
proxy configuration.....	28
required hosts/ports .....	5
ini files	
ADManager.ini .....	17, 20
Dispatcher.ini .....	5
LCSGateway.ini .....	31
LdapAuthentication.ini.....	20, 21, 33
OCSGateway.ini.....	30
SSLDispatcher.ini.....	34
Jabber	
firewall settings.....	5
Gateway configuration parameters .....	30
IM Networks Proxy Accounts .....	11
proxy configuration.....	28
required hosts/ports .....	5
keys	
allowdomainlist.....	30
LCS	
firewall settings.....	5
Gateway configuration parameters .....	31
IM Networks Proxy Accounts .....	11
LDAP Authentication Gateway.....	10
Server interoperability .....	32
LDAP Administration Tool .....	25
MS SQL .....	7
Server 2000.....	7
Server 2005.....	7
MSDE.....	7
MSN	
Gateway configuration parameters .....	29
IM Networks Proxy Accounts .....	11
proxy configuration.....	28
required hosts/ports .....	5
OCS	
firewall settings.....	5
Gateway configuration parameters .....	30
IM Networks Proxy Accounts .....	11
LDAP Authentication Gateway.....	10
Server 2007 interoperability .....	32
Oracle .....	7
parameters	
account_creation.....	33
account_type.....	33
ADManager.ini .....	20
BuddyListSync .....	31
ColumnSeparator.....	20
dllname .....	33
FirstIniFile .....	20
FullName.....	23, 34
getstatusmessage .....	29, 30
HostX .....	22, 33
infomsgs.....	29
LdapAuthentication.ini.....	21
MethodX.....	22, 33
NameY .....	20, 21
newmailnotification.....	29, 30
PassY.....	21
PathYX.....	20, 21
PortY .....	21
PropEX.....	21

PropMX .....	20	hardware configuration (evaluation only) .....	5
ProxyY .....	21	hardware configuration (recommended) .....	5
rtcserveraddress .....	28, 31	network for server .....	5
rtcserverport .....	31	software .....	5
SecondIniFile .....	20	Reuters Messaging	
serveraddress .....	28, 30	firewall settings.....	5
serverport.....	30	Gateway configuration parameters .....	31
ServerY .....	21	IM Networks Proxy Accounts .....	11
service_name.....	33	required hosts/ports .....	5
set_proxy_password_domains.....	22	Server interoperability .....	32
showblockeduser .....	30	Sametime	
SSLPortX .....	22, 33	firewall settings.....	5
stage .....	33	Gateway configuration parameters .....	31
tasklist.....	33	IM Networks Proxy Accounts .....	11
transport.....	30, 31	LDAP Authentication Gateway .....	10
typingnotification .....	29, 30	proxy configuration.....	28
UseDomainNTName .....	20	sections	
performance objects		ADMAUTH .....	22, 33
WM Gateway .....	26	Database.....	20
WM Server .....	26	LDAP.....	20, 22, 33
ports		PERFORMANCE .....	26
Add Domain dialog.....	15	security.....	34
AIM/ ICQ Gateway .....	29	Service Info .....	33
changing .....	5	SSL Proxy .....	29
firewall settings default (9000) .....	5	TRACKING.....	25
internal communication .....	34	Virtual PC .....	7
LCS Gateway.....	31	VMWare .....	7
LCS Server listening .....	31	Windows XP Professional Edition .....	7
LDAP section .....	22	WM Server Services .....	25
LDAPAuthentication.ini .....	21	WM User Manager .....	11
OCS Gateway .....	30	<i>wmpadmin</i> user.....	10
OCS Server listening .....	30	WMPlatform Administration Tool	
Reuters Messaging Gateway .....	31	Domain Management.....	39
Reuters Server listening.....	31	Property Management.....	39
SSL/TLS connection .....	33	User Management.....	35, 36, 37, 38
third-party required.....	5	Yahoo!	
RDBMS		Gateway configuration parameters .....	29
MS SQL .....	7	IM Networks Proxy Accounts .....	11
Oracle .....	7	proxy configuration.....	28
requirements		required hosts/ports .....	5