



MWI 2007 v.1.9.5

MWI Service for Microsoft Unified Messaging

System Manual

Last updated on: 11/20/2008



TABLE OF CONTENTS

OVERVIEW.....	4
References	4
SYSTEM ARCHITECTURE	5
MWI service	5
SECURITY PERSPECTIVE.....	7
SYSTEM OPERATION	9
Active Directory Connector	13
Exchange Connector	13
Pull strategy	13
Push strategy	14
SIP Gateway Connector.....	14
SMS Gateway Connector	14
WEB BASED ADMINISTRATION.....	15
Pausing the MWI Service	15
Activating MWI Service.....	16
CONFIGURATION.....	20
Active Directory Connector	20
Exchange Connector	21
SIP Gateway Connector.....	23
SMS Gateway Connector	24
LICENSING	27
REPORTING	29
Mail Notification Delay	29
MWI Change Time	29
Average Synch Time.....	30
Exchange Autodiscovery Response Time.....	30
Computer usage	31
SMS History.....	32
Email History.....	32
MWI Change History.....	33
TROUBLESHOOTING.....	35
Telephony Connectivity	35
GSM Connectivity	35
Alarm History	36
Event History	36
COMMAND LINE UTILITIES	38
SYSTEM LOGS	39



TEST ENVIRONMENT 40



Overview

The subject of this document is an application which extends the Microsoft UM solution with MWI service. The primary purpose of the underlying MWI application is to synchronize the user's voice-mailbox content and the lamp state on the user's physical phone. More precisely, if and only if the number of unread voicemails in the Exchange 2007 mailbox is greater than 0, the lamp will be lit.

Geomant support

Geomant provides e-mail support for questions and problems with MWI 2007. The support email address is

mwi-support@geomant.com

For additional information see the Geomant Web site:

<http://www.mwi2007.com>

References

This document is strongly based on information coming from several external sources. All of them can be found in the following documents:

- [1] MWI2007 - Design Document – MWI Service for Microsoft Unified Messaging – Detailed Design
- [2] RFC 3261 – SIP: Session Initiation Protocol
<http://www.ietf.org/rfc/rfc3261.txt?number=3261>
- [3] RFC 3842 – A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol
<http://www.ietf.org/rfc/rfc3842.txt?number=3842>
- [4] RFC 3458 – Message Context for Internet Mail
<http://www.ietf.org/rfc/rfc3458.txt?number=3458>
- [5] Intel NetStructure PBX/IP Media Gateway – SIP Compliance
<http://download.intel.com/network/csp/applnotes/8911app.pdf>
- [6] Intel NetStructure PBX/IP Media Gateway – User Guide – 2005 July
<http://resource.intel.com/telecom/support/pimg/manuals/1947-01.pdf>
- [7] AudioCodes – CPE Configuration Guide for Voice Mail
- [8] Mediant 2000 VoIP Media Gateway
http://www.audiocodes.com/objects/mediant2000_wireline.pdf
- [9] Cisco CallManager Administration Guide
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sys_ad/5_0_1/ccmcfg/bccm.pdf



System Architecture

The MWI solution has the following main software components:

- *MWI service* performing core operations (polling Active Directory and Exchange mailboxes, sending MWI requests to IP gateways, communicating with SMS gateways);
- *Web-based administration* application used to configure, monitor the MWI service and perform troubleshooting actions;

These 2 components communicate via the *.NET remoting* as depicted in Figure 1. Because of this, they can be installed on separate hosts.

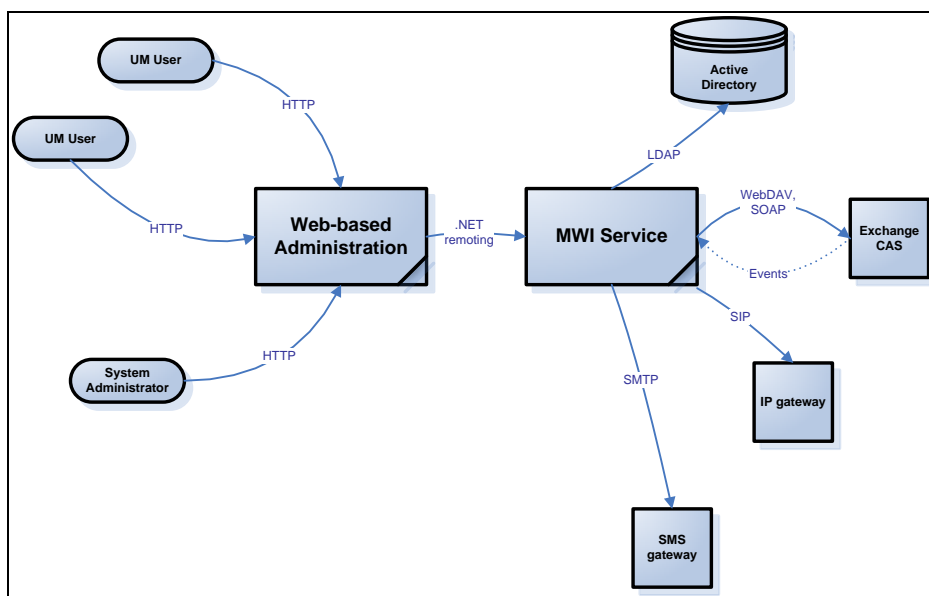


Figure 1. Software architecture

The complete application is written in managed code (C#). It requires Microsoft .NET Framework 2.0.50727 or above.

MWI service

The core component of the system is the MWI service. It manages the system configuration, licensing, log handling and offers administrative, maintenance and reporting interfaces for other components. It initializes and maintains references to each connector instances and determines their lifetime.

This executable one is linked to several dynamic linked libraries containing the special purpose connectors. Each connector is implemented in a different assembly. Connectors are classified as follows:

- *Active Directory Connector* to retrieve UM related configuration data from the Directory Service;
- *Exchange Connector* to detect state changes in mailboxes of MWI enabled UM users;
- *SIP Gateway Connector* to communicate with IP gateways and perform all of the MWI related VoIP signaling;
- *SMS Gateway Connector* to send outbound SMSs upon the occurrence of certain events;

As Figure 2 indicates, the MWI service hosts an ASP.NET web service. This web service receives call-back events from Exchange client access servers.

The connector implementations completely hide the underlying communication protocols from the core service. The specified connector interfaces ensures that the core system is not affected by changes to vendor gateways or vendor specific protocol extensions. This makes the core system independent of the directory and mail access protocols.

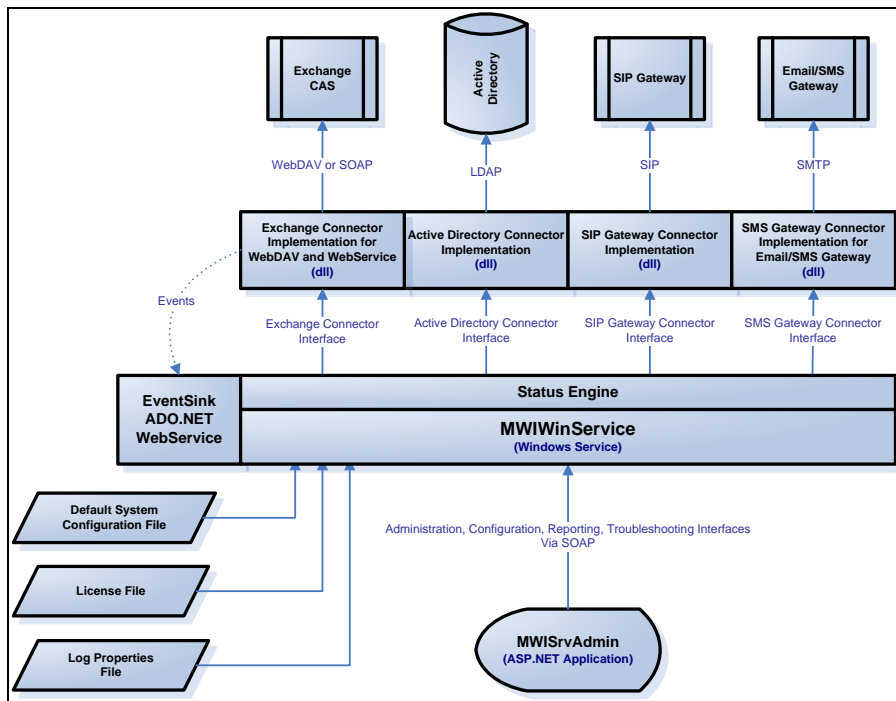


Figure 2. MWI service architecture

Security perspective

The user running the MWI service has to be an Exchange administrator and if the Dial out option is needed, UM-enabled.

Assuming the default system configuration, the following credentials have significant roles (Figure 3):

- User credentials used to access the administrative web forms (*MWIUserCredential*);
- The credential used by the IIS to execute the web application (*MWIWebAppCredential*);
- The credential used by the SCM to execute the MWI service (*MWIServiceCredential*);

The MWI solution uses the *Integrated Windows authentication* feature of the IIS to authenticate users who try to access the administrative, monitoring and troubleshooting web forms. The web application authorizes the authenticated users by retrieving the *MWIUserCredential* from the IIS and checking their AD group memberships. The web application distinguishes 3 application level roles:

- *MWI system administrator*: the required AD group membership can be configured in the web application configuration file. Users having this application level role can perform any administrative, monitoring and troubleshooting tasks;
- *MWI user administrator*: the required AD group membership can be configured like system administrators. This is let the one to administrate the UM users, but the service engine cannot be reached.
- *Simple UM user*: meaning UM enabled AD users. Users having this application level role can activate/inactivate their subscription for the MWI service. Note that the existence of this application level role can be disabled in the web application configuration file;

To check the AD group membership of *MWIUserCredential*, the *MWIWebAppCredential* should have permissions to perform the corresponding AD queries.

TCP channels between the web application and the MWI service are authenticated and encrypted communication channels (this fact has only relevance if the 2 components are installed on different machines). The MWI service authorizes each incoming connection by checking the remote endpoint from which the connection is trying to be established and the Windows identity of the remote endpoint. Allowed remote endpoints and identities can be configured in the configuration file of the MWI service. Generally this contains only one IP address (an IIS host where the web application is running) and the *MWIWebAppCredential*.

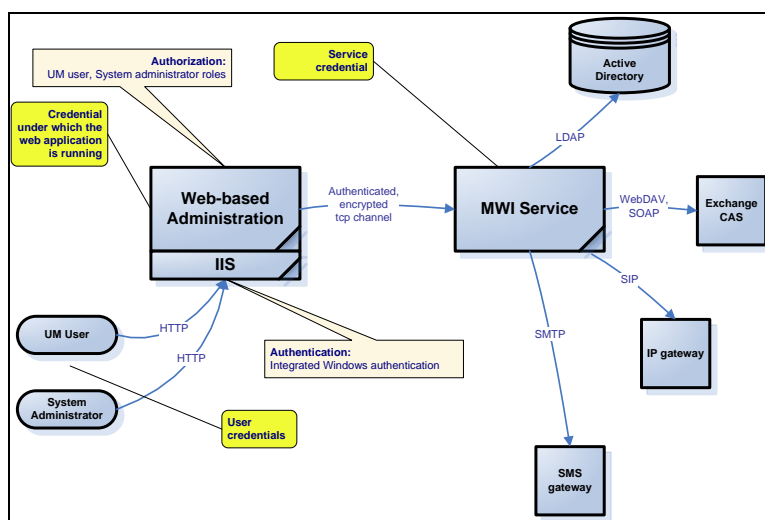


Figure 3. Security perspective

Summarizing, these features ensure that users are authenticated in the front-end and then that publicly available MWI service operations can be invoked only through trusted connections.

Finally, the following table lists all the permissions the above described credentials should have.



	Required permission
<i>MWIUserCredential</i>	In order to have the <i>MWI system administrator</i> role, a given AD user should be the member of the group specified in the configuration file of the web application (default is <i>Exchange Organization Administrator</i>). In order to have the <i>Simple UM user</i> role, a given AD user should be UM enabled.
<i>MWIWebAppCredential</i>	It should have permissions to <ul style="list-style-type: none"> • check AD user group membership; • write the <i>Logs</i> subdirectory of the web application install directory on the file system;
<i>MWIServiceCredential</i>	It should have permissions to <ul style="list-style-type: none"> • read UM configuration data <p><i>msExchUMHuntGroup, msExchUMIPGateway, msExchUMRecipientTemplate, protocolCfgHTTPServer, msExchUMDialPlan, msExchUMRecipientTemplate</i></p> <p>from the AD <i>Configuration</i> partition. This require to have '<i>List Contents</i>', '<i>Read All Properties</i>' and '<i>Read Permissions</i>' permissions on the Configuration Naming Context and its sub-containers;</p> <ul style="list-style-type: none"> • read AD <i>User</i> object properties and store application level flags as <i>extensionData</i> attributes. This require to have '<i>List Contents</i>', '<i>Read All Properties</i>', '<i>Write All Properties</i>', '<i>Read Permissions</i>' and '<i>All Validated Writes</i>' permissions on the domain <i>User</i> container and its sub-containers; • read the Exchange mailbox of each UM enabled AD user; • create search folders in the Exchange mailbox of each MWI enabled UM user; • host the ASP.NET Webservice called <i>MWIEventSink</i>. This 'MWI service hosted' application is used to receive event notifications from Exchange CASs; • write access to the install directory of the MWI service on the file system;

Table 1. Required permissions



System Operation

At system startup, the core service loads the following files:

1. The system configurations file from the *conf* subdirectory. The entire MWI specific configuration is stored in an XML file called *geomant.mwi.config.xml*. The MWI system is shipped with a default configuration file whose content can be changed:
 - by using a text editor if the MWI service is not running;
 - via the web administration forms if the MWI service is already running;

All changes via the web forms are sent directly to the core service and take effect immediately. Additionally, the service updates the configuration file with each configuration change. The schema file belonging to this configuration file is called *geomant.mwi.config.2006.02.01.xsd*. Table 2 describes the most important parameters of this configuration file. The last column indicates whether the given parameter should be initialized manually before starting up the MWI service;

Parameter section	Parameter name	Description	Default value in the file	Most probably should be changed
ActiveDirectoryConnector	Host	The fully qualified host name of the directory service. If no host is specified, standard DNS resolution is used to find directory service.	Nothing	No
	Port	The LDAP port of the directory service.	389	No
	Base DN	Base distinguished name to search in the directory service.	Nothing	Yes
	Append host	Specifies whether to append host names to DNs or not.	Yes	No
	Delegate	Flag to indicate whether to use integrated authentication (passing service credentials to AD for authentication) or not.	Yes	No
	Anonymous	Specifies whether to use anonymous access or not.	No	No
	User	Explicit user name for AD authentication. Use only if delegation and anonymous access is disabled.	Nothing	No
	Password	Explicit user password for AD authentication. Use only if delegation and anonymous access is disabled.	Nothing	No
	Domain	The fully qualified domain name of the given explicit user account. Use only if delegation and anonymous access is disabled.	Nothing	No
	Encrypt	Specifies whether to use data encryption or not.	No	No
	Sign	Specifies whether to use digital signature or not.	No	No
	Refresh period	The period length (in seconds) to synchronize internal state to AD.	18000	No
	Gateway list size	Length of the list of the IP Gateways	50	No
	Search filter	Search criteria of the LDAP query	(&(objectClass=user)(msExchUMEnabledFlags:1.2.840.113556.1.4.803:=1))	
ExchangeConnector	Protocol	The used Exchange access protocol. Implementation exists for 'WebDAV-Pull', 'WebService-Pull' and 'WebService-Push'.	'WebService-Push'	No
	Delegate	Flag to indicate whether to use integrated authentication or not.	Yes	No



User	Explicit user name for Exchange authentication. Use only if delegation and anonymous access is disabled.	Nothing	No
Password	Explicit user password for Exchange authentication. Use only if delegation and anonymous access is disabled.	Nothing	No
Domain	The fully qualified domain name of the given explicit user account. Use only if delegation and anonymous access is disabled.	Nothing	No
Default sender	The display name of a domain user acting as the sender of email notifications about critical conditions.	Nothing	Yes
Event sink IP	Local IP address used to receive push notification events from Exchange. This address is used to construct call-back URLs sent in push subscription requests. The first IP address in the local address list is used if nothing is specified.	Nothing	No
Event sink port	Local TCP port used to receive push notification events from Exchange. This port is used to construct call-back URLs sent in push subscription requests.	15201	No
Create VM folder	Specifies whether to create a separate search folder for voicemails or use the UM created one.	No	No
Exchange VM folder	The display name of the voice mail search folder created by UM. The display name is language dependent.	'Voice Mail'	No
Secure layer	Specifies whether IIS virtual directories on client access servers can be accessed without SSL or not. Generally, no SSL is required in test environments. On the other hand, almost each production environment requires secure connection.	Yes	No
Impersonate user	Specifies whether to impersonate an UM user on the client access server before accessing his mailbox.	No	No
Impersonate acces type	The Exchange Impersonation provides the following three methods to identify the impersonated account: the User Principal Name (UPN), the Security Identifier (SID) and the primary Simple Mail Transfer Protocol method.	SID	No
Enable Dial Out	Enabling dial out option. Available only from Exchange 2007 SP1.	Yes	Yes
Use Autodiscovery	Specifies whether to use Exchange Autodiscovery service or not.	Yes	No
Failure penalty	Penalty time in minutes in case of mailbox access failure.	10	No
Forced Exchange subscription	Re-subscription of all of the Exchange-users.	0	No



SIPGatewayConnector	Protocol	Default transport protocol used for SIP.	TCP	No
	Remote Port	Default remote port used for SIP.	5060	No
	Local IP	Local IP address included into SIP messages. The first IP address in the local address list is used if nothing is specified.	Nothing	No
	Use FQDN	Specifies whether to use fully qualified domain names or IP addresses in SIP messages.	No	No
	Use AD User Domain	Specifies whether to use AD user domain names in SIP request URIs and To headers.	No	No
	Local IP" value	Local IP address of the Exchange server included into SIP messages (in case of Server 2008).	Nothing	Yes
SMSGatewayConnector	Type	The type of the SMS gateway. Currently only two SMS delivery methods are supported: "Email/SMS gateway" and "Email/SMS gateway with DNS MX query". Each method encapsulates the SMS into MIME format and passes that to a remote endpoint through SMTP protocol.	'Email/SMS gateway'	No
	Destination DN	It meaning depends on the gateway type. For "Email/SMS gateway", this parameter specifies the fully qualified domain name of the SMS gateway host. For "Email/SMS gateway with DNS MX query", this parameter specifies the domain name used to retrieve MX records from the DNS.	Nothing	Yes
	Port	Default gateway access port.	25	
	From	The MIME 'From' header for outbound MWI related messages.	Nothing	Yes
	Subject	The MIME 'Subject' header for outbound MWI related messages.	Nothing	No
	Charset	The default character set for outbound MWI related messages.	'ISO-8859-2'	No
	Anonymous	Specifies whether to use anonymous access or not.	Yes	
	User	Explicit user name for authentication. Use only if anonymous access is disabled.	Nothing	No
	Password	Explicit user password for authentication. Use only if anonymous access is disabled.	Nothing	No
	Max SMS size	The maximum size (in bytes) of outbound messages.	160	No
	Notification text	Specifies the text being sent in e.g. SMS notifications.	Dear \$USER_DISPLAY_NAME\$, you have received a voicemail: \$VM_DATE_CREATED\$ (GMT) - \$VM_SUBJECT\$.	No
	Notification about missed calls	Specifies the text sent in SMS	Notification text on Missed Call" value="Dear \$USER_DISPLAY_NAME\$, you missed a call: \$MC_DATE_CREATED\$ (GMT) - \$MC_SUBJECT\$.	No
	Notification text on Fax	Specifies the text sent in SMS or Fax.	Dear \$USER_DISPLAY_NAME\$, you have received a fax message: \$FX_DATE_CREATED\$ (GMT) - \$FX_SUBJECT\$.	No
Enabling Out Of OfficeNotification	Enabling the SMS-sending option about being Out Of Office	Yes	No	
Specified Out Of Office Message	The text of the message sent in case of being out	Default	No	



	Text of the notification in case of being out of office	of office.Internal:specified internal message. External. specified external message Specifies the text of te message that will be sent to the caller, if the calle person's status is out of office	The person whose number (\$USER_DISPLAY_NAME\$, \$USER_EXTENSION\$) you have called is out of office between \$FROM\$ and \$TO\$. Your call has been registered in the user's mailbox.	No
Mapping rules	Start with	The rule concerns to the GSM-numbers starting with the given characters		Yes
	Truncation of the beginning	Deletes the first x characters of the GSM-number, where x is pre-defined	1	Yes
	Removing characters	Removes he specified characters	"-+()"	Yes
	Appending a prefix	Appends the specified characters to the beginning of the GSM-number		No
	Enabling SMS-.sending	Enabling SMS-sending from the numbers allowed by this rule	No	Yes
StatusEngine	Forced synch period	Time period (in minutes) to force phone lamp synchronization.	720	No
	Supervisor	The display name of an AD user who receives emails, SMSs upon critical failures.	Nothing	Yes
Static	Service port	TCP port for remote access.	15200	No
	Client hosts	Comma separated list of IP addresses from which client connections are accepted.	'*'	Yes
	Client identities	Comma separated list of client identities from which client connections are accepted.	'NT AUTHORITY\ NETWORK SERVICE'	Yes

Table 2. Parameters in the MWI service configuration file

- The property file for log details from the *log* subdirectory. This file contains details about log directories, log size constraints and log levels. Parameters in this file can be changed by using a text editor. Changes take effect only after restarting the service. Table 3 lists the most important parameters;

Parameter section	Parameter name	Description	Default value in the file
log4net.Appender.RollingFileAppender	File	Relative path to the current log file.	'log/MWIService.log'
	MaximumFileSize	Maximum size of a log file.	10000KB
	MaxSizeRollBackups	Number of archived log files.	3
Root	Level	Current log level.	DEBUG

Table 3. Most important parameters in the log property file

- The signed XML license file and its schema from the *lic* subdirectory. The license file is called *geomant.mwi.license.xml* while the schema file has the name *geo.license.2004.01.30.xsd*.

Parameter section	Parameter name	Description
Customer	Name	Customer name the license file is issued. The default is 'Temporary license' which can be used by everybody.
Host	Domain	Fully qualified domain name for which the license is issued. The default is an empty string – meaning that valid for every domain - for 'Temporary license'.
License	Volume size	Number of UM users for which MWI service can be activated at the same time. The default is 10 for 'Temporary license'.
Expiration	Volume expiration	The date of license expiration. The default is '2010-01-01' for 'Temporary license'.

Table 4. Most important parameters in the license file



If these steps are performed successfully, the service simply creates an instance from each type of connector and coordinates their operation according to the design document.

Active Directory Connector

The Active Directory Connector spawns only one working thread. This thread retrieves UM related configuration data from the Directory Service via LDAP. First of all, it checks the list of the UM IP gateways. Among others, it retrieves the following gateway attributes:

- Distinguished name;
- Display name;
- IP address;

If there is at least one gateway, the connector searches for the users for which UM service is enabled. For each such a user, it retrieves the following attributes:

- Distinguished name;
- Display name;
- Canonical name;
- Home mail database;
- Email address;
- Mobile number;
- UM dialplan link;
- Proxy addresses;

Based on the home mail database and the proxy addresses, it constructs the URL for email web access. If Exchange autodiscovery feature is configured and available on the intranet, then the MWI service ignores this value and turns to autodiscover in order to follow a more reliable CAS resolutions process. The outcome is an URL again which is used by the Exchange Connector to check the UM user's mailbox state. All of the retrieved data is stored in memory, it is not saved to the file system.

Also note that this resource consuming operation, namely collecting the required data for each UM enabled user is performed only at system startup. Afterwards, the working thread only performs attribute synchronization, searches for new users and removes existing ones from memory. The synchronization of the internal state and directory content is performed periodically, the length of these periods can be configured.

An AD user is assumed to be an active UM user if and only if the following LDAP condition is satisfied:
(&(objectClass=user)(msExchUMEnabledFlags:1.2.840.113556.1.4.803:=1)).

Exchange Connector

There are 2 Exchange Connector implementations currently: one of them uses WebDAV, the other one uses the new XML WebService interface as a mailbox access protocol. The WebDAV based implementation applies pull strategy for detecting changes in mailbox states. The second one may use a more sophisticated event based (push) strategy. By default, the XML WebService based solution is used by the MWI system.

Pull strategy

The Exchange Connector spawns multiple threads to create a fixed-size thread pool. Each of these threads performs the following operation: selects an MWI-enabled UM user and checks its mailbox state. It should be emphasized that only mailboxes belonging to MWI enabled UM users are checked. For pull strategy the minimum interval length between 2 consecutive mailbox polls can be configured. If it has already elapsed, then the time taken from the last mailbox check determines the priority of selecting the given user to perform the next check. So, the system tries to achieve an even mailbox polling rate for each MWI enabled UM user.

The WebDAV based connector implementation searches for emails based on the content class and the email flag indicating whether the email is new or not. It may retrieve the subject and the creation date of each such an email. These 2 email properties are used to construct the content of the outbound SMS, if the SMS service is enabled for the UM user. So these email properties are retrieved only if SMS notification about new voicemails is activated for the user.

The following query string is used to create search folders for MWI enabled UM users:



```
SELECT "DAV:displayname", "DAV:creationdate", "urn:schemas:httpmail:subject"  
FROM Scope ('deep traversal of [emailWebURI/inbox]') WHERE "DAV:contentclass" = 'Voice-CA'  
AND "urn:schemas:httpmail:read" = false
```

The search folder is called **'Unread Voicemails'** and is created in the user's message root folder. If an error code is received from the Exchange CAS – indicating that the folder does not exist – the Exchange Connector automatically creates that. When the MWI service is disabled for a given user, the search folder is deleted. Since the pull strategy might be very resource consuming, please use it only with small UM user population and only in test environment.

Push strategy

The new XML WebService based Exchange Connector implementation may use a more sophisticated event based solution. When the MWI service is activated for a given UM user, a subscription request is sent to the proper Exchange CAS. During an active subscription period, events are received from the CAS. These events indicate changes in the user mailbox state. Subscriptions are issued in order to receive the following types of events from voicemail search folders: 'Modified event' and 'Created event'. The former is used to update in-memory message counters; the latter may be used to send SMS notifications. Notification events are received by the MWI service through a self-hosted ASP.NET web service called *MWIEventSink*.

SIP Gateway Connector

The SIP Gateway Connector may also spawn multiple threads. However, its thread pool size is dynamic. The connector spawns a thread for each gateway port allocated for the MWI service. The number of MWI ports can be specified on the web administration forms.

A given thread selects an MWI enabled UM user for which the supposed MWI lamp state is not in synch with the mailbox state, constructs a SIP NOTIFY [REF.3] message and sends it to the proper gateway via TCP. The default TCP port for each gateway is 5060, but can be changed via the web administration forms. The next UM user is not selected by the same thread until all the required SIP responses are received for the previous request. The exact FSM related to the operation is included in the design document.

The SIP Gateway Connector may use vendor specific SIP protocol extensions to address specific gateway ports. It manages SIP SUBSCRIBE requests coming from gateways. Some vendor requires subscription before accepting NOTIFY messages, some do not.

Regarding those users whose supposed MWI lamp state is not in synch with the mailbox state, the time taken from the last lamp state change determines the priority of being selected. So, again the system tries to achieve fair operation.

Regardless whether the supposed lamp state is in synch or not, the SIP Gateway Connector periodically synchronizes each lamp state. The length of this period can be configured in the web administration forms.

SMS Gateway Connector

The SMS Gateway Connector spawns only a single working thread. This thread checks the FIFO queue containing outbound SMS requests and sends the one from the head of the queue.

Currently only Email/SMS gateways are supported, where the connector implementation simply sends the SMSs in email forms via SMTP.



Web based administration

The web administration is implemented as an ASP.NET web application. The web application communicates with the core MWI service through .NET remoting. It uses TCP channels, authenticates itself and encrypts the communication. By default, port 15200 is used to open communication channels (see Table 5).

Parameter section	Parameter name	Description
Configuration	MWIServiceHost	The host name or IP address of the machine where the MWI Service is running. The default value is the 'localhost'.
	MWIServicePort	The TCP port on which the MWI Service is listening for client connection attempts. The default value is 15200.
	AdminMembership	An AD group name. Each AD user being member of this group have <i>MWI system administrator</i> role. The default value is 'Exchange Organization Administrators'.
	CreateLog	A Boolean value which specifies whether the web application should generate log entries or not.

Table 5. Application level parameters in the web.config file

The web application can be accessed either by users having *MWI system administrator*, *MWI user administrator* or *Simple UM user* role. Users having the first type of role can use the whole administration, configuration, reporting, troubleshooting functionalities. User administrators can administrate users, have access some of the troubleshooting features, but can only view the engine state. Simple UM users can only activate/deactivate their MWI service.

To be able to use the dial out option, the user who runs the application should be UM-enabled.

In the following pages, several screens are included from the web administration application. Although a detailed description can be found in the user manual, some of them – especially the ones related to the system configuration – may help to give more insight into the system operation.

Pausing the MWI Service

On the screen depicted in Figure 4, the system administrator can suspend the operation of the MWI service without stopping the service itself. This action results in pausing working threads in each connector instance. After doing this, Exchange, Active Directory, SIP gateway and SMS gateway related maintenance can be performed conveniently.

- [-] Administration
- MWI Service
- MWI Users
- [+] Configuration
- [+] Information
- [+] Real-time Report
- [+] Historical Report
- [+] Troubleshooting

PRODUCT INFORMATION

Product Name	MWI SERVICE FOR EXCHANGE 2007	Company Name	MWI2007 - GEOMANT
Current Version	1.9.5.0	GR Version	1.9.5.0
Domain locked	GEOMANT.COM	Licensed to	CORPORATE NAME
License expires	1/1/2020	Number of licenses	10000 USERS AND 5 SERVERS
Support expires	1/1/2020	Support type	1 (SUPPORT TYPE 0: NONE, 1: TIER1-2, 2: TIER3-4)
Email Address	SOFTWARE.DEVELOPMENT@GEOMANT.COM	Current SMS balance	1917.9
Current State	RUNNING	State Since	8/28/2008 2:41:17 PM
Memory Usage	152 MB	CPU Usage	1 %
Host Name	EXCH-W0	Uptime	5 DAYS 02:30:24
UM users	65	MWI users	58
MWI OFF	339	MWI ON	120
Messages sent	459	SMS sent	30

Pause Service

Figure 4. Pausing the MWI service

Activating MWI Service

The MWI Users menu item (Figure 5) in the main menu lists the available UM users and some of their system maintained properties. The supposed MWI lamp states are indicated graphically by using the following icons:

Icon	Internal state	Description
	ST_INIT	Initial state at system startup, the state of the MWI lamp is unknown.
	ST_OFF_NO_ACK	SIP NOTIFY with 'Messages-Waiting: no' is sent to the gateway, but no response is received yet.
	ST_OFF	Response with success code is received for previously sent SIP NOTIFY (with 'Messages-Waiting: no').
	ST_ON_NO_ACK	SIP NOTIFY with 'Voice-mail-Messages-Waiting: yes' is sent to the gateway, but no response is received yet.
	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Voice-mail-Messages-Waiting: yes').
	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Missed call -Waiting: yes').
	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Fax-Messages-Waiting: yes').
	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Fax-and Voice-mail-Messages-Waiting: yes').







	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Fax- and Missed call -Waiting: yes').
	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Voice-mail- and Missed call -Waiting: yes').
	ST_ON	Response with success code is received for previously sent SIP NOTIFY (with 'Voice-mail -, Fax_ and Missed call -Waiting: yes').
	ST_INIT_TEST	Starts the test mode.
	ST_ON_TEST	Lamp On test – turns the user's lamp on and keeps it like that till the end of the test mode.
	ST_OFF_TEST	Lamp Off test – turns the user's lamp off and keeps it like that till the end of the test mode.

Table 6. Icons indicating phone different lamp states

If there is some problem with a user, the lamp-state column is constantly white.

Another warning sign is when the background color of the user's side is mauve (Figure 5). This happens in the following cases:

- the subscription is wrong
- the user is MWI-enabled, but cannot receive any kind of message because of the settings (there are no messages allowed)
- access to the user's account in the AD is denied
- the user doesn't exist
- the password is not valid (the user cannot log in)
- in INIT state (because it's not a good sign when a user remains in INIT state on the long term)

The so-called flying windows that you occasionally can see report the state of the user and errors, as shown on the figure below.



CURRENTLY AVAILABLE UNIFIED MESSAGING USERS

Refreshed: 2008.09.02 17:10:51 Page size: 10 50 100 250 500 1000 ALL Searching Criteria: [Unspecified]
 Refresh now Refresh time: 30 150 300 seconds Column's visibility: all default user
 Users: 0/62

Lamp	VM / F / MC / CA	Display name	E-mail	Extension1	Extension2	GSM Number	MWI Service Enabled	MWI on Voicemail	MWI on Fax	MWI on Missed Calls	MWI on Custom Action
	0/0/0/-	ALFRED SKRZEPKOWICZ	ASKRZEPKOWICZ@GEOMANT.COM	3320@HU_INTEL	NOT SET	+36 70 455 3320	YES	YES	YES	YES	NO
	0/0/0/-	ANTONIN DASTYCH	ADASTYCH@GEOMANT.COM	260@INVALID	NOT SET	+420 602 340 409	YES	NO	NO	NO	NO
	0/0/1/-	BRUCE END	BRUCEEND@GEOMANT.COM	3344@HU_INTEL		5 3344	YES	YES	YES	YES	NO
	0/0/0/-	BRYAN FERENC	BFERENC@GEOMANT.COM	3304@HU_INTEL		5 3304	YES	YES	YES	YES	NO
	0/0/0/-	BRUKA BROSZKA	BRUKAB@GEOMANT.COM	3302@HU_INTEL	NOT SET	+36 70 455 3302	YES	YES	YES	YES	NO
	-/-/-/-	CZARDESI	CZARDESI@GEOMANT.COM	9911111@HU_INTEL	NOT SET	[UNSPECIFIED]	NO	NO	NO	NO	NO

Figure 5. Flying windows providing state infos

MWI service for a given UM user can be activated/deactivated by clicking on the display name.

UNIFIED MESSAGING USER PROPERTIES

John Smith

Distinguished Name	CN=JOHN SMITH,CN=USERS,DC=GEOMANT,DC=COM		
Display Name	JOHN SMITH		
Logon Name	JSMITH		
Email Address	JSMITH@GEOMANT.COM		
Principal name	JSMITH@GEOMANT.COM		
User's AD account	ENABLED		
User's SIP address	SIP:JSMITH@GEOMANT.COM		
User's OCS presence		DO NOT DISTURB	
Last OCS Presence change	9/3/2008 4:11:35 PM		
Since this presence	00:00:06 (PREVIOUS PRESENCE: AVAILABLE)		
Email WebDAV Access	HTTPS://EXCH-HQ.GEOMANT.COM/EXCHANGE/JSMITH		
Email WebService Access	HTTPS://EXCH-HQ.GEOMANT.COM/EXCHANGE.ASMX		
Primary extension	3354	SIP Gateway	HU_Intel
Gateway Port	0		
Fax Messages	0	Missed Calls	0

Figure 6. User properties



To activate the MWI service an IP gateway should be specified. Each MWI request related to the user is sent to the given gateway.

The user's SIP-address, OCS-presence, the date of the last change of the state and the elapsed time since the last login will be shown only if the OCS Integration is set on (please see it below).

Besides activating the MWI service, the administrator can specify whether to send SMS notifications about new voicemails or not. Each SMS notification has the following form:

"Dear [User Display Name], you have received a voicemail: [Voicemail Creation Time] – [Voicemail Subject]"

The voicemail subject contains the length of the voicemail and may contain the caller's name or simply the calling number. It depends on the caller's identity.

Each of these 3 user parameters (**SIP Gateway, MWI Service Enabled, SMS on Voicemails**) are stored by the Active Directory Connector as user extension data attributes (*msExchExtensionData*) in the Active Directory.

The User has the possibility to test the extensions (practically a PBX-test). It is possible by using the icons at the end of the extension-row:

- Lamp On test – turns the user's lamp on and keeps it like that till the end of the test mode
- Lamp Off test – turns the user's lamp off and keeps it like that till the end of the test mode
- End lamp test – end the test mode by regenerating the lamp state based on the MWI-events

The dial-out and the GSM row also allows the user to test the application by the icons to be found at the end of the row:

- The GSM-test sends a test message to the user's GSM-number (if there is any) ["MWI Test message" or the one that had been set under Troubleshoot/GSM Access].
To re-set the message, there has to be at least one successful sending to a valid (not necessarily existing) phone number [the application checks only the format of the number]
- The Dial out test dials the given number and plays the greeting message.

To carry out any modification, the user has to be MWI enabled.



Configuration

The configuration submenu enables the administrator to specify system parameters for each connector instance. Changing any of the parameters takes effect immediately. Each parameter change is sent to the MWI server directly, which starts to use the new value and saves changes to the local XML configuration file. Each configuration form provides help regarding the parameters. By moving the cursor above the name of a given parameter, the corresponding short description is automatically displayed.

Figure 7. Status Engine configuration

Figure 8 depicts the parameters belonging to the core service. These include a time interval length in minutes (**Forced Synch Period**) to force periodic synchronization of lamp states to mailbox contents. The second parameter (**Supervisor**) may specify the display name of a user receiving alarms via email or SMS on the occurrence of a critical condition.

OCS Integration is a brand new feature of the application. This feature allows you to get more information about the user: the SIP-address, the actual OCS-state, the last time when the user's state changed and the elapsed time since the user's state last time became available.

Active Directory Connector

The parameters related to the Active Directory Connector covers the following (see Figure 9): Directory Services host (**Host**), LDAP port (**Port**) and base distinguished name (**Base DN**). Some parameters are related to the LDAP authentication e.g. to use a given user name/password (**User, Password, Domain**) or delegate the credential under which the core MWI service is running (**Delegate**). Based on the value of the other parameters, the LDAP traffic can be encrypted (**Encrypt**) or signed (**Sign**). Finally the last parameter (**Refresh Period**) specifies the interval length of synchronizing the Active Directory content to the internal state.



Figure 8. Active Directory Connector configuration

Clicking to the **Start Synchronization to AD Contact** link, the user can instruct the MWI service to interrupt the current **Refresh period** and download IP gateways and UM user from the Active Directory immediately. Based on this parameter, the Active Directory Connector retrieves the IP gateways in the following way:

- If any directory service host is specified, the component connects directly to the given host. If no one is specified, directory services are resolved through the standard DNS procedure;
- The *configurationNamingContext* attribute is retrieved from the *rootDSE*;
- Starting from this directory entry, the component searches for gateways by using the query condition **(objectClass=msExchUMIPGateway)**;

UM users are retrieved in the following way:

- An attempt to retrieve UM users is carried out only if at least one IP gateway is found;
- If any directory service host is specified, the component connects directly to the given host. If none are specified, directory services are resolved through the standard DNS procedure;
- If a base DN is specified, the component searches for UM users starting from this directory entry. The query condition used for LDAP searching is described in section 'Active Directory Connector';

Note that, each LDAP URL is started with the value of the Host parameter if the **Append Host** parameter is set to true.

Exchange Connector

Figure 10 shows the parameters belonging to the Exchange Connector. This specifies which mail access protocol to use (**Protocol**); whether to use integrated authentication (**Delegate**) or use a specific user name/password (**User, Password, Domain**) when communicating with Exchange client access servers.



SETTINGS FOR EXCHANGE SERVER ACCESS	
Protocol	WebService - Push
Delegate	<input checked="" type="checkbox"/>
User	
Password	
Domain	
Default sender	
Event sink IP	
Event sink port	15201
Create VM folder	<input type="checkbox"/>
Exchange VM folder	Voice Mail
Secure layer	<input checked="" type="checkbox"/>
Impersonate user	<input type="checkbox"/>
Impersonate Access Type	SID
Enable Dial Out	<input checked="" type="checkbox"/>
Use Autodiscovery	<input type="checkbox"/>

Figure 9. Settings for Exchange Server access

The default sender parameter (**Default Sender**) may specify the display name of a domain user. Each email notification about critical system conditions will be sent on behalf of this user. The above mentioned user account should have permission to send emails on behalf of this domain user.

The event sink IP address (**Event sink IP**) and TCP port (**Event sink port**) is used to construct the call-back URL sent in each push subscription request. This is the URL through which the MWI service hosted ASP.NET web application accepts notification events from Exchange CASs. If no particular IP address is specified, then the first address from the local IP address list is used.

The **Create VM folder** specifies whether to create a separate search folder for voicemails or use the UM created one. If it is unchecked, the MWI service subscribes to the UM created search folder in order to receive notifications. Otherwise, the service creates a separate search folder called "Unread Voicemails" in the message root and subscribes to that. The voicemail search folder (**Voicemail search folder**) created by Exchange is called "Voice Mail". Note that the name of this folder might be language dependent. The next parameter (**Secure layer**) specifies whether accessing IIS virtual directories on client access servers requires SSL or not. Secure connections are required in almost every production environment. However, test environments generally offer unsecured access to these folders.

The **Impersonate user** specifies whether to instruct the client access server to impersonate an UM user before accessing his mailbox or not. If the parameter is set to yes, then each UM user's mailbox is accessed by using the UM user's credentials. So the MWI service account (or the account specified by the **User, Password, Domain** triplet if **Delegate** is set to no) should not have any permission on the UM users' mailboxes. The service account should have only permission to impersonate users on the client access servers and should have permission to impersonate UM users. If the Impersonate user parameter is set to no, then the MWI service account (or the account specified by the **User, Password, Domain** triplet if **Delegate** is set to no) should have *fullaccess* permission on the UM users' mailboxes.



Impersonate Access Type: the ExchangeImpersonation provides you the following three methods to identify the account as impersonated:

- the user principal name (UPN) method
- the security identifier (SID) method
- the primary simple mail transfer (SMTP) protocol access method

It is recommended to use the UPN method because it is the most stabil one (and the primary SMTP the most unstabil).

The **Enable dial out** allows you to use the dial-out function globally. If this is not allowed, all f the connected field on the user's side will appear in grey – in others words the settings cannot be modified (but testing is allowed) To enable dial out, the user who runs the service has to be UM enabled – and SP1 is a prerequisite. The last parameter (**Use Autodiscovery**) specifies whether to use Exchange Autodiscovery service or not. Please note that no Autodiscovery is required in a single domain test environment with only one client access server. However, Autodiscovery should be configured in more complex AD environment (thus this parameter should be set to yes).

SIP Gateway Connector

The SIP Gateway menu item depicted in Figure 11 lists the available IP gateways. This list comes from the Active Directory and maintained by the SIP Gateway Connector. For each gateway, the administrator can specify what type of transfer protocol to use (**Transport**); the default SIP port (**Gateway Port**) on the gateway; the number of ports (or channels) allocated for MWI on the given gateway (**MWI Ports**); whether unsolicited NOTIFYs are supported by the given gateway or SIP SUBSCRIBE is required (**Subscription**).

If the gateway supports unsolicited NOTIFYs, it is recommended to use this feature by leaving the Subscription flag unset. In this case the value of the Local Port parameter is ignored by the system.

SETTINGS FOR SIP GATEWAY ACCESS

Display Name	Transport	Gateway Port	MWI Ports	Domain Name	Outbound Proxy	Subscription	Authentication	Username	Password	Local Port
HU_INTEL	UDF	5060	5	Not available		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not available	Not available	5060
OCS	UDF	5060	1	Not available		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not available	Not available	5060
SPQMSIP	TCP	5060	1	Not available		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not available	Not available	5060

Update Gateways

Figure 10. SIP Gateway Connector Configuration

If IP gateways – used for MWI - in a given environment do not support unsolicited NOTIFYs, then the MWI solution and the Microsoft UM servers might have collocation problems. The ability of 2 systems to collocate depends on the available parameter set of the IP gateways (see Table 7).



	Separate IP address for the MWI server can be configured on the gateway	Separate IP address for the MWI server cannot be configured on the gateway
Separate SIP port for the MWI server can be configured on the gateway	MWI system & UM can collocate on the same host (using different SIP ports)	MWI system & UM can collocate on the same host (using different SIP ports)
Separate SIP port for the MWI server cannot be configured on the gateway	MWI system & UM should be located on different hosts	No such type of gateways are supported by the MWI system

Table 7. Collocation of the MWI and UM system

Please note that the MWI system supports only gateway level subscriptions. This means that – after gateway subscription – it sends MWI NOTIFYs with the given SIP call-id for each telephony extension.

It is important for the SIP Gateway Connector to know the number of gateway ports for several reasons:

- the connector starts a separate working thread to handle each gateway port;
- a given thread never sends the next MWI request until response is received for the previous one;

This system operation also applies to gateways using SMDI connections, or Q.SIG. For such gateways, the value of the **MWI Ports** parameter means logical channels instead of real PBX ports.

Please note that none of these gateway parameters are saved into the Active Directory. The MWI system maintains the current settings in a backup file (*[MWI home]\backup\geomant.mwi.backup.xml*). This design consideration was taken in order to avoid schema modification in the directory service.

SMS Gateway Connector

Finally, the last configuration submenu lists the parameters belonging to the SMS Gateway Connector. These are mainly related to SMTP access (**Destination DN, Port**), authentication (**Anonymous, User, Password**) and encoding (**Charset**).

Figure 11. SMS Gateway Connector configuration

If you set the “Geomant Sms Center” option by the “Type” field, most of the options that you can see listed on this site, will become unavailable, as they would make no sense in case of this setting. (Please note that after changing the Type field you have to submit the change and then you can change the optional parameters)

Currently, only email/SMS gateways are supported. Messages are transmitted to SMS gateways through SMTP. There are 2 methods to resolve SMTP server address:



- ✓ If the **Type** parameter is set to "Email/SMS gateway" then the **Destination DN** should specify either the fully qualified domain name or the IP address of the SMTP server;
- ✓ If the **Type** parameter is set to "Email/SMS gateway with DNS MX query" then the **Destination DN** should specify a domain name. This domain name is used to retrieve MX records from the DNS. The MX record having the smallest preference number will determine the SMTP server address;

In both case, the MIME 'To' header is constructed as *[UM user's GSM number]@[Destination DN]*. The **From** and **Subject** parameters specify other MIME properties of emails sent to the SMTP server. The **Notification text** specifies the email body to be sent. In order to construct the email body based on the UM user's identity, the following parameters are available:

- USER_DISPLAY_NAME – UM user's AD display name;
- USER_EMAIL_ADDRESS – UM user's primary SMTP address;
- USER_EMAIL_ALIAS – UM user's email alias;
- USER_PHONE_EXTENSION – UM user's first extension;
- USER_PHONE_GSM – UM user's GSM number;
- USER_LOGON_NAME – UM user's Windows logon name;
- VM_DATE_CREATED – Timestamp when the voicemail is recorded by UM;
- VM_SUBJECT – Voicemail subject;
- VM_DATE_RECEIVED – Timestamp when the voicemail is delivered by Exchange;
- VM_DATE_SENT – Timestamp when the voicemail is sent by UM;
- VM_DISPLAY_CC – MIME 'CC' header in the voicemail;
- VM_DISPLAY_TO – MIME 'To' header in the voicemail;
- VM_IMPORTANCE – Voicemail importance;
- VM_SENSITIVITY – Voicemail sensitivity;
- VM_SIZE – Voicemail size in bytes;

Please note that only AUTH LOGIN type of authentication method is supported. There is no TLS support currently. No GSSAPI, NTLM or other Windows specific authentication methods are supported.

Mapping rules for phone numbers

The system offers the possibility to transform the phone numbers retrieved from the Active Directory (see Figure 13). Currently this transformation is applied only to the GSM phone numbers before sending SMS notifications to the MWI enabled UM users.



GSM NUMBER MAPPING RULES						
Starting With	Truncate Beginning	Remove Characters	Append Prefix	Enable SMS sending	Delete Selected Rules	
+420	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+44	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+361	1	..+0	[Empty]	<input type="checkbox"/>	<input type="checkbox"/>	
+3670	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+3630	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+3620	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+48	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
+41	1	..+0	[Empty]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="button" value="Update Selected Rules"/>					<input type="button" value="Create New Rule"/>	

Figure 12. Transforming phone numbers

Rules should be interpreted as follows: if a phone number starts with the string specified by the **Starting With** parameter, then the system applies the given rule. Applying a given rule means that

1. the number of characters indicated by the parameter **Truncate Beginning** will be deleted from the beginning of the phone number;
2. then the characters specified by the parameter **Remove Characters** will be removed from the result;
3. and finally the string specified by the parameter **Append Prefix** will be inserted into the beginning of the result;

If multiple rules could be applied to a given phone number then the system applies the most specific one.



Licensing

As previously described, the system is shipped with a signed XML license file. The content of this file can be displayed by using the License submenu. Beside of the customer information and software details, this license file contains only a simple volume license. The value of this license specifies the maximum number of UM users for which the MWI service can be activated at the same time and the maximum number of MWI2007 Vista Gadget users. The license file also contains the type of the MWI online support (none, tier1-2, tier3-4) and that the customer have ordered the MWI LogFile Viewer or not.

The license is linked to the domain name, so the MWI service can be installed on any host belonging to the given domain.

Category Name	Size	Expiration	Restricted to	Description
MM ENABLED UM USERS	10000	1/1/2020	GEOMANT.COM	NUMBER OF MM2007 USERS
MM SERVERS	5	1/1/2020	GEOMANT.COM	NUMBER OF MM2007 SERVERS
MM ONLINE SUPPORT	1	1/1/2020	GEOMANT.COM	SUPPORT TYPE 0:NONE, 1:TIER1-2, 2:TIER3-4
MM LOGFILE VIEWER	1	1/1/2020	GEOMANT.COM	LOGFILE VIEWER APPLICATION FOR MM2007
MM VISTA GADGET	10000	1/1/2020	GEOMANT.COM	NUMBER OF USERS OF MM2007 VISTA GADGET

YOUR LICENSE FILE HAS TO BE LOCKED TO THE FOLLOWING DOMAIN: 'GEOMANT.COM'.

[Order SMS Credits For Geomant SMS Center](#)

[Download Current License](#) [Order License](#)

UPLOAD A NEW LICENSE FILE [Tallózás...](#)

[Start Upload](#)

Figure 5. License properties

By pushing the **Download Current License** button, the current license file can be downloaded from the MWI service. The web form also offers the possibility to upload and activate a new license file. This procedure does not interrupt the MWI service.

You can order new license or sms-credits for sending sms-es by using the appropriate button.



The screenshot shows a web application interface with a navigation menu on the left, a central content area, and a form on the right. The navigation menu includes: Administration, Configuration, Information, License (highlighted), Real-time Report, Historical Report, and Troubleshooting. The central content area features the logo and the text "MESSAGE WRITING INDICATOR" above a list of links: Home, Downloads, FAQs, Help, Contacts, Partners, and Purchase license over PayPal. The form on the right contains fields for Date (2008-03-26 16:38:37), Company, Contact name, Phone, Invoicing details (Purchase Order Number, Company Name, Address, City, State/Area, Zip/Post Code, Country, Project Name/ID), SMS Username, and Quantity (100 USD). At the bottom of the form are "Reset form" and "Send form" buttons.

Figure 6. Download the current license file



Reporting

There are several graphical real-time reports. Each of these depicts the value of a given measured parameter in the moving average form. The moving average is calculated as

$$p[k+1] = a*p[k] + (1-a)*x[k+1]$$

where p is the moving average value of the parameter, x refers to the samples coming from the measurement. In normal circumstances the values of each of the following measured parameters should converge to its mean value.

Mail Notification Delay

The parameter value depicted in Figure 15 shows the average time elapsed between the mailbox state change and the time when the Exchange Connector is notified about such a change.

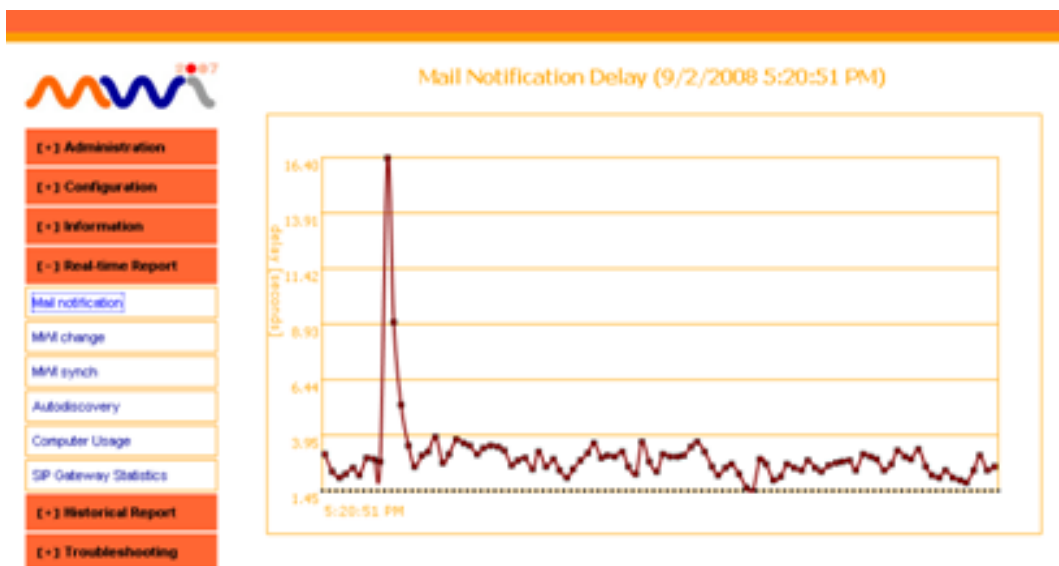


Figure 15. Mail notification delay

MWI Change Time

Figure 16 depicts the average time spent by the SIP gateway to answer NOTIFY messages. This parameter is strongly PBX and IP gateway vendor specific. The value of this parameter determines how many ports should be allocated for a given user population.

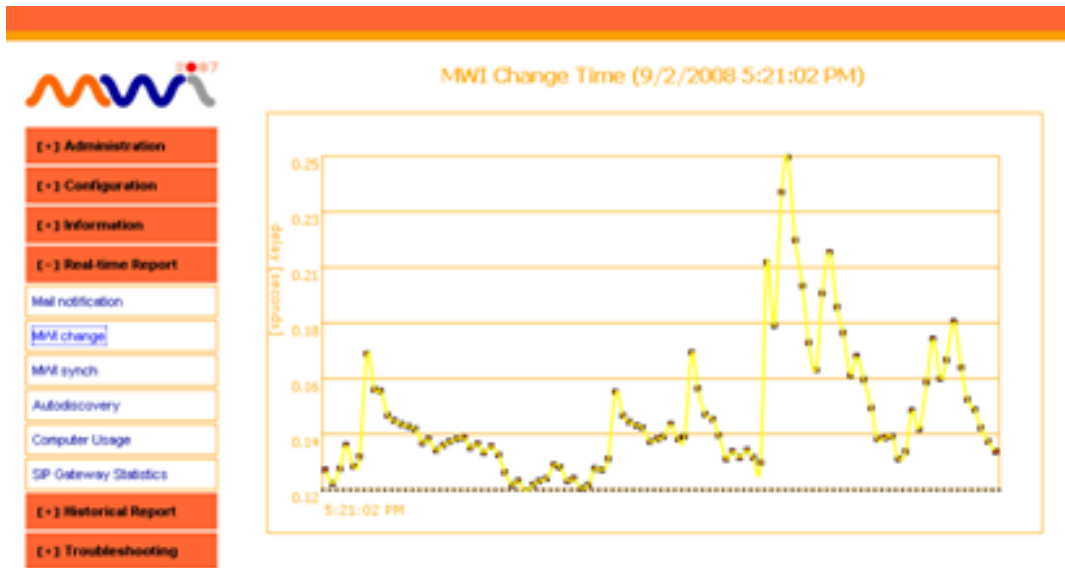


Figure 7. MWI change time

Average Synch Time

The next graphical report depicted in Figure 17 shows the average time taken to synchronize MWI lamp states to mailbox states. The depicted value shows the average time elapsed between notifying about mailbox state change and receiving response to the corresponding SIP request.

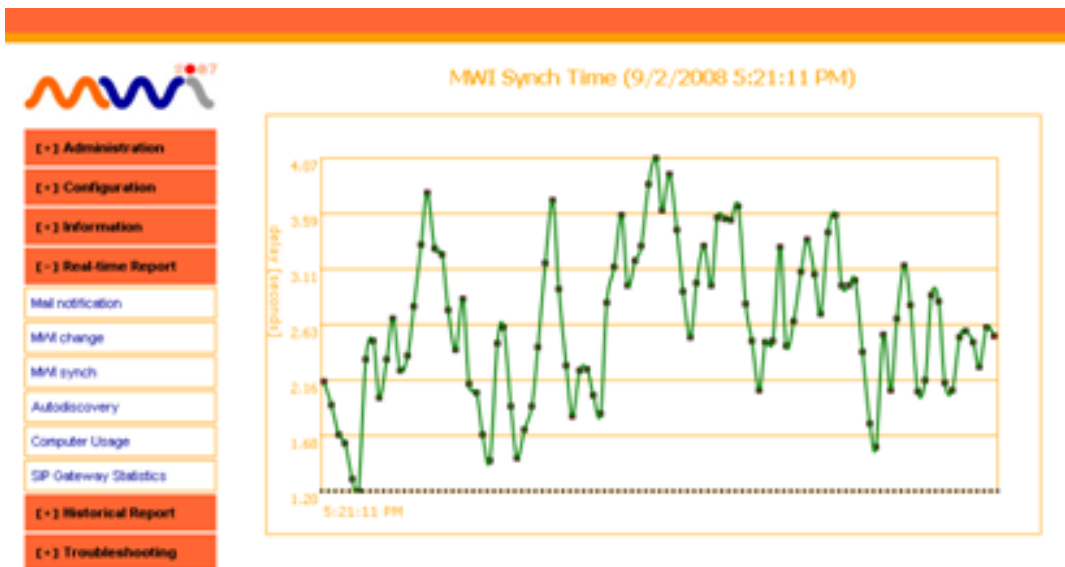


Figure 17. Average synch time

Obviously, the value of this parameter cannot be smaller than the one described in the previous section.

Exchange Autodiscovery Response Time

Another graphical report depicted in Figure 18 shows the average time taken to get response from the Exchange Autodiscovery service.

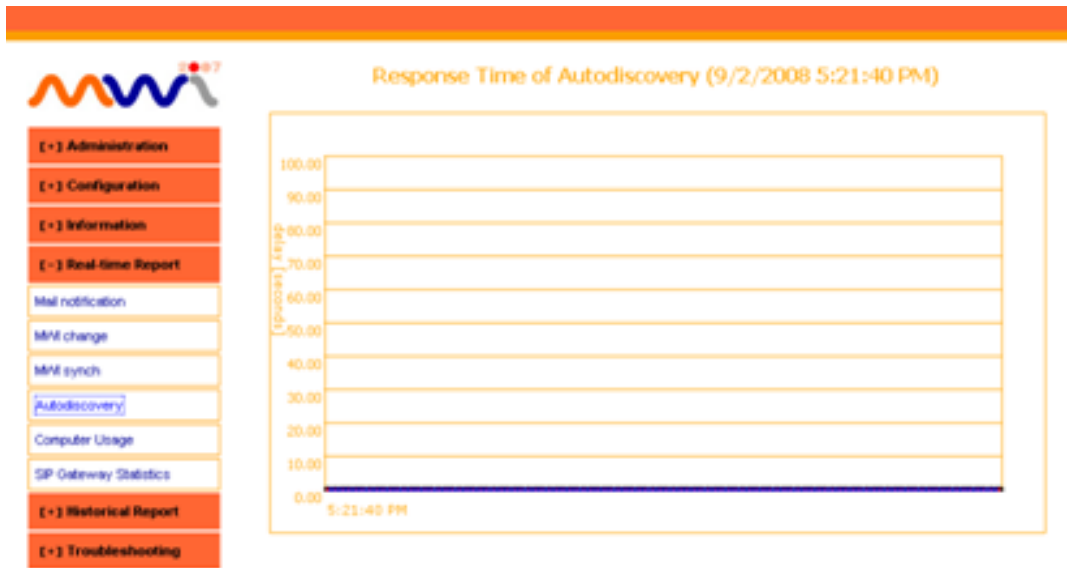


Figure 18. Average Autodiscovery response time

Computer usage

The final graphical report depicted in Figure 20 shows the average Central Processor Unit and Pagefile usage in percents.

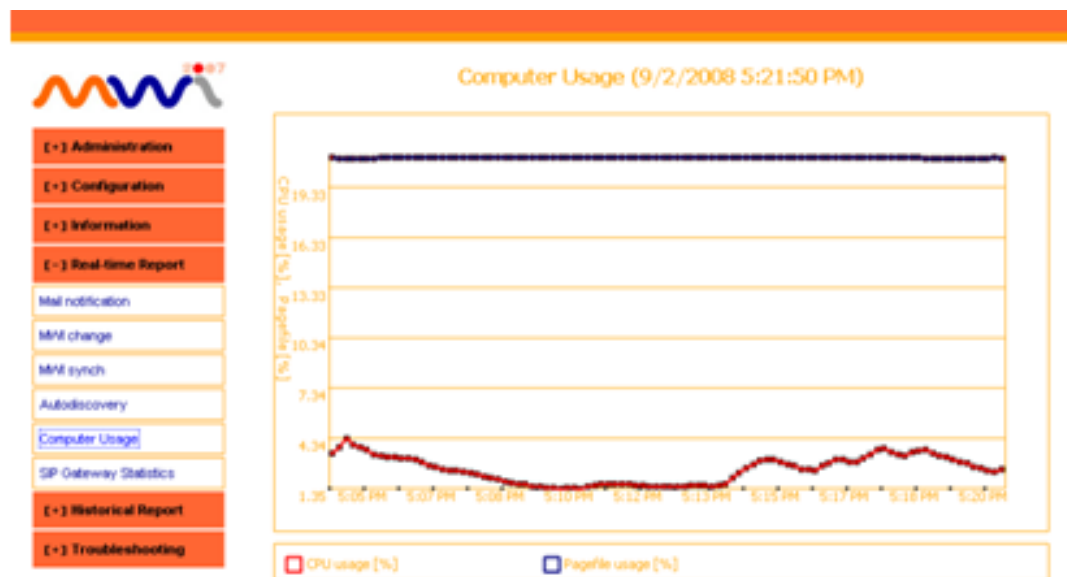


Figure 19. Average CPU-usage

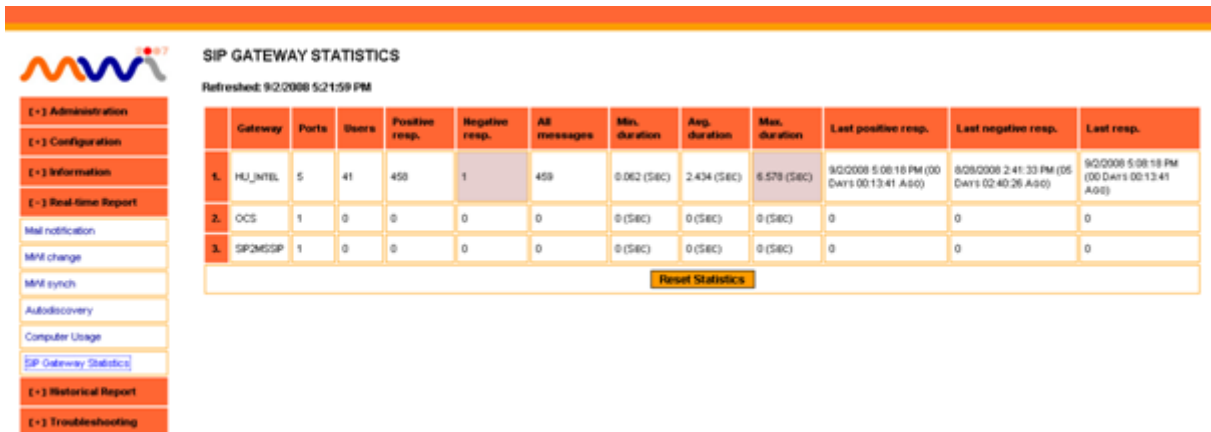


Figure 20. SIP Gateway Statistics

SMS History

The report shown in Figure 19 allows listing the most recently sent outbound SMSs. These messages are sent to MWI enabled UM users to whom SMS notification about voicemails has been enabled.



Figure 21. SMS history

The following types of outbound SMSs can be sent by the system:

- *MWI enabled UM users*: notifications about new voicemails;
- *Supervisors*: notification about critical system conditions;
- *Arbitrary GSM number*: message sent from the troubleshooting submenu;

Email History

The MWI system may send outbound emails to supervisors. These emails contain a short description of the failure condition.




Figure 22. Recently sent e-mails

	Gateway	Ports	Users	Positive resp.	Negative resp.	All messages	Min. duration	Avg. duration	Max. duration	Last positive resp.	Last negative resp.	Last resp.
1.	HU_MTEL	5	41	458	1	459	0.062 (SEC)	2.434 (SEC)	6.578 (SEC)	9/2/2008 5:08:18 PM (00 DAYS 00:13:41 AGO)	8/28/2008 2:41:33 PM (05 DAYS 02:40:26 AGO)	9/2/2008 5:08:18 PM (00 DAYS 00:13:41 AGO)
2.	OCS	1	0	0	0	0	0 (SEC)	0 (SEC)	0 (SEC)	0	0	0
3.	SPQMSSP	1	0	0	0	0	0 (SEC)	0 (SEC)	0 (SEC)	0	0	0

Figure 23. SIP gateway statistics

MWI Change History

The next historical report lists the most recently performed MWI change requests.



RECENTLY PERFORMED STATE CHANGES

Refreshed: 9/2/2008 5:22:35 PM

ID	Timestamp	Source	Content
30	9/2/2008 5:08:18 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: KEVIN ROSS EXTENSION: 3385 GATEWAY: HU_INTEL IS SWITCHED OFF
29	9/2/2008 5:06:52 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: KEVIN ROSS EXTENSION: 3385 GATEWAY: HU_INTEL IS SWITCHED ON
28	9/2/2008 4:37:42 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: KUN SZABOLCS EXTENSION: 3319 GATEWAY: HU_INTEL IS SWITCHED ON
27	9/2/2008 3:33:47 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: BIRKÁS BRIGITTA EXTENSION: 3302 GATEWAY: HU_INTEL IS SWITCHED OFF
26	9/2/2008 3:27:39 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: KRÁLL PÉTER EXTENSION: 3338 GATEWAY: HU_INTEL IS SWITCHED OFF
25	9/2/2008 3:27:24 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: BIRKÁS BRIGITTA EXTENSION: 3302 GATEWAY: HU_INTEL IS SWITCHED ON
24	9/2/2008 3:19:05 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: MEDYERI ATTILA EXTENSION: 3347 GATEWAY: HU_INTEL IS SWITCHED OFF
23	9/2/2008 3:15:58 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: MARY STEVENS EXTENSION: 3356 GATEWAY: HU_INTEL IS SWITCHED OFF
22	9/2/2008 2:41:37 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: FAX GEDONAI HU EXTENSION: 3398 GATEWAY: HU_INTEL IS SWITCHED ON
21	9/2/2008 2:41:24 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: TAKÁCS VIKTOR LAZLO EXTENSION: 3332 GATEWAY: HU_INTEL IS SWITCHED OFF
20	9/2/2008 2:41:24 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: JOHN SMITH EXTENSION: 3354 GATEWAY: HU_INTEL IS SWITCHED OFF
19	9/2/2008 2:41:24 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: KOVÁCS IMRE EXTENSION: 3314 GATEWAY: HU_INTEL IS SWITCHED OFF
18	9/2/2008 2:41:22 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: TUNKLI ATTILA EXTENSION: 3330 GATEWAY: HU_INTEL IS SWITCHED OFF
17	9/2/2008 2:41:22 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: VINCZE ANDRÁS EXTENSION: 3341 GATEWAY: HU_INTEL IS SWITCHED OFF
16	9/2/2008 2:41:22 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: MURKALÁZSLÓ EXTENSION: 3305 GATEWAY: HU_INTEL IS SWITCHED OFF
15	9/2/2008 2:41:21 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: BÁNYAI FERENC EXTENSION: 3304 GATEWAY: HU_INTEL IS SWITCHED OFF
14	9/2/2008 2:41:21 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: NEMAD JÓLAC EXTENSION: 3366 GATEWAY: HU_INTEL IS SWITCHED OFF
13	9/2/2008 2:41:21 PM	SP GATEWAY CONNECTOR	LAMP FOR USER: VÁGÁRHÉLYI ZSÓFIA EXTENSION: 3303 GATEWAY: HU_INTEL IS SWITCHED OFF

Figure 24. Lamp state change history

MWI lamp state can be changed for the following reasons:

- *MWI enabled UM users*: the number of unread voicemails is decreased to or increased above 0;
- *MWI enabled UM users*: periodic lamp state synchronization;
- *Arbitrary extension*: change request is issued by using the troubleshooting submenu;



Troubleshooting

The troubleshooting submenu allows administrators check telephony and GSM connectivity.

Telephony Connectivity

PBX connectivity (Figure 22) can be checked by selecting either a username or an extension:

- In case of the username, the system looks for the user:
 - o if it finds only one user, then navigates to her/his side – and there the test can be carried out the above written way
 - o in case there are more users who meet the search conditions, then a user list appears with the candidates – the right one can be selected manually
- If an extension is selected, then the system navigates to another side (which is similar to the above mentioned one) – where you have to give the gateway to the extension (you have to choose it from a list, which contains the system's every gateway), and tell if the lamp should be turned on or turned off. Then the „Test user“ changes the state of this lamp. The drawback of this method is that the user may not understand why his/her lamp's state has changed...That is why the proposed way of testing is to use the icons on the user's side.

The screenshot shows a web interface titled "TESTING TELEPHONY CONNECTIVITY". On the left is a sidebar menu with the following items: Administration, Configuration, Information, Real-time Report, Historical Report, Troubleshooting (highlighted), PBX Access, GSM Access, Alarms Raised, Event History, and Online Help. The main content area contains two input fields: "Username" and "Phone Extension". Below these fields is a yellow button labeled "Change Lamp State in Selected User".

Figure 25. Testing PBX connectivity

GSM Connectivity

The GSM connectivity can be checked by simply entering a destination GSM number and a message body. Some of the previous comments are also valid for GSM connectivity testing.



Figure 26. Testing GSM connectivity

Please note that a command line tool called **MWITestTool** is also available to test the telephony and GSM connectivity. This tool, similarly to the above described web interface, calls directly into the core service's assembly, thus, test instructions are performed by the same code executed in the real environment.

Alarm History

Besides testing the connectivity, the next 2 menu items may be very useful for finding the cause of error conditions. One of the menu items lists the alarms raised by different software components. Such alarms can be related to, for example, authentication failures or data integrity errors.

ID	Timestamp	Source	Category	Severity	Description
1	8/20/08 2:41:33 PM	SP GATEWAY CONNECTOR	SP GATEWAY ACCESS PROBLEM	ERROR	FAILED TO SWITCH ON THE MWI LAMP FOR THE USER: CN=KOUAC1 HUNDR,OU=USERS,OU=EDMANT_HJLDC+EDMANTDC+COM. SP RESPONSE INDICATING SERVER SIDE ERROR IS RECEIVED FROM THE GATEWAY. 192.168.0.91. CHECK THE LOG FILE FOR MORE DETAILS.

Figure 27. Raised alarms

Event History

The last menu item lists the most recent events. These events are related to normal system operation. This information covers how many UM users are retrieved from the Active Directory, how many new voicemails a given user has.



SERVICE EVENTS
Refreshed: 9/2/2008 5:23:26 PM Refresh time: 150 000 seconds

ID	Timestamp	Source	Content
30	9/2/2008 2:45:05 PM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF OCS USERS RETRIEVED FROM THE DIRECTORY: 122
29	9/2/2008 2:45:05 PM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF UM USERS RETRIEVED FROM THE DIRECTORY: 1675
28	9/2/2008 2:44:58 PM	ACTIVE DIRECTORY CONNECTOR	LDAP PAGE 1 - NUMBER OF UM USERS RETURNED: 67. DURATION: 0.5624784 SECONDS.
27	9/2/2008 2:44:57 PM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF IP GATEWAYS RETRIEVED FROM THE DIRECTORY: 3
26	9/2/2008 2:40:56 PM	USAGE STATISTICS	UM USERS: 1608, MN USERS: 58, 'ON' MSG: 116, 'OFF' MSG: 321, ALL MSG: 437, POSNED ACK: 436/1, SMS: 29, UPT: 119:59:53 (INCMSS)EVENTS: 312
25	9/2/2008 9:44:58 AM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF OCS USERS RETRIEVED FROM THE DIRECTORY: 122
24	9/2/2008 9:44:58 AM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF UM USERS RETRIEVED FROM THE DIRECTORY: 1608
23	9/2/2008 9:44:49 AM	ACTIVE DIRECTORY CONNECTOR	LDAP PAGE 1 - NUMBER OF UM USERS RETURNED: 67. DURATION: 0.2187416 SECONDS.
22	9/2/2008 9:44:49 AM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF IP GATEWAYS RETRIEVED FROM THE DIRECTORY: 3
21	9/2/2008 8:40:58 AM	USAGE STATISTICS	UM USERS: 1541, MN USERS: 58, 'ON' MSG: 101, 'OFF' MSG: 302, ALL MSG: 403, POSNED ACK: 402/1, SMS: 24, UPT: 113:59:54 (INCMSS)EVENTS: 255
20	9/2/2008 4:44:49 AM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF OCS USERS RETRIEVED FROM THE DIRECTORY: 122
19	9/2/2008 4:44:49 AM	ACTIVE DIRECTORY CONNECTOR	NUMBER OF UM USERS RETRIEVED FROM THE DIRECTORY: 1541

Figure 28. Event history

Both in the alarms and events page, the user can set the refresh time. This is 150 seconds by default, but it can be set to lower and higher value as well.

Figure 29. Log file analyzer



Command line utilities

Most of the administrative tasks - generally performed via the web based forms - are also supported through the command line. There are 2 options to perform command line administration:

1. Passing command line arguments to the executable *MWICmdTool*;
2. Starting the PowerShell shell, *MWI Custom Command Shell*, and executing *cmdlets*;

The following table lists the most important tasks which can be performed through the command line. The first column indicates the command line arguments which should be passed to the *MWICmdTool* executable in order to perform the given tasks. The second column indicates how to perform the same tasks in the *MWI Custom Command Shell* environment by listing the *cmdlets* to run.

Command line arguments (MWICmdTool.exe)	PowerShell alternative (MWI Custom Command Shell)	MWI service should be running?	Description
-MWIHelp	Get-MWIHelp	No	Displays help information
-Test MWISIPFunctionality -Standalone 0	Test-MWISIPFunctionality -IPGateway <IPGateway Display Name> -Extension <Phone Set Extension> -NumberOfVoicemails <Number of Unread Voicemails>	Yes	Tests SIP functionality by sending SIP NOTIFY messages to the required IP gateways.
-Test MWISIPFunctionality -Standalone 1	-	No	Tests SIP functionality by sending SIP NOTIFY messages to the required IP gateways.
-Test MWISMSFunctionality -Standalone 0	Test-MWISMSFunctionality -DestinationGSM <GSM number> -Message <Message Text>	Yes	Tests SMS functionality by sending messages to the required SMS gateways.
-Test MWISMSFunctionality -Standalone 1	-	No	Tests SMS functionality by sending messages to the required SMS gateways.
-List MWIIPGateways	List-MWIIPGateways	Yes	Lists IP gateways retrieved from the Active Directory.
-List MWIUMUsers	List-MWIUMUsers	Yes	Lists UM users retrieved from the Active Directory.
-List MWIServiceAlarms	List-MWIServiceAlarms	Yes	Lists recently raised alarms from the internal cache.
-List MWIServiceEvents	List-MWIServiceEvents	Yes	Lists recent events from the internal cache.
-List MWISentEmails	List-MWISentEmails	Yes	Lists recent emails from the internal cache.
-List MWILampStatusChanges	List-MWILampStatusChanges	Yes	Lists recent lamp state changes from the internal cache.
-Enable MWIService -UMUser <UMUser Display Name or Account Name> -IPGateway <IPGateway Display Name> [-Extension <User extension>] [-VM <yes no>] [-FX <yes no>] [-MC <yes no>] [-SmsOnVM <yes no>] [-SmsOnFX <yes no>] [-SmsOnMC <yes no>] [-OOF <yes no>]	Enable-MWIService -UMUser <UMUser Display Name or Account Name> -IPGateway <IPGateway Display Name> [-Extension <User extension>] [-VM <yes no>] [-FX <yes no>] [-MC <yes no>] [-SmsOnVM <yes no>] [-SmsOnFX <yes no>] [-SmsOnMC <yes no>] [-OOF <yes no>]	Yes	Enables MWI service for the given UM user.
-Disable MWIService -UMUser <UMUser Display Name or Account Name>	Disable-MWIService -UMUser <UMUser Display Name or Account Name>	Yes	Disables MWI service for the given UM user.
-Reset MWIService	Reset-MWIService	Yes	Disables MWI service for each UM user.
-Display MWIServiceInfo	Display-MWIServiceInfo	Yes	Displays MWI service information.
-Display MWIUMUserInfo -UMUser <UMUser Display Name or Account Name>	Display-MWIUMUserInfo -UMUser <UMUser Display Name or Account Name>	Yes	Displays the internal UM user record maintained by the MWI service.
-Display MWIIPGatewayInfo -IPGateway <IPGateway Display Name>	Display-MWIIPGatewayInfo -IPGateway <IPGateway Display Name>	Yes	Displays the internal IP gateway record maintained by the MWI service.

Table 8. Command line options

Please note that command line arguments are case-sensitive. Use "" to delimit parameters which contain white space characters. For example, to enable MWI service for the UM user called "Tom Stone" through the IP gateway called "Intel PIMG 1", you should execute

```
MWICmdTool.exe -Enable MWI -UMUser "Tom Stone" -IPGateway "Intel PIMG 1"
```

From the table above, it can be seen that there are several tasks which require the MWI service to run. Indeed these tasks are performed by the service itself. The *MWICmdTool* and the *cmdlets* use .NET remoting to connect to the MWI service. The remote endpoint to connect to is specified in the *MWICmdTool.exe.config* file. The TCP channels are encrypted. The connections are authorized by the MWI service similarly to the connections received from the web application. So, the hosts and credentials which are allowed to run commands are covered by the *client hosts* and *client identities* configuration parameters of the MWI service (see Table 2).



System logs

The system creates log files in the log subdirectory. Parameters for logging can be specified in the log property file. This includes the maximum log file size, size of log to maintain and the current log level. The system uses multiple log levels – specified in the design document –to help detection of more serious problems. These log levels are the following:

- INFO – normal system operation;
- FAILURE – incorrect configuration;
- ERROR – data integrity error, negative acknowledgements from gateways;
- CRITICAL – no correct functionality can be guaranteed by the system;

Log files contain the whole trace of SIP communication with the gateways.

Test Environment

Figure 26 depicts Geomant's test UM environment. This was created for proof of concept and functional testing purposes. The test environment connects to Geomant's live telephony network through 2 IP media gateways. The first gateway came from Intel [REF.5] and second one is from AudioCodes [REF.7]. The test environment also includes a 'Cisco subnet' with a CallManager [REF.9] and 2 IP phones.

Functional tests were performed in the following way:

- Between the Definity ECS and IP gateways, 5 gateway ports were allocated to perform MWI requests; the other 27 ports were used for UM calls;
- 25 Geomant employees were administered in the test AD domain as well and enabled UM and MWI service for them;
- A coverage path was configured in the Definity ECS to route redirected 'live' calls to the test UM system;
- Employees dialled into the test UM system to listen to voice mails or used OWA to download voicemails;

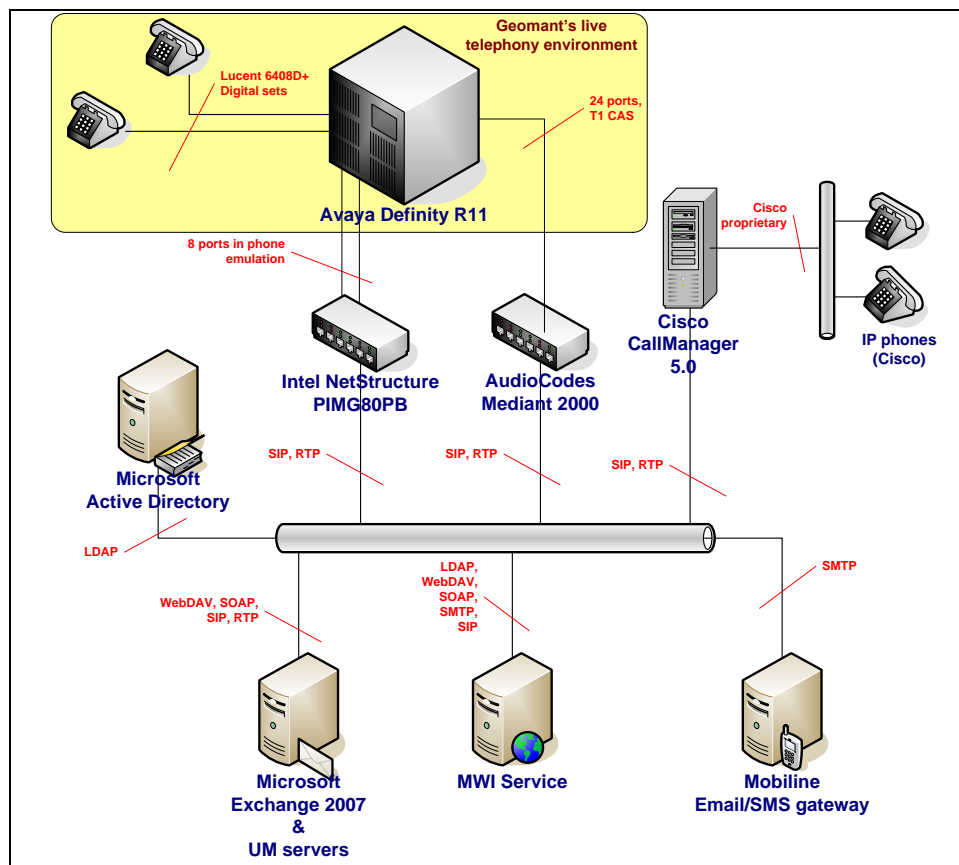


Figure 30. Current test environment



ABBREVIATIONS

AD	Active Directory
API	Application Programming Interface
ASP	Active Server Pages
CAS	Client Access Server
DN	Distinguished Name
FSM	Finite State Machine
IIS	Internet Information Services
IP	Internet Protocol
LDAP	Light-weight Directory Access Protocol
MWI	Message Waiting Indicator
OWA	Outlook Web Access
PBX	Private Branch Exchange
SCM	Service Control Manager
SID	Security Identifier
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
UDP	User Datagram Protocol
UM	Unified Messaging
URL	Unified Resource Location
VoIP	Voice over IP
WebDAV	Web Distributed Authoring and Versioning
XML	eXtensible Markup Language



LIST OF FIGURES

Figure 1. Software architecture.....	5
Figure 2. MWI service architecture	6
Figure 3. Security perspective	7
Figure 4. Pausing the MWI service.....	16
Figure 5. Flying windows providing state info.....	18
Figure 6. User properties.....	18
Figure 7. Status Engine configuration.....	20
Figure 8. Active Directory Connector configuration.....	21
Figure 9. Settings for Exchange Server access.....	22
Figure 10. SIP Gateway Connector Configuration.....	23
Figure 11. SMS Gateway Connector configuration.....	24
Figure 12. Transforming phone numbers.....	26
Figure 8. License properties.....	27
Figure 9. Download the current license file.....	28
Figure 15. Mail notification delay.....	29
Figure 10. MWI change time.....	30
Figure 17. Average synch time.....	30
Figure 18. Average Autodiscovery response time.....	31
Figure 19. Average CPU-usage.....	31
Figure 20. SIP Gateway Statistics.....	32
Figure 21. SMS history.....	32
Figure 22. Recently sent e-mails.....	33
Figure 23. SIP gateway statistics.....	33
Figure 24. Lamp state change history.....	34
Figure 25. Testing PBX connectivity.....	35
Figure 26. Testing GSM connectivity.....	36
Figure 27. Raised alarms.....	36
Figure 28. Event history.....	37
Figure 29. Log file analyzer.....	37
Figure 30. Current test environment.....	40



LIST OF TABLES

Table 1. Required permissions	8
Table 2. Parameters in the MWI service configuration file	12
Table 3. Most important parameters in the log property file	12
Table 4. Most important parameters in the license file	12
Table 5. Application level parameters in the web.config file.....	15
Table 6. Icons indicating phone different lamp states	17
Table 7. Collocation of the MWI and UM system	24
Table 8. Command line options.....	38