CommuniGate SYSTEMS

CommuniGate® Pro v5.1

Reviewer's Guide

January 2007

Outline

OUTLINE

I. INTRODUCTION

A. Purpose and Market Overview

This document provides a guide to help a "Reviewer" or evaluator experience key component areas of the CommuniGate Pro Internet Communications Platform™. At CommuniGate Systems, Inc., we strongly encourage the trial and evaluation of the product, and we are glad to assist in your server setup. Please contact support@communigate.com if you have any questions that are not answered in this document.

The CommuniGate Pro Internet Communications Platform™ is a server-based software solution and application platform for e-mail, collaboration, and voice over IP (VoIP). CommuniGate Pro provides a flexible, standards-based technology infrastructure for voice and data communication and collaboration, giving users the tools they need to conduct their business. A robust, easy-to-administer, full-featured, and secure messaging system increases the sophistication of business communications, while lowering administrative costs and reducing business risk.

CommuniGate Pro delivers advanced e-mail, collaboration, and voice built upon a unique clustered architecture. Dynamic Clustering at the heart of the application makes the CommuniGate Pro Internet Communications Server a truly legendary system and the only messaging system capable of true, real-world 99.999% uptime.

Corporations are seeking software that provides more reliability and scalability with a lower cost of ownership. Service and broadband providers require voice and data infrastructure that can support the increasingly sophisticated requirements of a user base which encompasses Telco/ISP/ASP services across hundreds to thousands of domains. CommuniGate Pro offers a solution - for both enterprises and service providers - that reflects the convergence of the two markets: standards-based messaging with a rich integration of VoIP and collaboration.

The end goal is to unify all forms of digital messaging – voice, e-mail, calendaring, groupware, instant messaging, and web services – onto a user's choice of desktop computer, laptop, or any mobile device (or all of them simultaneously) using the same profile, the same features and security, and with the same capacity to communicate.

B. Key Differentiators

While a well-known and an established leader in e-mail and collaboration marker, CommuniGate Systems is a relative newcomer to the emerging world of Real-Time Communications. If your company has not deployed our products yet, we would like to outline the main factors placing us apart from competition:

- Our business model is based on selling software, not support services. As a result, our monetary interest is in providing high-quality products. No code within the product is dependant on open-source licenses such as GPL, BSD License, CPL, etc.; however, applications and interfaces within the product are generally provided as "open" applications easily adapted to your requirements.

- Our solutions are complete. We clearly specify what we do NOT provide (hardware, PSTN gateways), and we take the full responsibility for the rest of the system. CommuniGate Pro does not require third-party databases, services, or products.

- Our solutions are true carrier-grade solutions. Unlike many other companies that start with office-grade products and then try to "scale them up", all CommuniGate Pro subsystems where designed for the highest scalability and reliability. Functionality was added later, only after ensuring that the new features do not jeopardize performance or scalability.

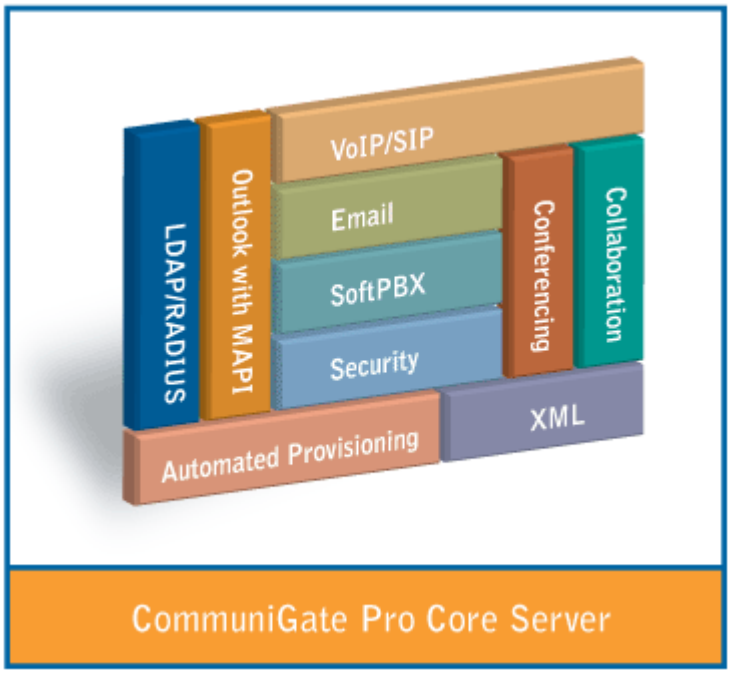
- Our solutions are highly manageable. Multi-level delegated administration provides a light, intuitive, and logical interface to all advanced product features. Self-administration functions (Web, IVR, e-mail, IM) allow users to control their accounts themselves, greatly decreasing the number of support and service calls. A Certified CommuniGate Engineer is needed only for large (several million accounts) Cluster installations.

- Our solutions are fully integrated. CommuniGate Pro "store-and-forward" and "real-time" functions all work in the same environment, complementing each other: a company Calendar can make an automatic phone call to all participants to invite them to a conference, an IM can be sent to notify a user about a specific e-mail, etc., to provide a truly-unified communications experience.

II. What is the CommuniGate Pro Internet Communications Platform?

CommuniGate System's flagship product, the CommuniGate Pro Internet Communications Platform, is the most technically advanced and complete messaging server. CommuniGate Pro combines e-mail, calendaring, VoIP and SIP, instant messaging, groupware collaboration, mailing lists, and webmail into a single IP Communications platform, and is designed and built as the critical foundation of your messaging infrastructure.

"Internet Communications" or "IP Communications" describe the range of protocols and methods offered by CommuniGate Pro for communication by data transfer, voice, and video - where the Internet is the medium and the protocols are open standards which interoperate between many different servers and clients. All users now have access to e-mail, instant messaging, voicemail in the INBOX, call control, and collaboration in one window or choice of client.



The CommuniGate Pro 5.1 full suite of IP Communications applications supports both IPv4 and IPv6 and includes:

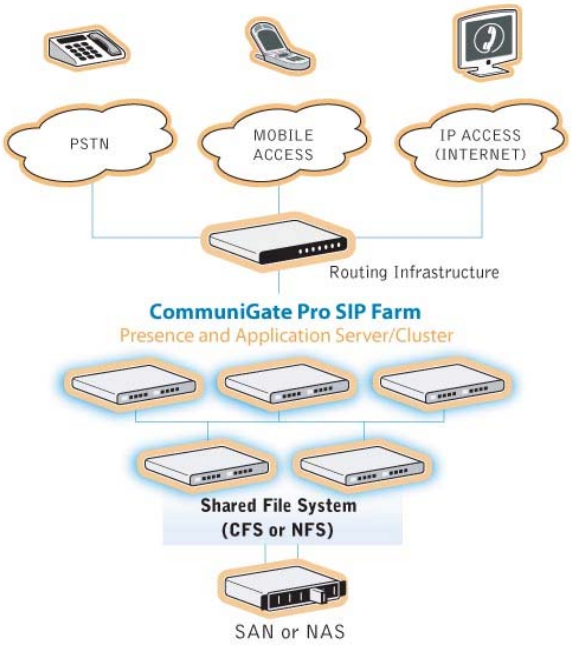
- E-mail, Collaboration, Instant Messaging (SIP and XMPP), and VoIP
- Pronto! flash client for secure, lightweight, and full-featured webmail and voicemail from anywhere
- XMPP/SIP clustering and server-side buddy-lists/presence with SIP Farm
- Complete PBX/Voicemail functionality including unified messaging, voice conferencing, unified voicemail, auto-attendant and call queuing/ACD
- Consolidated SIP infrastructure with built-in SBC, NAT traversal, and scalable SIP proxy/registrar
- Customizable interfaces for hosted e-mail/PBX services with the capacity to scale to many thousands of virtual domains

CommuniGate Pro is an IP Communications platform with applications and APIs that serve all of these needs. We develop carrier-class Internet Communications software for broadband and mobile service providers, enterprises, universities and OEM partners worldwide. CommuniGate Systems provides unsurpassed scalability and an expansive feature set all with unique clustering technology for 99.999% uptime for building your Internet Communications with a solid and proven foundation.

CommuniGate Systems is proud to be the most scalable platform with over 125-million end users including 45-million voice customers, with the highest customer satisfaction, and is constantly seeking out new emerging standards for IP Communications.

A. Total Solution

The following diagram illustrates the CommuniGate Pro Internet Communications Server in its most commonly deployed state, when architected for real-world 99.999% uptime and for a user base between 500 and 15-million users (where a Super-Cluster would be used for scaling beyond approximately 15M accounts). CommuniGate Pro provides the "five nines" of uptime required for today's voice and data with the truly unique architecture of the Dynamic Cluster:



A single CommuniGate Pro server or cluster can provide all of your Organization's fixed/mobile convergence – including PSTN, Mobile, and Internet-based connectivity needs.

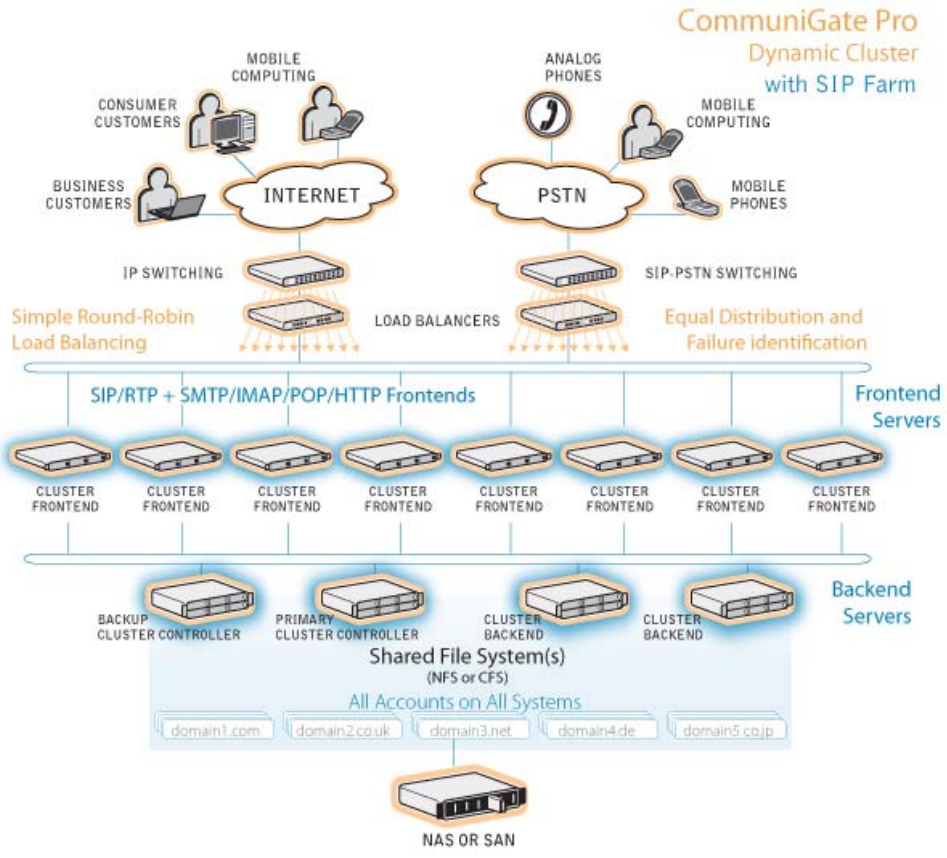
B. SIP Farm

SIP Farm is CommuniGate Pro's technology for clustering voice-over-IP (VoIP) for 99.999% uptime, redundancy, and scalability.

The CommuniGate Pro Dynamic Cluster maintains the information about all servers enabled for SIP Farm. Incoming SIP UDP packets and TCP connections are distributed to those servers using regular/simple load balancers.

Packets not directed to a particular SIP Farm server are distributed to all SIP Farm members based on the CommuniGate Pro cluster algorithms and the currently available set of the active SIP Farm cluster members. In the case of the addition or loss of a SIP Farm member (such as a hardware failure), the traffic is redistributed to other SIP Farm members to maintain consistent signaling.

The following diagram demonstrates a "8+4" Dynamic Cluster (8 Frontends and 4 Backends) using the optional "SIP Farm Specialization", which allows for a subset of all Dynamic Cluster members to be allocated as part of the SIP Farm. This technique can be used to protect the Quality of Service (QOS) of voice and real-time requirements by separating the e-mail traffic from the SIP/RTP traffic, while continuing to maintain the single-system image of the Dynamic Cluster with consolidated identity management.



The 8+4 SIP Farm Dynamic Cluster can provide E-mail and VoIP services to millions of accounts. The E-mail and Voice/IM/Presence Frontends can be separated into two groups, in order to protect QOS of low-latency communications methods (such as Voice and IM) from E-mail loads, spam, or attacks.

C. Reliability with Portability

The CommuniGate Pro server runs on more than 35 OS/hardware, offering Customers maximum flexibility for their backend infrastructure, along with protection and reuse of hardware investments. Since the same C++ code base is used in CommuniGate Pro across all platforms, this provides an additional level of reliability and stability that benefits all Customers – since the same code base is used, a problem that may arise on one platform may indicate a more pervasive problem that may eventually be revealed on other platforms; so, the CommuniGate Pro application stability can be continually improved across all platforms simultaneously. The far majority of Customers deploy their production systems on Linux, Solaris, HP-UX, AIX, Windows, or Mac OSX.

A single Dynamic Cluster installation can be comprised of multiple OS platforms, as the product performs identically and interchangeably as a solitary system. The full list of OS/hardware versions available includes:

Sun Solaris SPARC	Apple MacOS X PowerPC
Sun Solaris x86	Apple MacOS X Intel
Sun Solaris x86-64	IBM AIX
Microsoft Windows NT/2000/XP/2003 Microsoft Windows 95/98/ME x86	SGI IRIX
FreeBSD 4 x86	HP/UX PA-RISC
FreeBSD 5 x86	HP/UX Itanium2
Linux x86	BSDI BSD/OS
Linux x86-64/EM64T	SCO UnixWare
Linux MIPS (Cobalt)	SCO Openserver for x86
Linux Alpha	OpenVMS Alpha
Linux StrongARM (NetWinder)	OpenVMS IA64
Linux IBM S/390s (64-bit)	QNX Intel
Linux IBM S/390 (32-bit)	IBM OS/2 Intel
Linux Itanium2 (IA64)	NetBSD
Linux Motorola 68K	BeOS Intel
Linux PowerPC	BeOS PowerPC
Tru64 (Digital Unix) Intel	IBM OS/AS/400 (iSeries)
Tru64 (Digital Unix) Alpha	

D. Client and Protocol Overview

The following diagram is provided to loosely illustrate the CommuniGate Pro Platform and the many client applications that integrate with it. While this diagram is not a technically-accurate "block diagram" for the internal modules and threads in CommuniGate Pro, it does provide a satisfactory top-down perspective on the many services and protocols available in CommuniGate Pro:

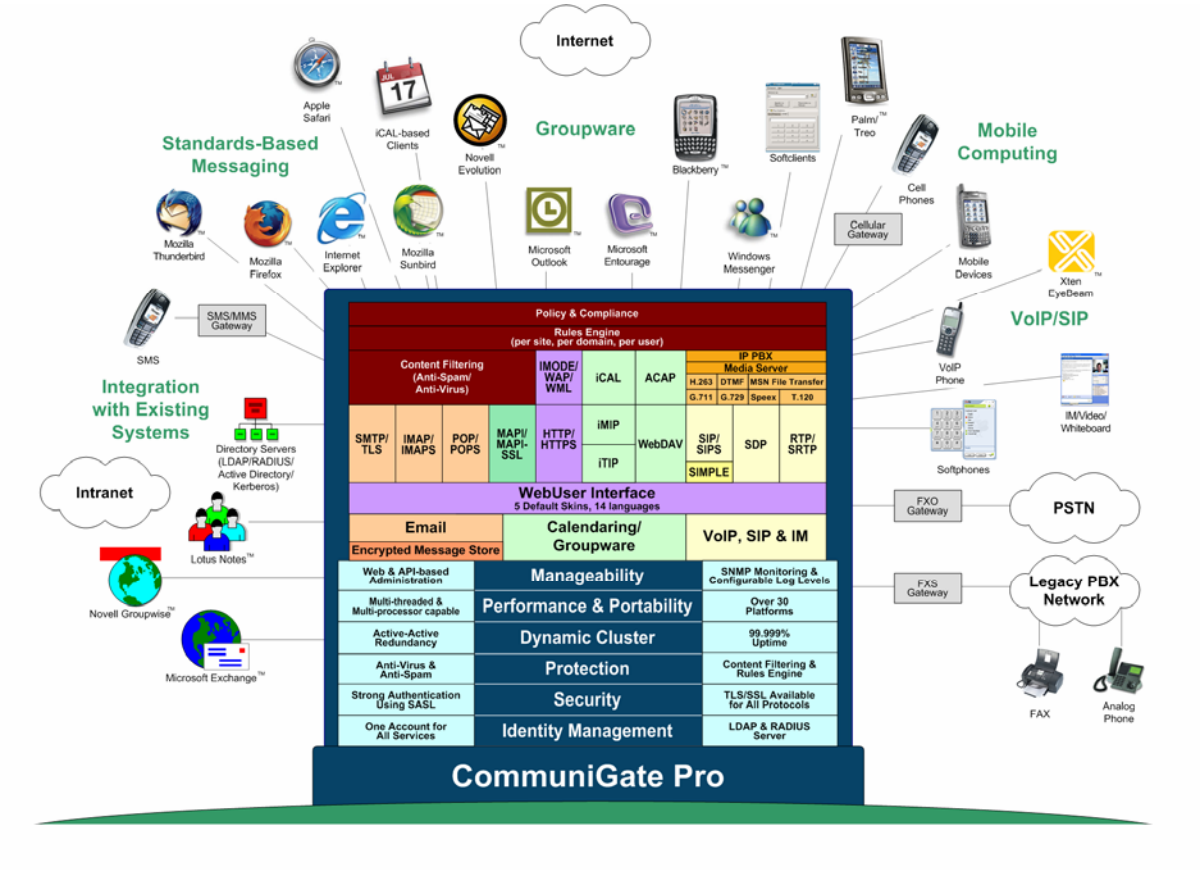


Illustration of the "Foundation" of CommuniGate Pro and Client Applications.

III. New Features in CommuniGate Pro v5.1

A. Pronto! Flash-based Interface for WebMail, IM, and Calendaring

Web browser based messaging clients are currently making an evolutionary leap in the rapidly expanding IP Communications landscape. There are now a few consumer service and open source examples of user interface enhancements supported by AJAX along with other script, parse, and rapid render methods. The attractive and impressive visual results of these efforts will continue to grow and integrate with more arriving technologies such as Presence, Instant Messaging, and Voice/Video over IP via applet style architectures that will borrow key functionalities from other software or systems. Eventually having all of this functionality accessible via the web will better the deployment, support, and transportability of all key business communications. A great reduction in "Travel to the desktop for install and upgrade" costs alone will avoid significant time and productivity loss in many organizations.

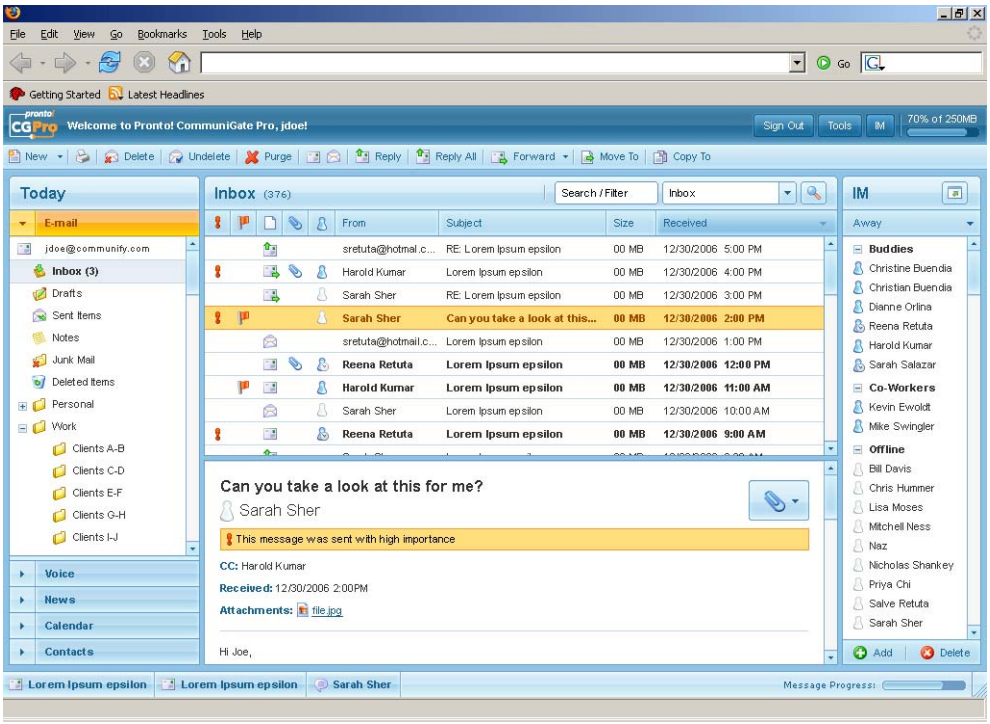
From both a security and productivity perspective there is much to be desired in the management of connecting many different technologies via different applications all with their own protocol and API sets to achieve what a few in the market have achieved as service providers today. While many buyers of advanced communications technology will wait for a future with truer points of integration, CommuniGate Systems presents this today with Pronto!

Pronto! is CommuniGate Systems IP Communications user interface for the scalable and IETF RFC-based (standards-based) and feature-rich CommuniGate Pro™ Internet Communications Platform. Pronto! delivers to users what CommuniGate Pro delivers to communications administrators, the most well fastened collection of standards-based communications tools from a single manageable interface. Based on business and web proven Macromedia Flash technology, Pronto! exchanges data with the communications infrastructure via the efficient XML Interface for Messaging Scheduling and Signaling (XIMSS) available from CommuniGate Pro. XIMSS enables Customers, Partners, and third-party vendors to develop applications **today** for Unified Communications and IMS/Fixed-Mobile-Convergence without having to understand complex protocols such as SIP, RTP, IMAP, XMPP, and others. Instead, XIMSS allows developers to write full client and web applications and portals simply using the XML they are already likely very familiar with as part of a standard web application development environment, but with access to all of the many communications protocols that CommuniGate Pro supports.

XIMSS expedites in-house value-add efforts by removing the development obligation to include, integrate, and debug bloated source code for every needed IP communications protocol (e-mail, calendar, IM using SIP and XMPP, click-to-call, etc.) that will benefit end users today. The result for Pronto! is a lighter and faster web-based communications tool abstracted using native XML that offers greater value and a greater return on investment than many of the emerging products today that

range from no dollar cost to high cost models with at-your-own-risk features and integration methods included.

For increased productivity, reduced communications costs and bandwidth usage, and simplified infrastructure, get Pronto! with the highly reliable CommuniGate Pro communications platform.



The Pronto! WebUser Interface for webmail, voice, news, calendar, contacts, and IM/Presence with buddy lists.

B. VoIP Infrastructure and Applications

While CommuniGate Pro version 4.3 introduced an advanced "VoIP Infrastructure" which enabled users to utilize SIP telephony anywhere in the world, CommuniGate Pro version 5.0 introduced "VoIP Applications", while version 5.1 refined these applications and added more features and attributes. These voice applications enable users to communicate using true IP-based telephony devices and applications as well as connect to the Publicly Switched Telephone Network (PSTN).

1) VoIP Infrastructure

Included in "VoIP Infrastructure" features are those which affect architecture, gateways, networks, and clustering:

- "SIP Farm" – all-active clustering
- "Just Add Nodes" – adding additional nodes to the live cluster adds capacity and redundancy
- CDR records API for billing
- Complete NAT traversal/SBC/media proxy functionality
- "SIP Workaround Features" – runtime workarounds for non-standard SIP softswitches and clients
- Multiple gateway support
- Advanced call digit routing control
- External Helper Routing for ENUM or number portability databases

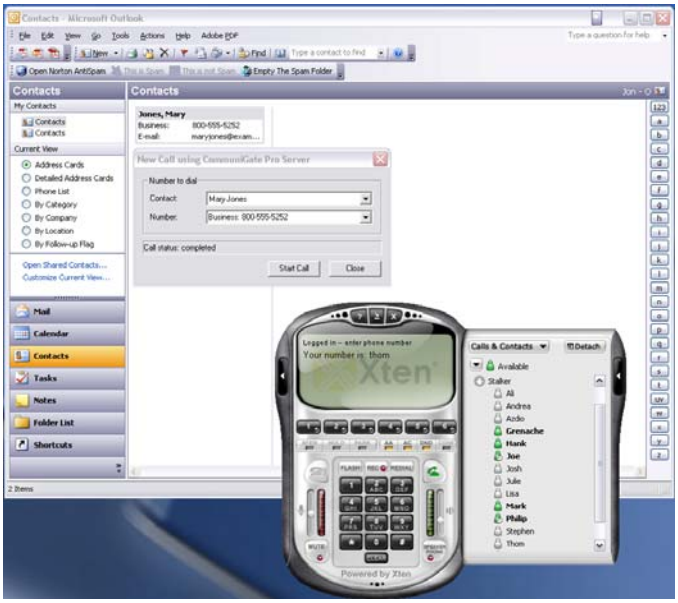
2) VoIP Applications

Included in "VoIP Applications" are a variety of CG/PL applications which run on the CommuniGate Pro platform. These applications are generally delivered in the CommuniGate Pro distribution package as "openly-sourced" scripts, meaning they can be easily modified or customized by Customers and Partners for their own use, development, or site personalization. Included applications include:

- Conference Server
- Auto-attendant/IVR
- Call queuing/Automatic Call Distribution (ACD)
- Voicemail and Self-Service
- Call Parking, Pickup, & Transfer
- Included VoIP applications are easily extendable
- B2BUA functionality using the built-in "GatewayCaller" application
- Open, documented "CG/PL" (CommuniGate Programming Language) for a powerful voice development platform

With CommuniGate Pro's standards-based foundation and SIP infrastructure, all end users are provided the ability to instant message, video conference and make VoIP phone calls from any Internet location to any Internet location. In addition to its e-mail, calendaring and groupware capabilities, CommuniGate Pro provides a advanced SIP infrastructure that requires no additional SBC hardware and that offers near-end and far-end NAT traversal to seamlessly interoperate with any VPN or firewall. CommuniGate Pro's foundation of identity management allows users to register with the same username, password, and profile that they already use for e-mail and groupware.

Now, with 5.1, all users have access to their voicemail and call control directly from the desktop, including productivity improving features such as click-to-call from the address book in Outlook and WebMail. This screenshot demonstrates the click-to-call capability from Outlook with CounterPath (formerly Xten) EyeBeam SIP-based client.



CommuniGate Pro Click-to-Call through WebMail and integrating with CounterPath (formerly Xten) EyeBeam with VoIP, Video, IM and Presence.

IV. Overview of CommuniGate Pro

The following bullets list the major features, protocols, and services included in the CommuniGate Pro server software, and should generally always be available at this online location:

http://www.communigate.com/CommuniGatePro/

Please note: the following list should appear as "clickable" links.

A. Identity Management

- Multi-Domain architecture (field-proven for over 120,000 domains per system), with multi-homing and shared-IP configurations.
- Account concept, including Mailbox Storage, File Storage, Account Settings, and Account Information databases.
- Groups, Forwarders, Aliases, and other Domain Objects.
- Meta-Directory with Local and Remote Units.
- LDAP access to Directory and Account databases.
- External Authentication mechanism for integration with 3rd party solutions.
- RADIUS services.

B. Storage Management

- Mailbox Storage with multiple Mailboxes, Shared access, ACLs.
- Mailbox formats - text files, file folders, other data containers.
- File Storage with public and private folders, virtual files.
- Groupware Information storage and processing using the iCalendar and vCard standards.

C. Mail Transfer

- ESMTP and LMTP mail exchange services.
- Anti-Spam and other protection mechanisms.
- Plugin Interface for high performance virus, spam, and content filtering.
- Automated Mail Processing Rules.
- Mailing List manager with automatic bounce processing and a Web interface to list archives.
- Remote Account Polling using the POP3 protocol.
- External Program Delivery for custom applications.
- Automated Invitation processing for shared resource scheduling.

D. Real-Time Signaling

- SIP protocol for Instant Messaging, Presence, audio and video communications, desktop sharing and real-time collaboration.

- XMPP protocol for Instant Messaging and Presence.
- XIMSS protocol for Instant Messaging, Presence, audio and video communications.
- NAT Traversal mechanisms (near-end and far-end) for RTP and TCP-based media protocols.
- Registrar, forking Proxy, and Presence server functionality.
- Automated Signal Processing Rules.
- Event packages for presence, message-waiting, registration, and other services.

E. Real-Time Application Environment

- Domain-specific application environments.
- CG/PL language for quick and robust application design.
- Built-in operations for call control, bridging, and multi-party conferencing.
- Integrated Access to Message and File stores.

F. Data Access Services

- POP3 and IMAP4 mail client access.
- MAPI interface for Microsoft® Windows clients (Outlook and other MAPI-enabled applications).
- WebUser Interface to Mailbox, Groupware and File Stores, to Settings and Information databases, to the Signaling and Message Transfer facilities.
- Multi-lingual Skins for customizable HTML, WAP/WML, and I-Mode Interfaces.
- XIMSS interface providing access to Mailbox, Groupware and File Stores, to Settings and Information databases, to the Signaling and Message Transfer facilities.
- HTTP, FTP, and TFTP access to Account File Stores.
- Publish/Subscribe HTTP-based operations with Calendar and Tasks mailboxes.
- ACAP access to the Account Information database.

G. Advanced Security

- SASL Secure Authentication methods.
- GSSAPI (including Kerberos V5) authentication, SSO (single sign-on), and security.
- Client Certificate-based Secure Authentication methods.
- Secure Mail (S/MIME) WebMail implementation (encryption/decryption, digital signing, signature verification).
- Automatic Encryption implementing secure information storage.
- SSL/TLS Secure Transfer for SMTP, SIP, IMAP, POP, HTTP, LDAP, ACAP, PWD and Administration sessions.
- Lawful Interception functionality.

H. Multi-tier Administration

- WebAdmin interface for administration, provisioning, and monitoring.
- CLI/API interface for administration, provisioning, and monitoring.
- SNMP Agent for remote monitoring.
- Triggers for proactive monitoring.
- Poppwd protocol for remote password modification.
- LDAP-based Provisioning (optional) for integration with legacy systems.
- BSD syslog Server to consolidate log records from third-party components.

I. Multi-Server Operation

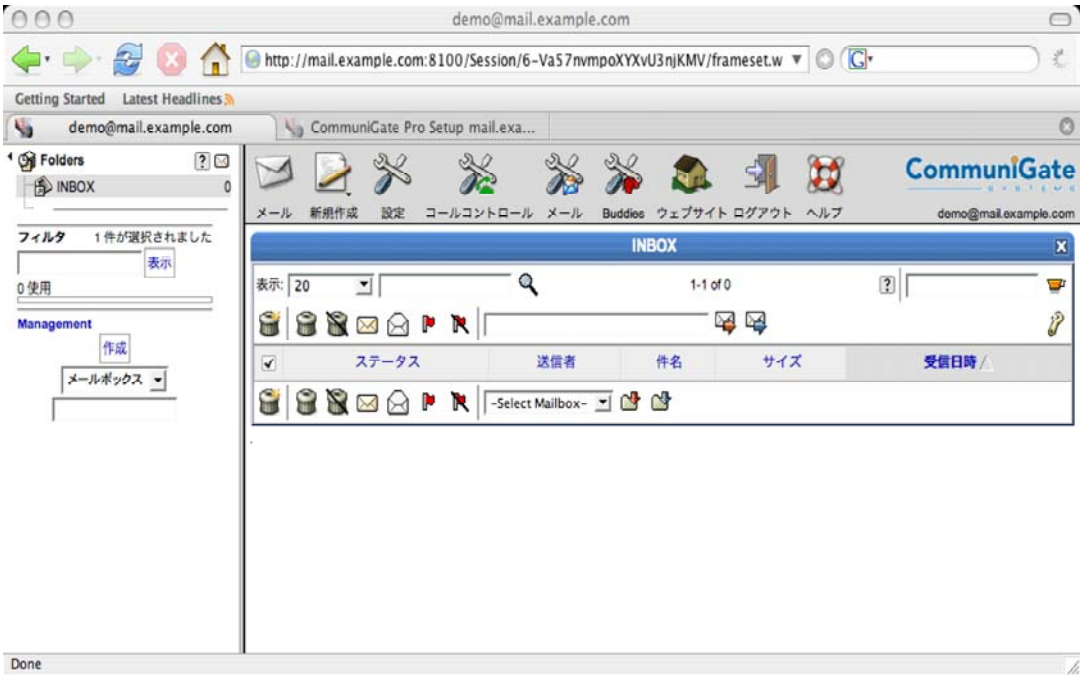
- Distributed Domains for Distributed multiple single-Server configurations.
- Static Clusters for Multi-Server Account partitioning.
- Dynamic Clusters for advanced scalability without Account partitioning. Carrier-grade 99.999%-uptime, field-proven for more than 5,000,000 real active Accounts.
- Cluster of Clusters for extra-large sites (over 10,000,000 active Accounts).

J. Language Support

CommuniGate Pro is implemented in native UTF-8 and has built-in support for many languages, including today:

- English
- Arabic
- Chinese
- Dutch
- French
- German
- Hebrew
- Italian
- Japanese
- Portuguese
- Russian
- Slovak
- Spanish
- Thai

Additional languages can easily be added to the package by Customers or Partners by adding a new "strings.data" file in the desired language. Only this one file needs to be used to allow use of the specified language throughout the WebUser Interface for webmail.



The Japanese WebUser Interface "skin" (note that the left side folders are user-created in any language that is supported).

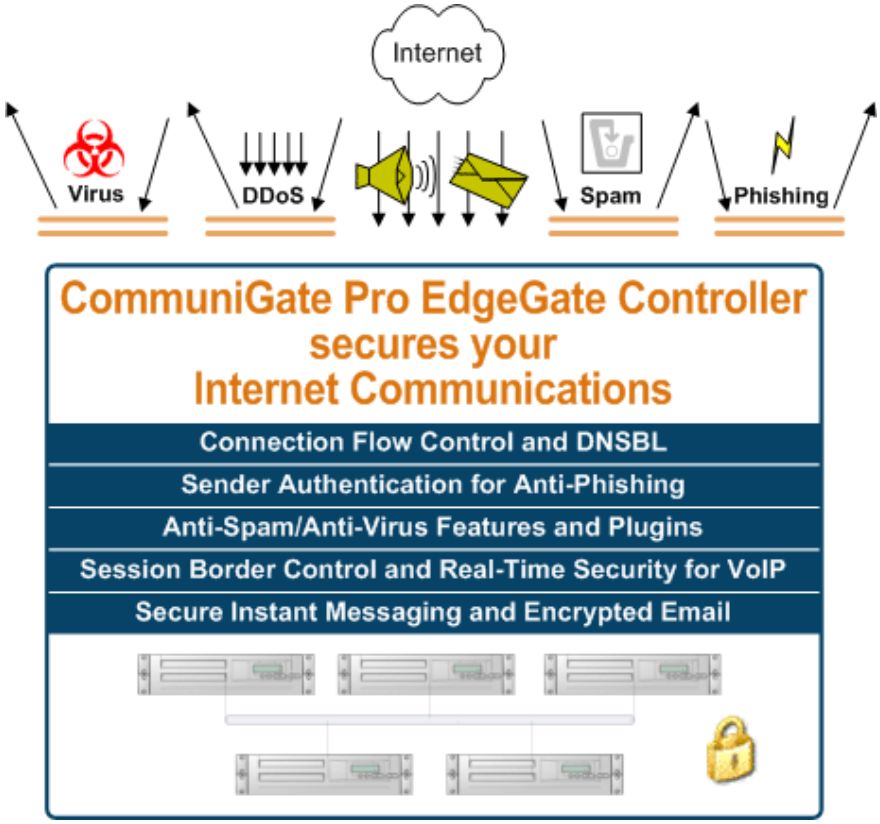
K. EdgeGate Controller

"EdgeGate Controller" protection includes the many built-in and third-party add-ons which comprise the CommuniGate Pro security infrastructure.

Third-party plugins for Anti-Spam and Anti-Virus include the following, in addition to the many open-source plugins available:

- McAfee Virus Scanner Plugin for CommuniGate Pro
- Sophos Virus Scan Plugin for CommuniGate Pro
- Kaspersky Anti-Virus Plugin for CommuniGate Pro
- MailShell SpamCatcher Plugin for CommuniGate Pro
- Cloudmark Authority Anti-Spam Plugin for CommuniGate Pro

CommuniGate Pro's built-in SIP session border control features for NAT traversal and SIP security such as relaying and authentication control ensures that all users can connect securely and consistently, no matter if they are located inside the internal network perimeter or from any remote source, such as the PSTN, mobile networks, or the Internet:



CommuniGate Pro contains built-in features to control and secure your network's perimeter edge, and provides secure accessibility "wherever you are".

V. CONFIGURATION AND USE

The following section describes the configuration and use of common desktop applications with CommuniGate Pro, including e-mail, groupware, real-time communications such as instant messaging and VoIP, and WebMail. For the reviewer, however, this may first require downloading and installing a test copy of CommuniGate Pro. Alternatively, CommuniGate Systems can provide a demo account on a demo server, please contact support@communigate.com for a demo account.

Fully-functional trial versions of CommuniGate Pro Internet Communications Server for single-server use are free to download off the CommuniGate website at:

http://www.communigate.com/download

Trial versions of the software function normally in all aspects, except that all e-mail messages sent contain a notice that the message was sent by a trial version of CommuniGate Pro. Also, it should be noted that Dynamic Clustering of CommuniGate Pro (recommended for most enterprises and service providers) is only possible through a license provided directly by CommuniGate Systems – if you wish to test a Dynamic Cluster in your environment, please contact a CommuniGate Systems representative directly by phone or e-mail:

http://www.communigate.com/content/contactus.html

Full documentation for installing, configuring, and administering CommuniGate Pro is also available online:

http://www.communigate.com/CommuniGatePro

The public CommuniGate Pro mailing list is a great place to get feedback or present questions to CommuniGate Systems staff or other CommuniGate Pro users:

http://www.communigate.com/content/mailinglist.html

Finally, CommuniGate Systems also provides free Technical Support assistance with Trial Installations of CommuniGate Pro – please visit this page to review the Technical Support options:

http://www.communigate.com/content/techsupport.html

A. Installing CommuniGate Pro and Setting Up Accounts

While full documentation for CommuniGate Pro installation is available at the following URL, this section provides streamlined install instructions:

http://www.communigate.com/CommuniGatePro

1) Download

Download the platform package of your choice (over 35 available today) from:

http://www.communigate.com/download

2) Install

Install the package using the method appropriate for your platform (e.g., unzip/untar the package, click the .exe or use "rpm –ivh", etc.)

3) Start the CommuniGate Pro Server

For various platforms:

- Most Unix/Linux:

  ```
  /etc/init.d/CommuniGate start
  ```

- Solaris

  ```
  /etc/init.d/STKCGPRO start
  ```

- Mac OSX

  ```
  /Library/StartupItems/CommuniGatePro/CommuniGatePro start
  ```

- Windows

  ```
  START -> Control Panels ->
  Administrative Tools -> Services ->
  CommuniGate Pro Server
  ```

4) Administer

Open a web browser, and connect to the CommuniGate Pro "WebAdmin Interface" at either of these locations, where "mail.example.com" is the name of your system in DNS (CommuniGate Systems recommends using encrypted protocols whenever possible – generally every component has an SSL/TLS partner:

https://mail.example.com:9010

http://mail.example.com:8010

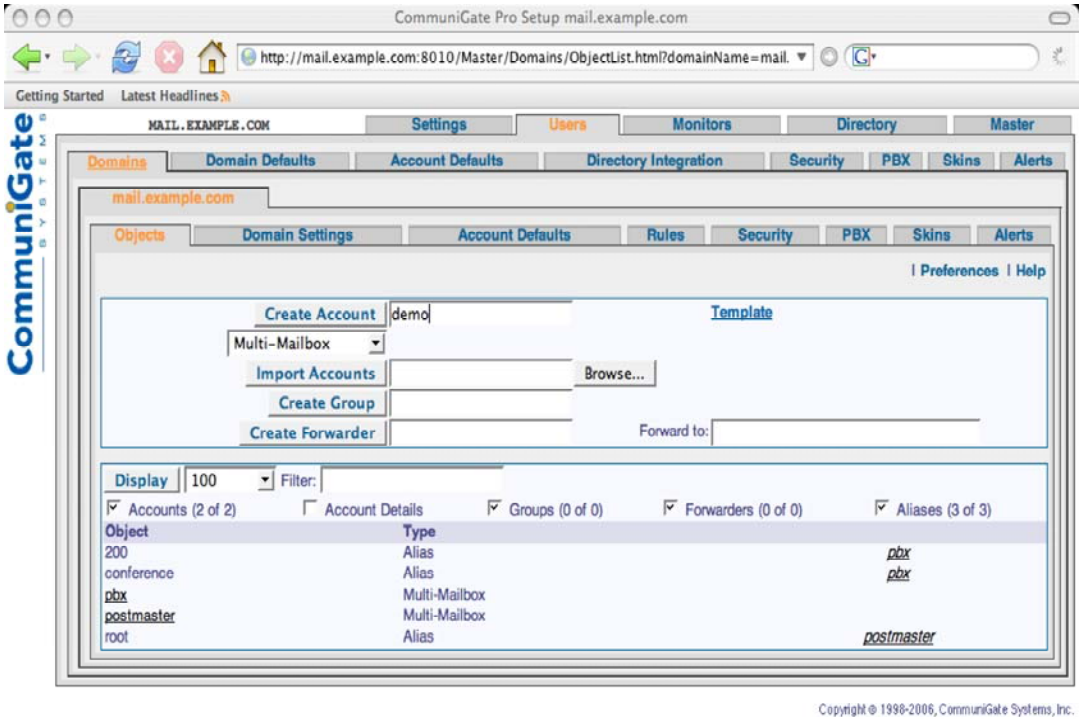
Or, if using the same system/laptop that you are using to read this document:

https://localhost:9010

5) Create an Account

In the WebAdmin Interface, select the "Users" tab along the top of the window. COMMUNIGATE PRO will ask you to authenticate – do so as "postmaster" and the password created after starting the CommuniGate Pro server for the first time.

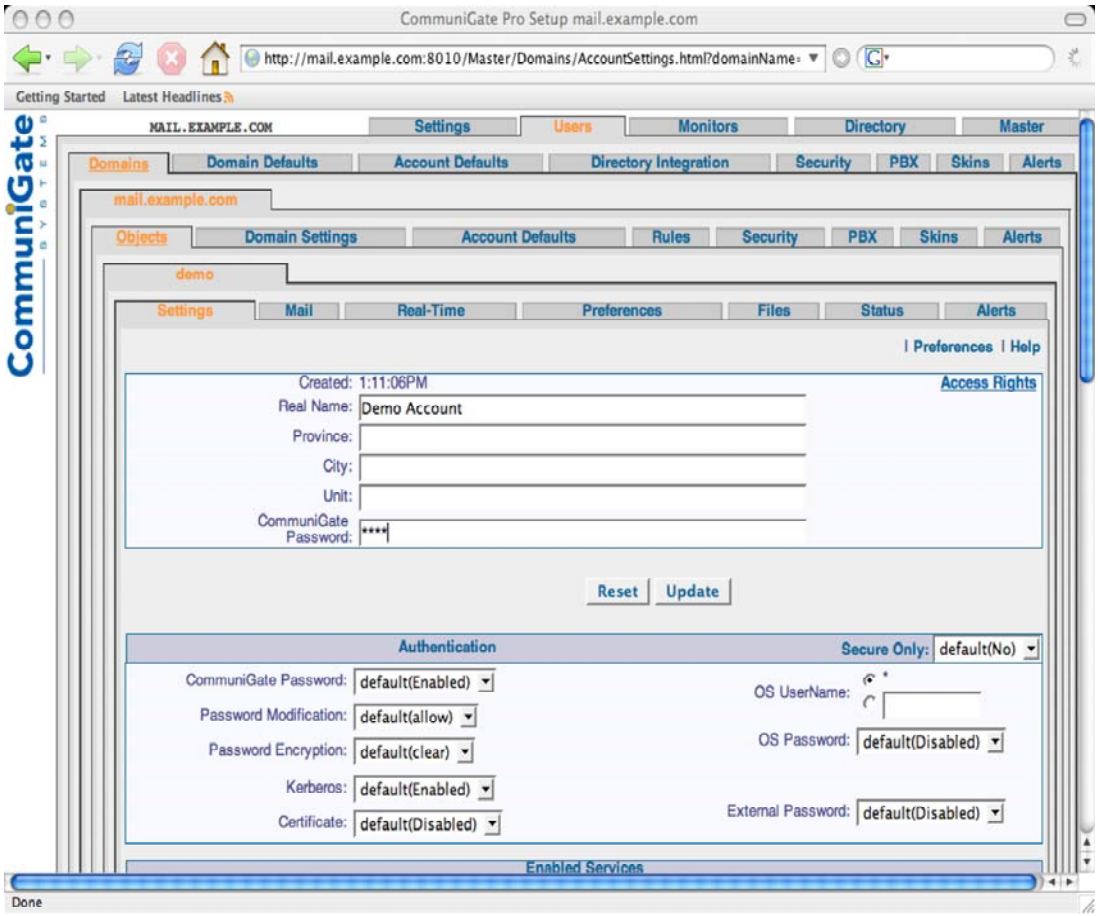
Select the domain name corresponding to the domain where the new user will be added. Find the field for "Create Account", and enter one or more new accounts, such as the example below for the account "demo". Don't forget to click the "Create Account" button once the new account name has been entered.



Creating an account through the CommuniGate Pro WebAdmin Interface.

6) Enter Other Account Details

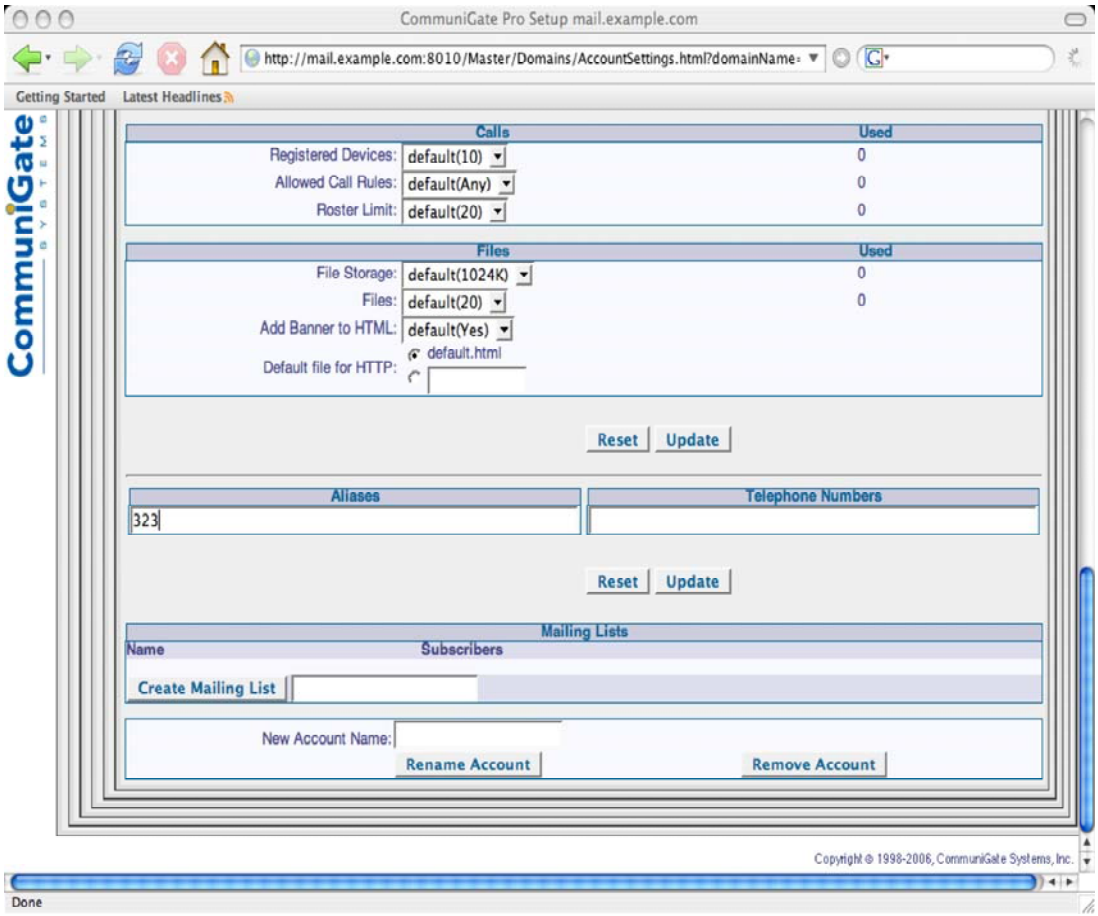
After the account has been created, enter a "Real Name" for the account, as well as a password. This password will be used for all client applications, such as those used for e-mail, voice, and video:



Adding a password through the CommuniGate Pro WebAdmin Interface.

7) Adding an Extension

If a user requires an "extension", this is very easy to add. All extensions are really just CommuniGate Pro "aliases" for an account. The below screenshot shows an extension "323" being enabled for this user:



Adding an Alias/Extension through the CommuniGate Pro WebAdmin Interface.

8) Enabling Voicemail for All Accounts in CommuniGate Pro

Enabling Voicemail and Self-Service for all CommuniGate Pro accounts requires just a few changes in the CommuniGate Pro WebAdmin Interface.

- Log into the WebAdmin Interface as described previously.

- Select the "Users" tab from the top of the window. Authenticate using the "postmaster" credentials whenever requested (each module within CommuniGate Pro requires authentication). Please select the domain for which enabling Voicemail is desired. In this example, "mail.example.com" is the domain. Then select the "Rules" tab near the top of the window.

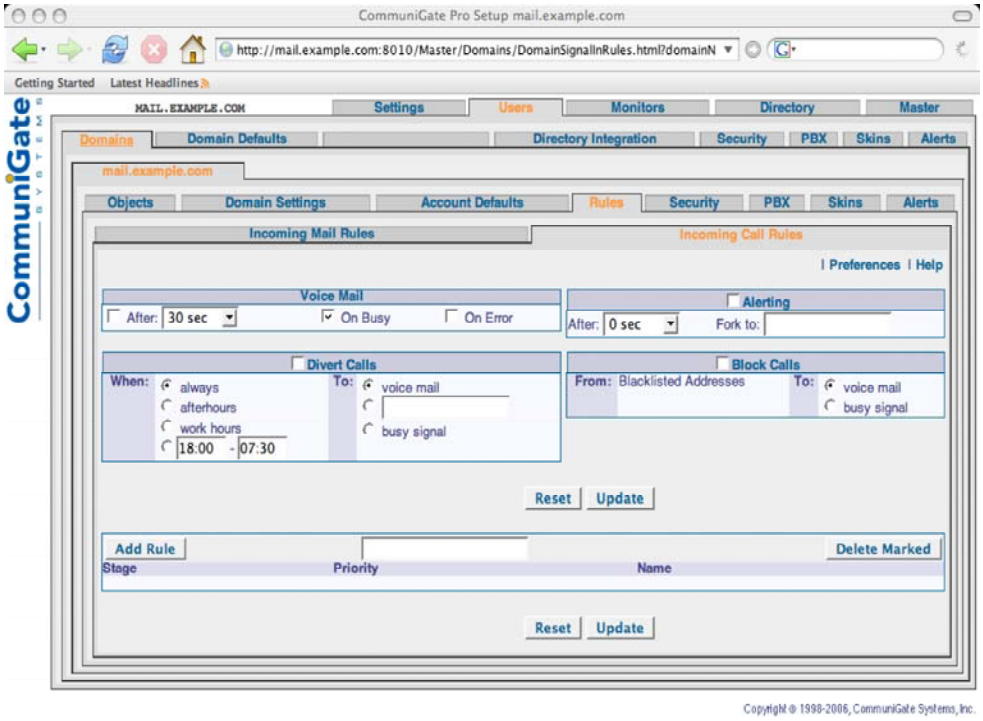
- Please select the "Incoming Call Rules" under Rules. In CommuniGate Pro WebAdmin navigation, you might see this series of clicks referred to as:

  Users->"mail.example.com"->Rules->Incoming Call Rules

- Under the "Voice Mail" heading, set the Incoming Call Rules to the following:

```
[ x ] After: [ 30 Sec ]
[ x ] On Busy:
```

- That's it – all users in the selected domain have now been enabled for the "voicemail" and "service" (a.k.a., "self-service") PBX applications. An example screenshot of this page follows:



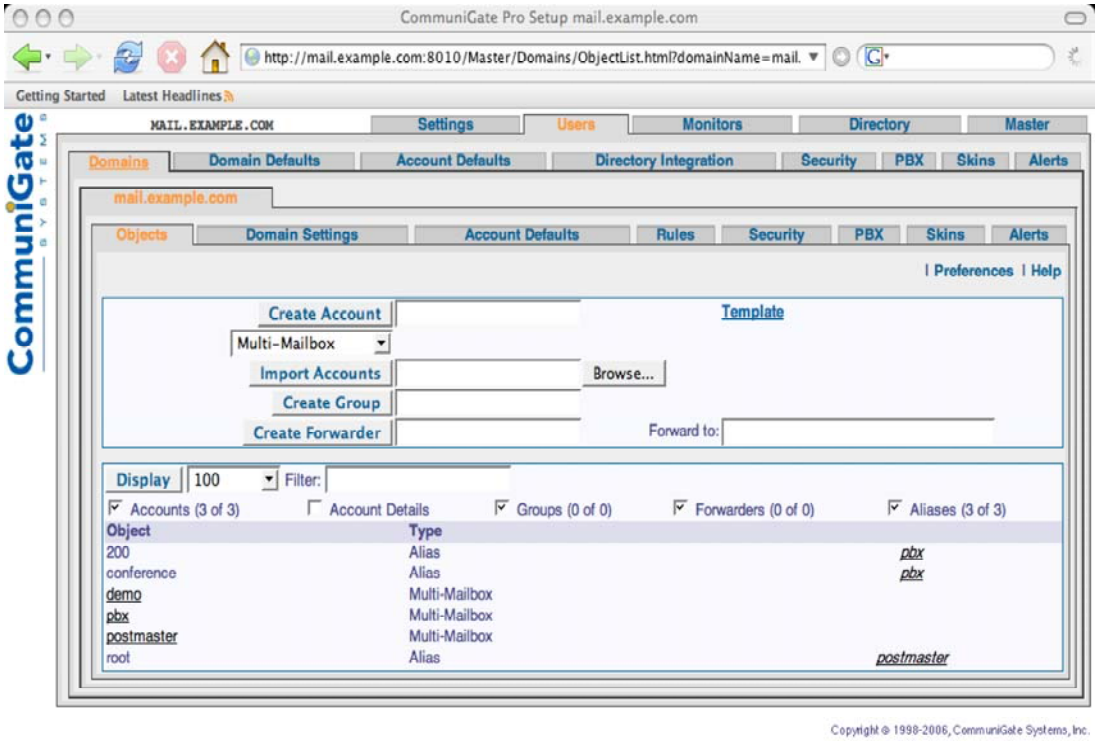
Managing default Call Rules for the Domain.

9) Enabling a "PBX" Account for Auto-Attendant/IVR

Creating a "PBX" (or "attendant") account allows your system to act as an Auto-Attendant/Interactive Voice Response system. Incoming calls from the PSTN or

Internet can be directed first to the Auto-Attendant to welcome callers to your company and provide a menu/IVR system for accessing departments, extensions, and other services such as conference calls.

- Create an account called "pbx", just as you created the "demo" account above: (Note: in version 5.1 of CommuniGate Pro, this account is created automatically. See below.)



Managing the "PBX" account, which is the designated account under which Auto-Attendant or Voice Menu applications normally run.

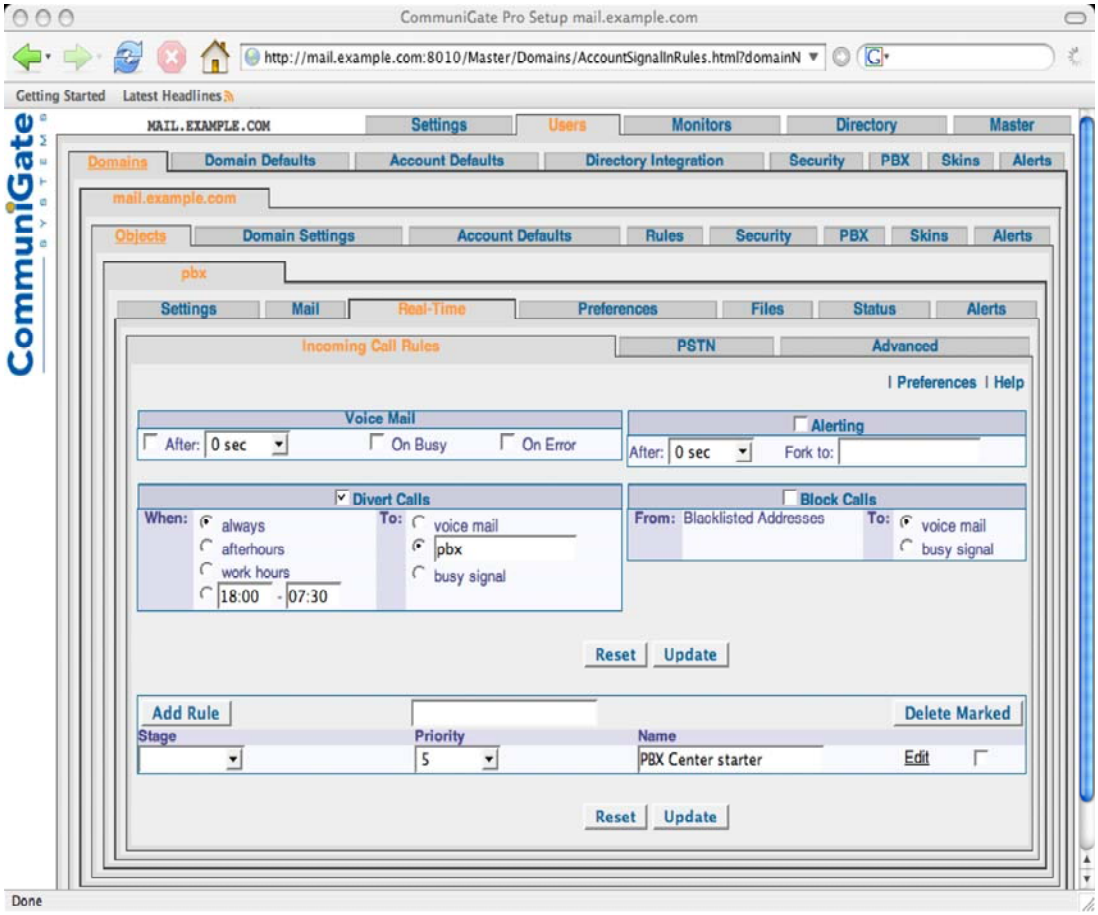
- Select the "pbx" object from the list of users in the domain.
- For the pbx account, select the "Real-Time" tab near the top of the page.
- Select "Incoming Call Rules" tab near the top of the window and enter the following options:

```
[ x ] Divert Calls
When: [ always ]
To: [ pbx ]
```

Please note that the setting was configured for "always", meaning that the pbx application will begin immediately upon receiving an incoming call. In the event that your site has a human receptionist, you would likely want to register the receptionist's

IP phone to authenticate as the "pbx" account (perhaps in addition to their own personal account, since many IP devices can REGISTER to more than one Account simultaneously – as well as that one Account can have many devices registered to it simultaneously; and instead set the "No Answer for" setting to 15 or 30 seconds. Only if the receptionist did not pick up the call, would it be answered by the pbx application.

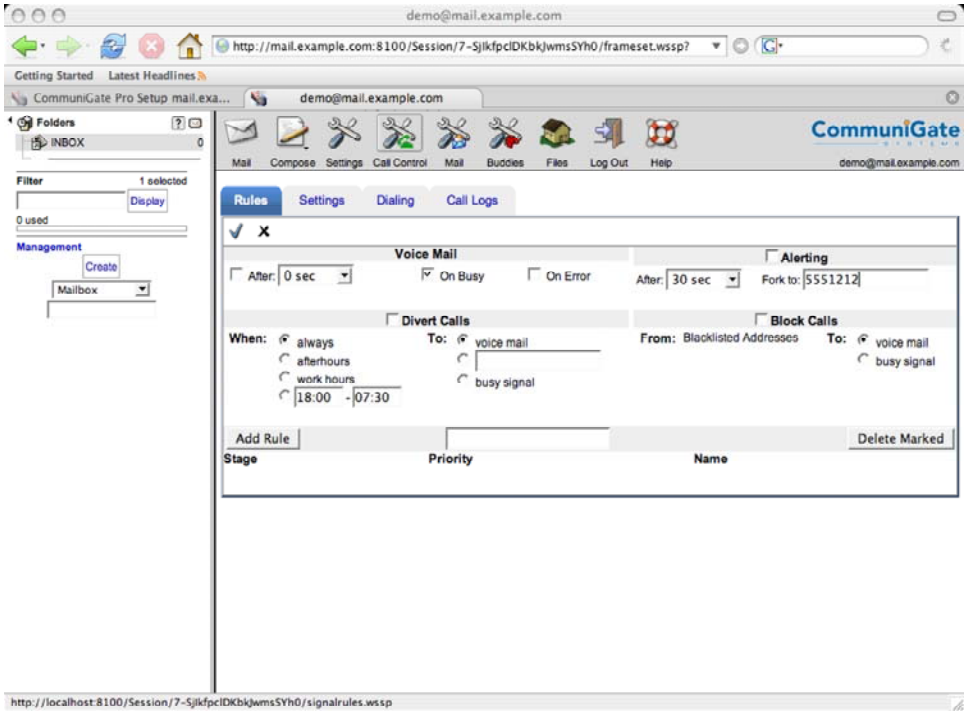
Following is a screenshot with a 0-second "No Answer for" configuration:



Configuring the PBX call-handling Call Rules.

10) "Call Control" for Users

Every user has the capacity to manage their Call Control settings from within the WebUser Interface:



WebMail (WebUser Interface) Call Control for users.

B. Configuring a Sipura 3000 FXO to Connect VoIP-to-PSTN

The Sipura 3000 (and more recent similar models) is a well-valued, better-than-average quality VoIP-to-PSTN gateway device. For less than $100, it supports three ports:

- An analog (RJ-11) line from your telephone provider (such as SBC)
- A LAN Ethernet connection (RJ-45)
- A second analog (RJ-11) line for connecting a standard telephone

This device is a good starter device for the introduction of VoIP-to-PSTN services. The term "FXO" refers to a traditional telephony term "Foreign Exchange Office", which simply describes a device at an outlying office which connects back to the central office. In our setup, the outlying office is your home or office, and the central office is the telco service provider, such as AT&T. This category of device functionality is called by many different names, including FXO gateways or switches, VoIP-to-PSTN gateways/switches, softswitches, trunking gateways, and so on, and range from single-line analog connections to the PSTN all the way up to direct backbone trunks over T1/E1, T3/E3, OC-45, etc. For CommuniGate Pro's use, the concept remains the same when connecting to the PSTN – traditional telephony signals (analog or digital) go in and out on one or more ports, and SIP/RTP traffic on Ethernet goes in and out on one or more ports, with the VoIP-to-PSTN switch routing back and forth between them.

The Sipura 3000 can be configured to work with CommuniGate Pro with the following streamlined steps:

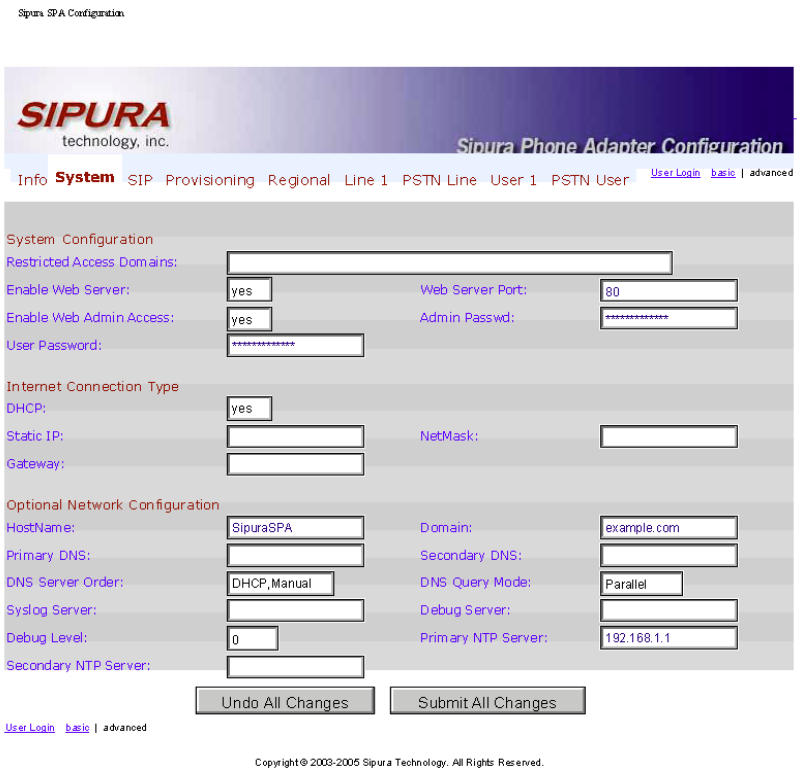
- Please plug in the Sipura – power, analog line (to your telco), and Ethernet (to your LAN)
- By default, the Sipura should get a DHCP address on your network and start its administration interface (accessible via a web browser)
- Connect to the administration interface (and fill in your device's primary IP address):

  http://192.168.1.2/admin

The default login is "admin", and there is no default password (it should accept a blank password).

- The Sipura uses a "tabbed" administration interface. The Info tab will display the current configuration:

- The "System" tab should be configured for a HostName, and any other relevant information to your site (DHCP, Domain, DNS, etc.):



- If just using the PSTN and Ethernet ports, then the only other configuration changes need to be set on the "PSTN Line" tab. These changes would include the following for a very simple setup. Please note that no security restrictions have been added here, so any system which can route SIP traffic to the Sipura device will be able to initiate outbound calls to the PSTN:

PSTN Line

```
Line Enable: yes
NAT Mapping Enable: no
SIP Port: 5060
```

Proxy and Registration

```
Proxy: mail.domain.com (replace with correct host)
Use Outbound Proxy: yes
Outbound Proxy: mail.domain.com (or IP address)
Register: no
Display Name: Sipura3000
Use Auth ID: no
```

Dial Plans

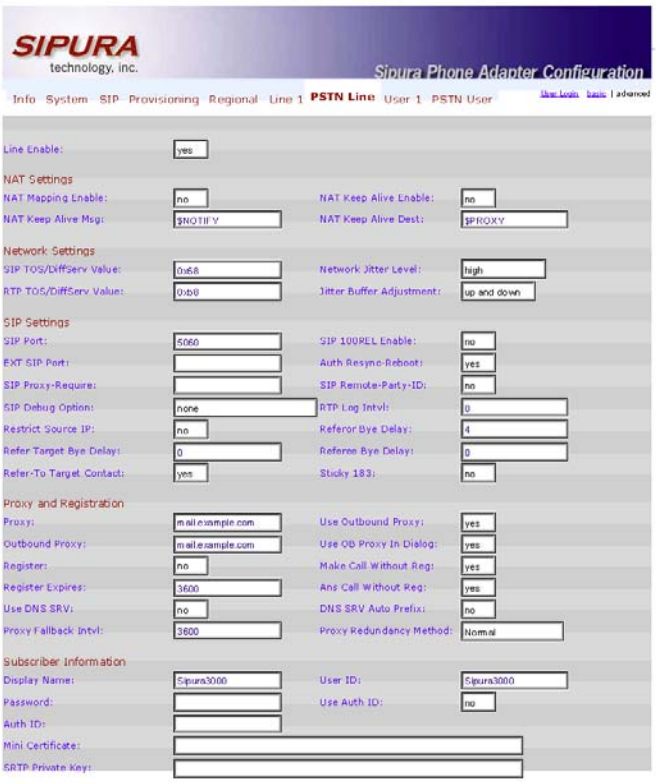
```
Dial Plan 1: S0<:pbx@mail.domain.com>
Dial Plan 2: (xx.<:@gw0>)
```

VoIP-to-PSTN Gateway Setup

```
VoIP-to-PSTN Gateway
Enable: yes
VoIP Caller Auth Method:
none
One Stage Dialing: yes
VoIP Caller Default DP: 2
```

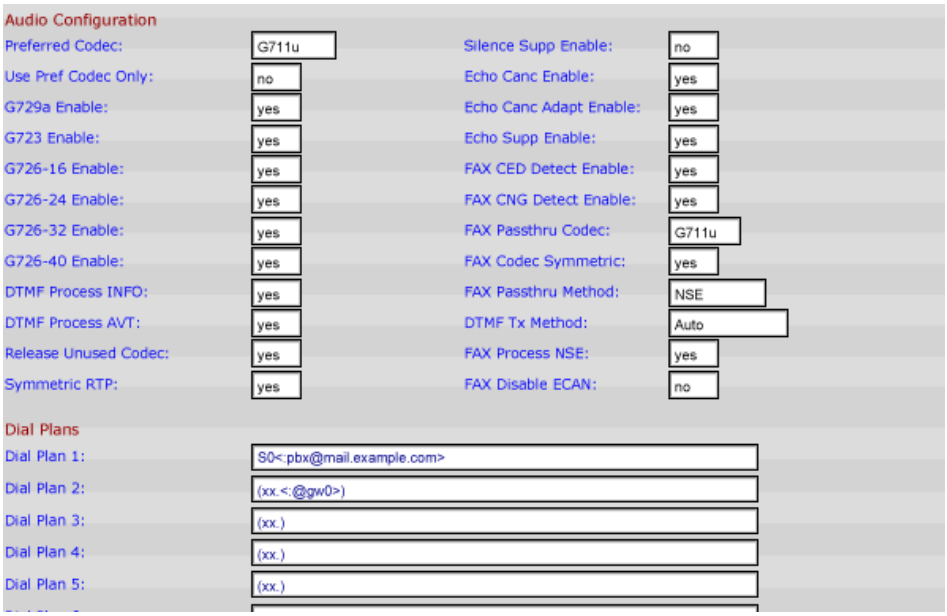
PSTN-To-VoIP Gateway Setup

```
PSTN-to-VoIP Gateway
Enable: yes
PSTN Caller Auth Method:
none
PSTN Caller Default DP: 1
```



The "Dial Plans" are required with the Sipura to select a routing destination. Many FXO devices do not require specific dial plans, as the default VoIP-to-PSTN and PSTN-to-VoIP directions are relatively straightforward. The above dial plans should be entered exactly as listed, except for the hostname of your CommuniGate Pro server. Note too the "pbx" account name – if you used a

different name as the main Auto-Attendant/Receptionist account on your CommuniGate Pro server, then it should be used here. All incoming calls from the PSTN line will be routed to the LAN network with a destination of this account on the CommuniGate Pro server.



C. Routing Outbound Calls to the VoIP-to-PSTN Gateway

Routing some or all numeric addresses (calls to the PSTN) from CommuniGate Pro to the FXO/VoIP-to-PSTN Gateway is very easy.

- Login to the WebAdmin Interface:

  https://mail.example.com:9010

- Select the "Settings" menu option then "Router" (Settings->Router)

- Add the desired routing table entries for the matched numbers you want routed to the FXO gateway. For example:

```
NoRelay:Signal:<1*@example.com> = 1*@192.168.1.2
```

This special syntax simply says "relay all calls starting with a 1 to the device at 192.168.1.2", which for this example would by a Sipura 3000 or other similar device.

Another common Router table entry for gateway routing would be to direct all Signaling events with 10+ digit destination Address(es) of Record (AOR) or what we would commonly call a "phone number":

```
N:S:<(10+d)@example.com> = *@192.168.1.2
```

Similar routing could be configured using a 9 prefix, or 011 or +[country-code] international calling:

```
N:S:<9*@example.com> = *@192.168.1.2
N:S:<011*@example.com> = 011*@192.168.1.2
N:S:<+(10+d)@*> = +*@192.168.1.2
```

Please note that for the 9-prefix example above, the 9 is stripped from the call when it is routed to the FXO device. Also – in the +[country-code] example, the first "*" character in the line matches all domains, while the second "*" character is replaced by the full number, including the Country Code.

Much more complex signal routing and digit matching plans can be configured – please reference the online CommuniGate Pro guide or contact Technical Support for assistance, if necessary.

D. Configuring CommuniGate Pro Network and Relaying Protection

CommuniGate Pro applies Internet-security protections to all protocols available within the product. Relaying protection for SMTP traffic is just as necessary for SIP and VoIP – you don't want to allow at-large remote Internet users to be able to make unauthenticated VoIP calls, just as you don't want them relaying SMTP traffic off your server.

- Connect to your CommuniGate Pro web administration interface:

  https://mail.example.com:9010

- If your subscribers will exist on your Local Area Network, you can define the local area network range of IPs under:

  SETTINGS -> Network -> LAN IPs

- you can then proceed to:

  SETTINGS -> Network -> Client IPs

  and please enable:

  Process LAN IP Addresses as Clients

- If your subscribers are on a separate network, please enter the range of IP addresses under "Client IP Addresses" that you wish to treat as local subscribers for your CommuniGate Pro voice network.

You can then control relaying for SIP under:

Settings -> Real-Time -> SIP -> Sending -> Protocol

The default setting of "Relay to Non-Clients for: [clients]" will allow authenticated users to call outbound, regardless of where they are located when making the call.

E. Softphones – Windows Messenger and Xten (CounterPath) X-Lite

CommuniGate Pro supports SIP (Session Initiation Protocol). SIP enables real-time communications including instant messaging, voice-over-IP, video conferencing, multimedia, whiteboard, and application sharing. Required for implementation is CommuniGate Pro version 5.0 or 5.1 and a SIP-enabled device.

There are many types of SIP-enabled clients (also called "SIP User Agents"). These include actual SIP phones, which are desktop phone models from Cisco and many other vendors, which are used just like any other desktop telephone but are connected via IP over Ethernet. Another type of SIP client device is a "softphone", which is a voice application run on your desktop computer, laptop computer, or mobile computing device which acts just like a normal phone, except that you use a microphone or computer headset to talk. Finally, there are "softclient" applications which are capable of providing multiple types of VoIP services – including instant messaging, voice, video conferencing, and whiteboarding - in one package. Some of these applications include Microsoft Windows Messenger™, linphone, and kphone, with more on the way from both the commercial and open-source worlds.

Three SIP clients available as free downloads include the following. We will also provide details on configuring two of these clients on the following pages – once you've configured one or two softphones, you will likely be comfortable with configuring most of them:

- Microsoft Windows Messenger™ 5.1 can be downloaded here (be sure to download version 5.1 that supports SIP Communication service):

  http://www.microsoft.com/windows/messenger

- CounterPath (formerly Xten) X-Lite ™ Softphone, available here:

  http://www.counterpath.com/index.php?menu=download

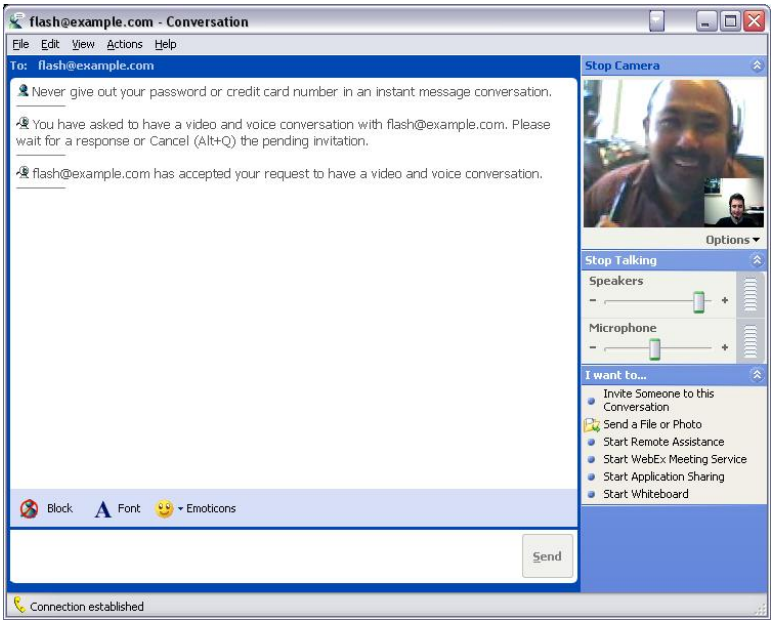
- SJlabs SJphone™ available on Windows/Mac/Linux:

  http://www.sjlabs.com/sjp.html

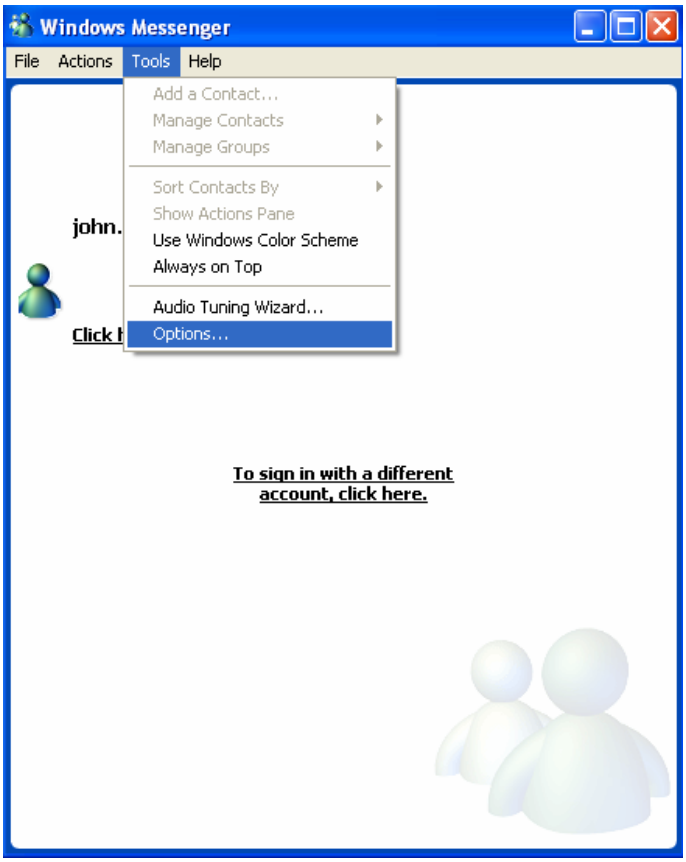
- Microsoft Windows Messenger™

You can easily demo any of the available services that Messenger facilitates by configuring it on two Windows clients. We will assume that two accounts have been created on CommuniGate Pro with passwords and that both client machines are on the same network as the server.

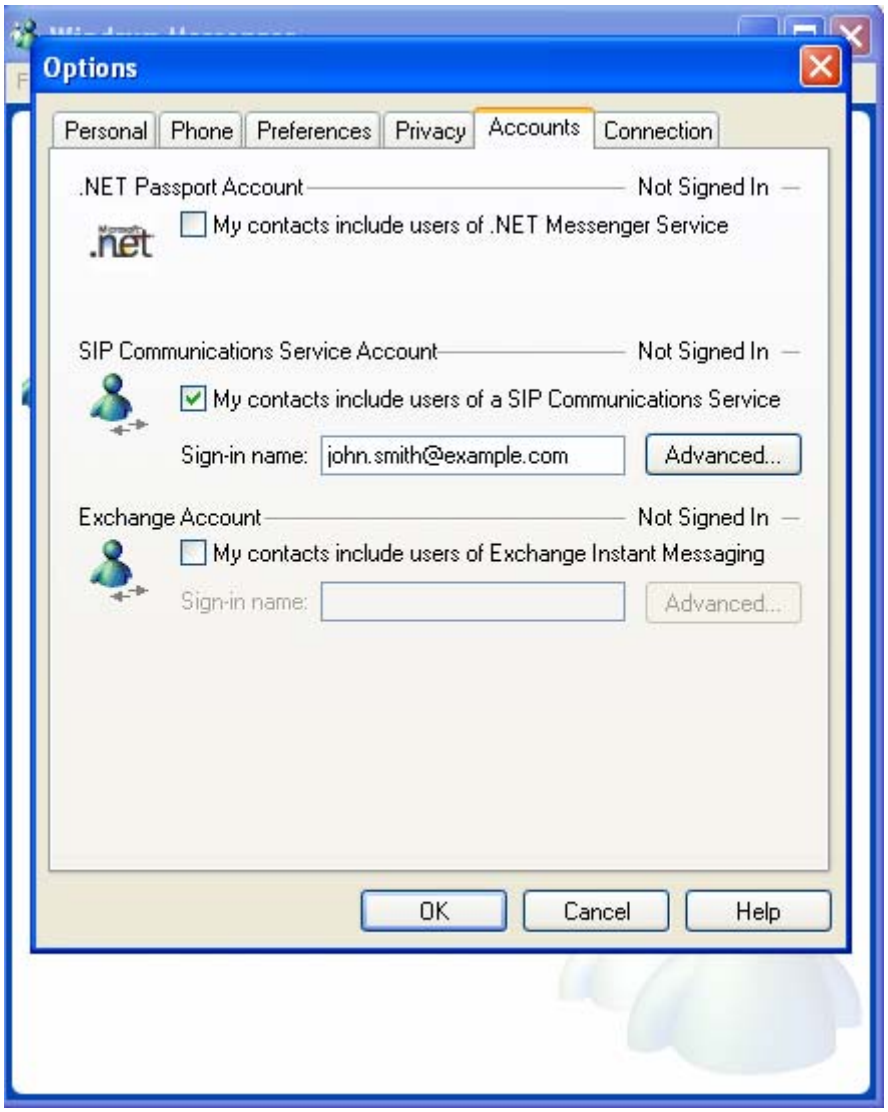
To configure an account: Open Windows messenger and go to the Tools menu and select Options.



Windows Messenger 5.1 provides Voice, Video, IM, and Desktop Sharing through CommuniGate Pro

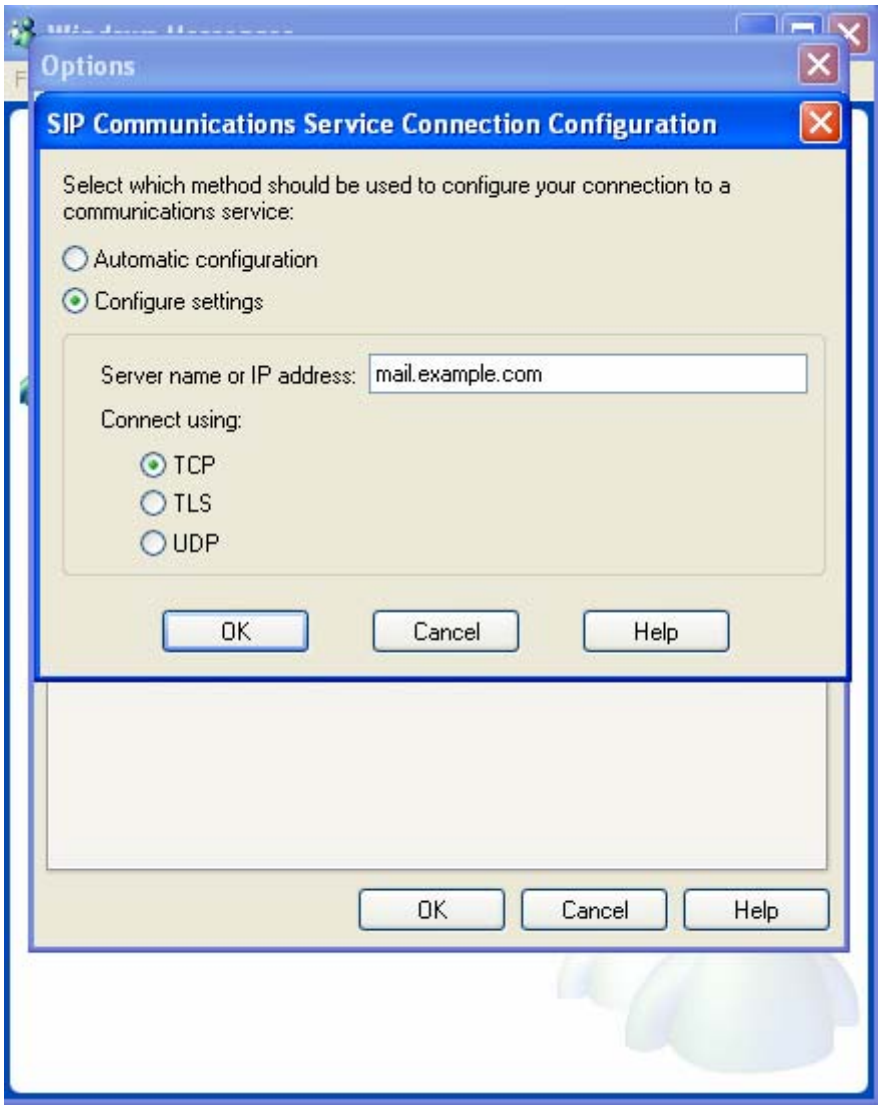


You will then want to please click on the Accounts tab. Once displayed, make sure that the check box for "My contacts include users of a SIP Communications Service". Then, please type your e-mail address as the Sign-in name:



The SIP protocol initiates a distributed, global, standards-based IP network for voice, video, IM, and multi-media.

You then click the Advanced button. Make sure that the Configure Settings Radio button is clicked. You will then type in the domain name or IP address of the CommuniGate Pro Server. The default setting of TCP for the "connect using" parameter is sufficient. Click Ok twice and that should conclude the set-up. You can also use the "TLS" option for secure, encrypted SIP signaling transport.



Windows Messenger works best with TCP-based connections. Particularly, CommuniGate Systems always recommends TLS-encrypted signaling.

Note: for secure IM, your IM client must recognize the signer of the SSL certificate supplied by the server. If your server uses a certificate signed by a recognized Certificate Authority (CA), then the certificate should be imported for the appropriate domain (Users->(Select Domain)->Security), and no additional handling should be required. If using a server-generated self-signed certificate, then all users must import the self-signed certificate - you can do this by going to the logon page for WebMail

and following the link "Security Certificate". Once the cert is imported into Windows, then select "TLS" here.

Note: On the Accounts tab you will see a check box for .Net Passport Account. If you are not already signed up for a Microsoft .Net Passport and/or never plan on using one, we suggest unchecking this box. It is not necessary for SIP communications with Messenger and you will avoid the .Net login screen each time Messenger is run.

If both clients have configured their settings properly, they should both be able to run Windows messenger. A password prompt will appear, use the same password as with the e-mail account.

Now each would add the other e-mail address as a contact. If the contact has been created properly and shows a status of online, the person can right click on the contact name and facilitate any of the previously mentioned functionality. Again this would include voice/video conversations, voice conversations, instant messaging, whiteboard and/or application sharing, etc.

- CounterPath X-Lite™

CounterPath X-Lite™ is a great, free "softphone" available for download. Xten also provides a number of other more sophisticated commercial tools (such as EyeBeam with voice, video, IM, and Presence with CommuniGate Pro), but X-Lite is a fantastic application for learning to appreciate Voice over IP:

http://www.counterpath.com/index.php?menu=download

The following screenshots demonstrate setting up X-Lite for use with CommuniGate Pro. After installing X-Lite, opening up the application pops up the X-Lite Softphone client, which will likely look at least familiar to anyone who has used a telephone.

The application will then immediately open up a menu page, asking the user to enter their VoIP/SIP server and user information:

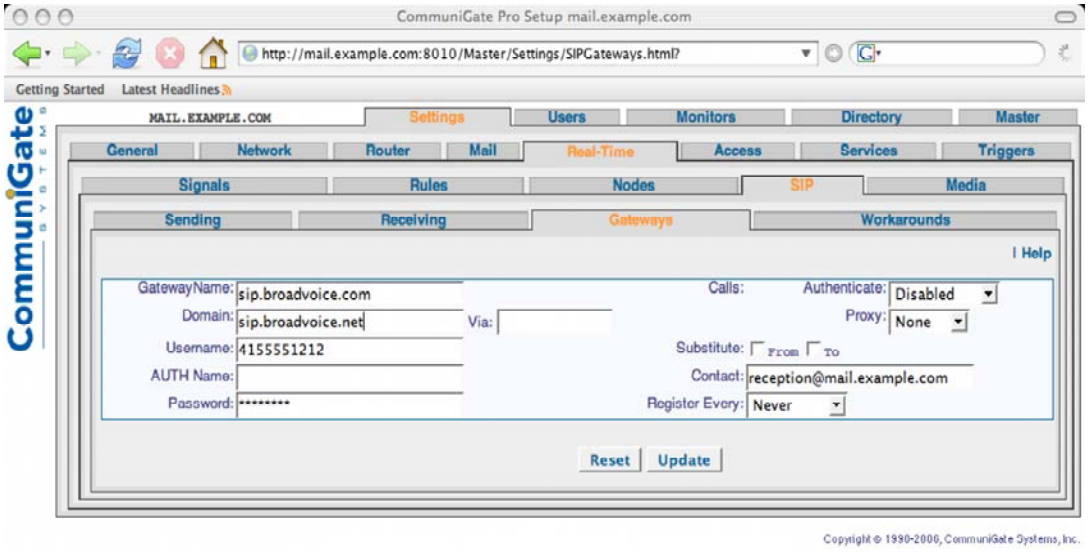
Entering the information in the menu is similar to entering in any other server and user information for use with the CommuniGate Pro Internet Communications Platform – this is the great ease of use and flexibility which arrives from using a single messaging solution for so many different forms of communication. The same username and password can provide users all the authentication and access those users require:

Once these settings have been entered, the softphone is now ready for use within the CommuniGate Pro system – calling other users on the system who also have a softphone is as easy as just entering their e-mail address or phone number alias, and clicking the telephone button:

The CommuniGate Pro system can also be integrated easily with a "VoIP to PSTN gateway", which provides a connection between an IP-based voice network and the Publicly Switched Telephone Network (PSTN). This allows a VoIP call to connect with any normal telephone or cellular phone network.

There are two main options for "VoIP to PSTN" connectivity. One option is to bring this system in-house, by purchasing a VoIP-PSTN gateway switch and connecting this switch to your telephone (land-line) service provider. A second option - often the easiest and most cost effective option for an enterprise or ISP just beginning to provide VoIP services is to get this service from one of the major VoIP Services Providers, such as VoicePulse, Broadvoice, and many others.

The below example demonstrates the configuration of CommuniGate Pro for use with the Broadvoice VoIP-to-PSTN service connectivity.



Configuring a SIP-PSTN Gateway.

Once the service has been enabled, the CommuniGate Pro users authorized to access this VoIP/SIP functionality can now make telephone calls anywhere in the world, to any public telephone or cellular network, from any of their voice-enabled SIP clients.

F. IP Phones, such as the Polycom 501

CommuniGate Systems integrates with all SIP-standards-based IP phones. Phones tested to date include (at the least) those from Polycom, SNOM, Grandstream, Zyxel, Hitachi Cable, Cisco, and various other lesser known. All SIP-standards phones should work with CommuniGate Pro. However, SIP has evolved and in the event that a specific device is found not to work, CommuniGate Pro provides a "SIP Workaround" Feature which can be configured at runtime (while the system is running) to provide specific workarounds to a specific device. And in the worst case, please notify Technical Support of an interoperability problem.

The following section describes the setup of a Polycom 501 IP Phone. Most IP phones will use a similar configuration process, but the Polycom 501 is clearly one of the best IP phones on the market, providing speaker phone and advanced call management options.

- Each Polycom phone contains a built-in webserver for configuration. After putting the phone on your LAN network, it will get a DHCP address, which can be viewed on the phone's LCD screen.

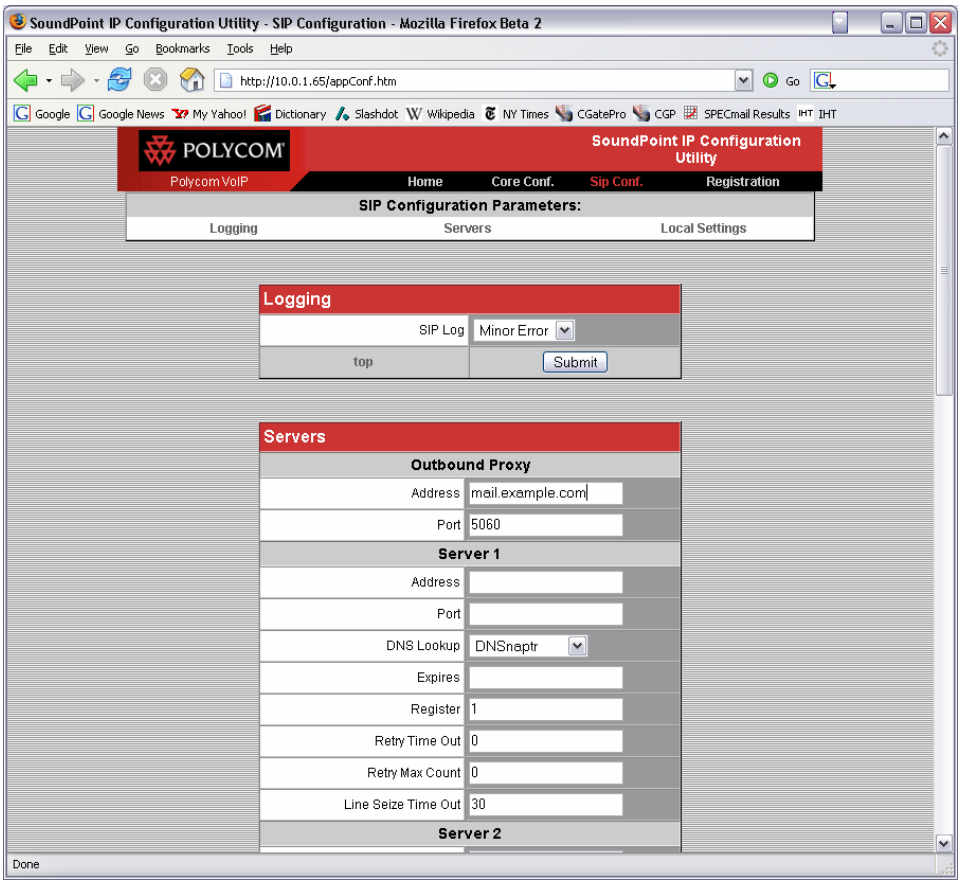
- Use your favorite web browser to connect to the IP address of the phone. The default login for the Polycom phones is (please be sure to replace the "192.168.1.2" with the actual IP address of your IP Phone, as discovered in Step 1):

  http://192.168.1.2

  username: `Polycom`

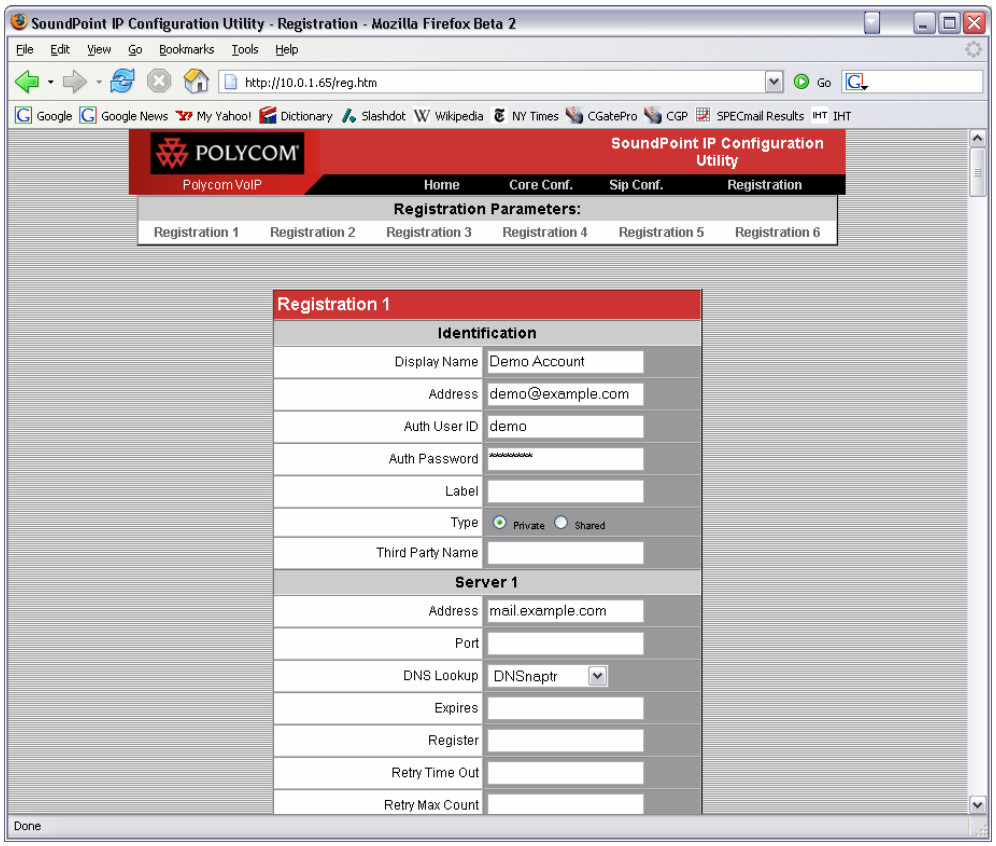
  password: `456`

- After logging in, select the "SIP Conf." tab, and enter the hostname or IP address of your CommuniGate Pro system for the Outbound Proxy:



Configuring an "Outbound Proxy", which should generally be the primary address of the CommuniGate Pro Server/Cluster.

- On the "Registration" tab, enter your "Display Name" (Real Name), SIP address (same as your e-mail address), and Auth User ID and Password. The Auth User ID could be just your short username, such as "demo", or it can also work as the fully qualified name, such as demo@example.com. Also enter the Address of the server, which in most architectures will be the hostname or domain name of your environment, and often times be the same as your Outbound Proxy address above.



The only fields one generally must fill-in are: Address, Auth User ID, and Auth Password, as well as the Server (1) Address.

- That's it. After updating each change, the Polycom will restart. After your last set of changes, the phone should "REGISTER" as your account, and your account name will be displayed on the phone's LCD screen. Incoming calls to your account or extension will ring the phone, as well as your other SIP devices.

G. Recording and Uploading a new Auto-Attendant/PBX "Welcome Greeting"

CommuniGate Pro is designed to allow granular control of the PBX environment - even on a multi-domain server or cluster, every domain can have its own WebMail skins, its own PBX menu system and auto-attendant, PSTN gateways, enabled/disabled services, etc.

This section briefly describes how to upload your own Organization's personalized PBX greeting.

1) Record a New Greeting

http://www.communigate.com/CommuniGatePro/PBXApp.html#Formats

> Supported Media Formats
>
> The following audio file formats are supported:
>
> **WAV** (data starts with the RIFF tag) -a file should contain a single data chunk with PCM 8-bit or 16-bit data.
>
> **AU** (data starts with the .snd tag) - a file should contain PCM 8-bit or 16-bit data, or 8-bit mu-Law data.

Note: all recording should be done in the 8 Khz Mono mode, 16 bit. If you record everything in 22Khz, and then scale it down to 8Khz, a lot of noise is heard. For best results, use a decent-quality recording setup, such as a USB-based microphone and mixer.

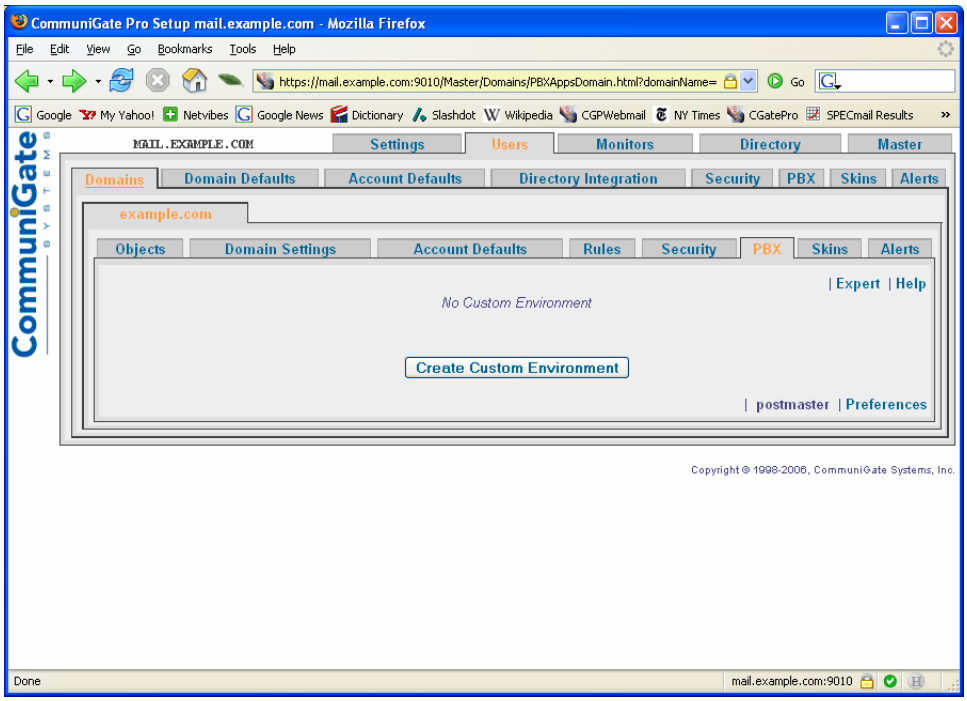
2) Save the new Greeting File

By default, the CommuniGate Pro PBX environment references a WAV file called "receptionprompt.wav". The easiest way to modify the Auto-Attendant/Receptionist Greeting then is to save your new Greeting as the same file name. The CommuniGate Pro object model will allow you to safely delete this file later, if you decide it is not right.

3) If using a "multi-domain PBX environment", then Create a Custom PBX Environment for one domain

If using a single-domain PBX environment, this step can be skipped.

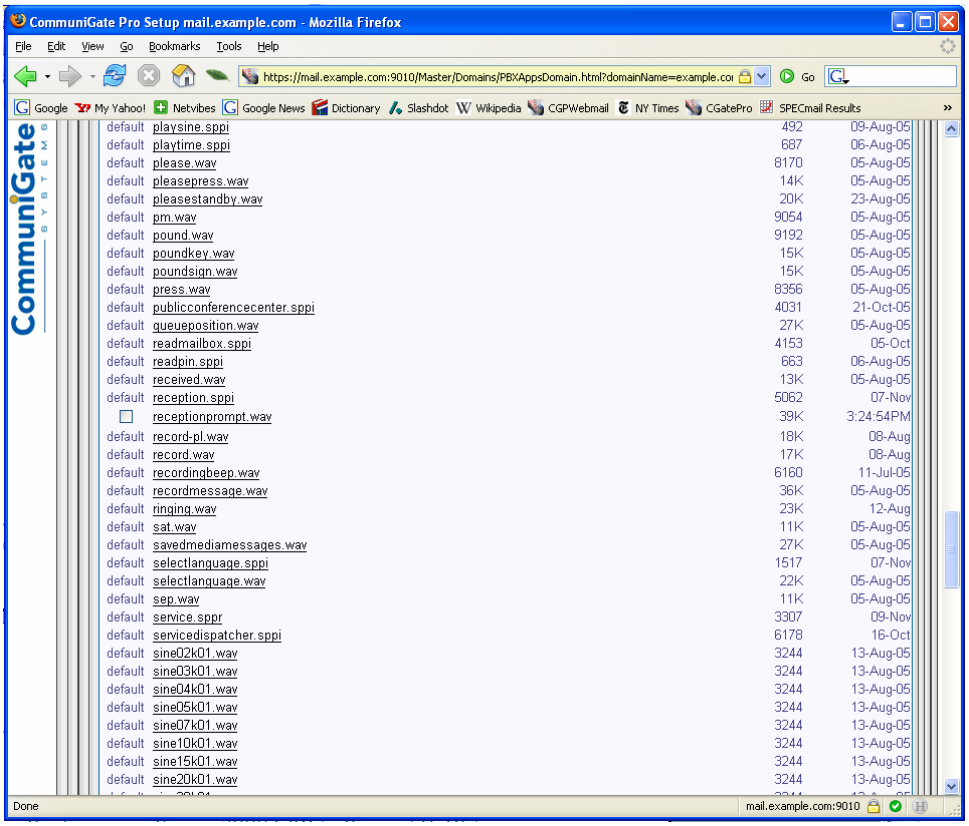
Please login to the WebAdmin Interface and select [Users->(Select Domain)->PBX] then click "Create Custom Environment":



Creating a Custom PBX Environment for just one domain on the server/cluster.

4) Upload the new WAV file using the "Browse" and "Upload File" options

After the new WAV file is uploaded, you should see in the WebAdmin Interface that the file is marked as a "custom file", as denoted by the checkbox here:



A new "receptionprompt.wav" file has been uploaded to the CommuniGate Pro PBX.

In order to test, use an IP phone, softphone, or normal call through a SIP-PSTN gateway to reach the CommuniGate Pro PBX/Auto-Attendant. This is normally accomplished by dialing extension "200" or "0".

H. E-mail

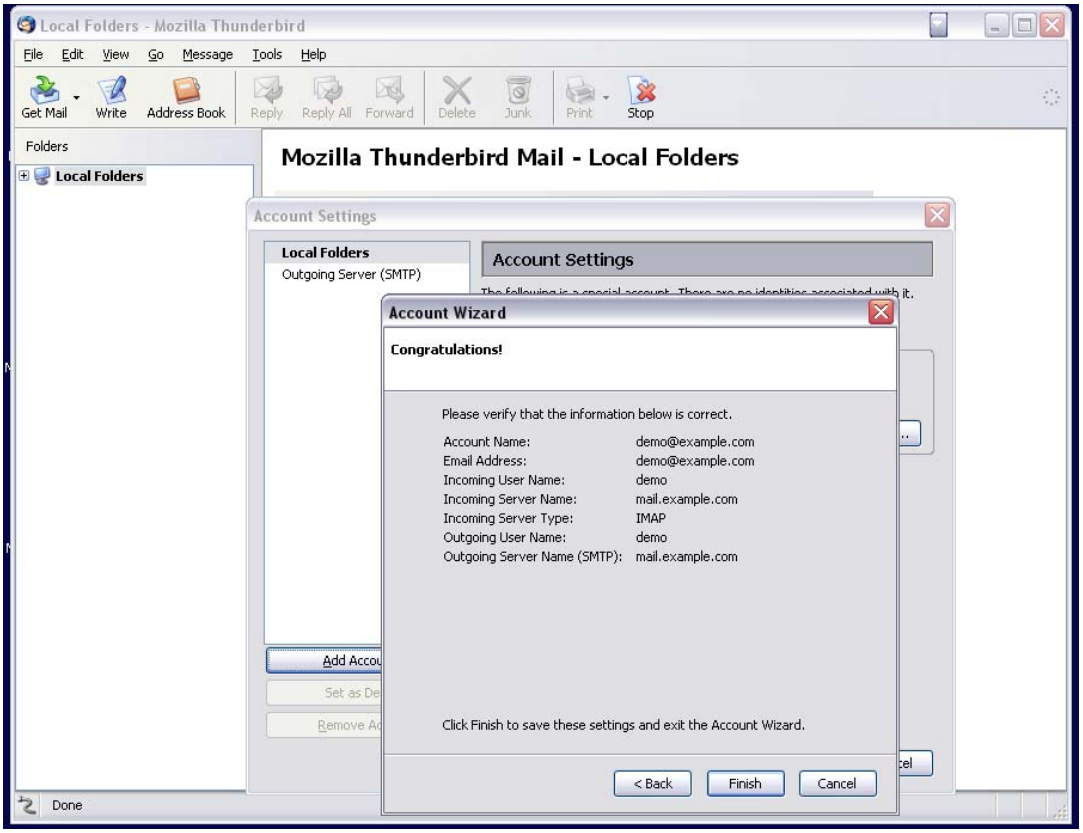
CommuniGate Pro is fully compatible with any "standards-based mail user agent" (MUA). There are many familiar ones to choose from – Microsoft Outlook™ or Outlook Express™ (using POP or IMAP), Eudora™, Mozilla Thunderbird™, Pine™, Netscape™, and lots of others. Feel free to choose your favorite.

The following section briefly describes how to configure Mozilla Thunderbird for POP use with CommuniGate Pro. Thunderbird can be downloaded in free or paid versions from:

http://www.mozilla.com

After downloading the Thunderbird installer, run the installer and use the default install options. The install process will place a Thunderbird start icon on your desktop. Clicking the icon will start the application.

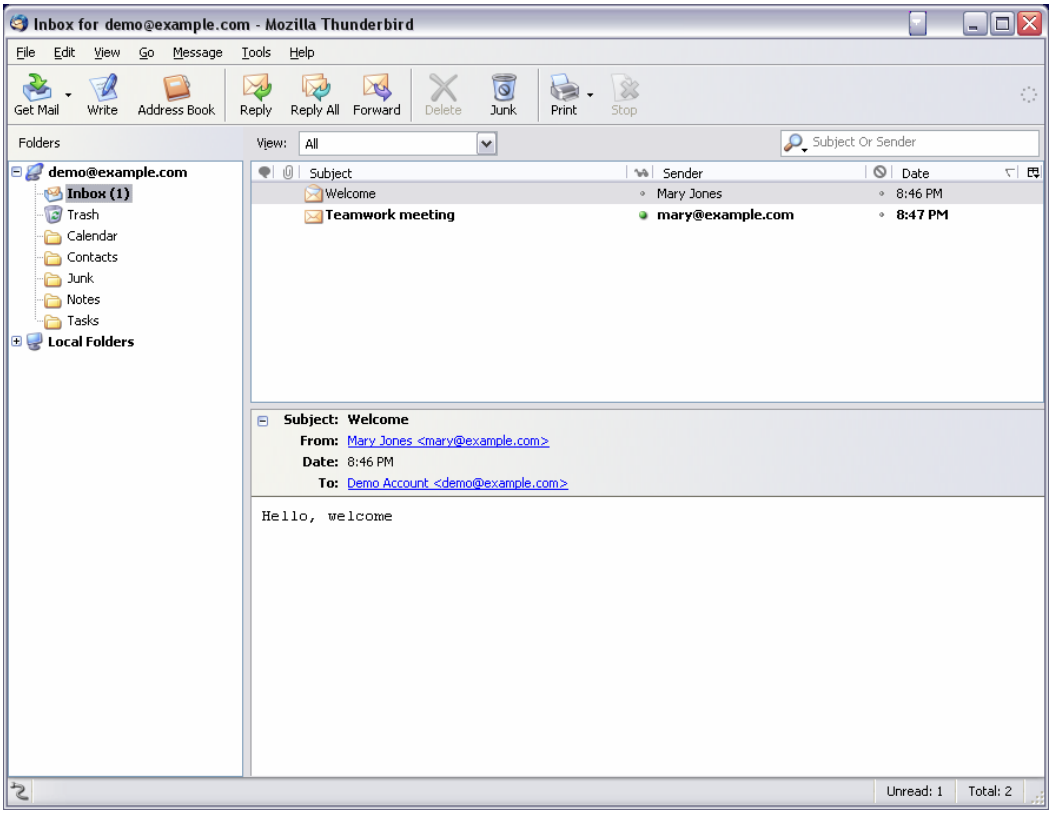
Configuring Thunderbird for e-mail sending and receiving (SMTP and POP/IMAP) is very easy – just use the Tools menu option, select Account Settings, then use the Add Account option for a new account for SMTP and POP or IMAP.



Configuring Thunderbird for IMAP with CommuniGate Pro.

The typical basic options required include your real name, e-mail address, and the CommuniGate Pro mail server name for both Incoming and Outgoing e-mail. Your User Name is usually the account part your e-mail address. In the below example, the User Name can be either "mary.jones" or "mary.jones@example.com", as CommuniGate Pro will recognize these names interchangeably.

Thunderbird should now be fully operational using POP or IMAP. The Get Mail toolbar option should connect to the server, which will then ask the user to login using the password. After a successful login, new messages are displayed in the INBOX:



Using Mozilla Thunderbird with CommuniGate Pro.

I. Collaboration and Groupware

CommuniGate Systems supports collaboration or "Groupware" functionality with the CommuniGate Pro Server. CommuniGate Pro enables e-mail, calendaring and scheduling using Microsoft Outlook's advanced functionality, and provides an integrated Web client allowing users to access their e-mail, calendaring, and scheduling information from any web browser.

1) How does the Groupware addition fit in the overall solution?

Groupware is a component within the overall CommuniGate Pro solution, just as the LDAP directory and IMAP module are components. The server stores all groupware data (i.e. calendars, tasks, contacts) and messaging data (i.e. e-mails) in Internet-standard formats, allowing users to access their information through a wide variety of client applications. Users have maximum flexibility when choosing clients:

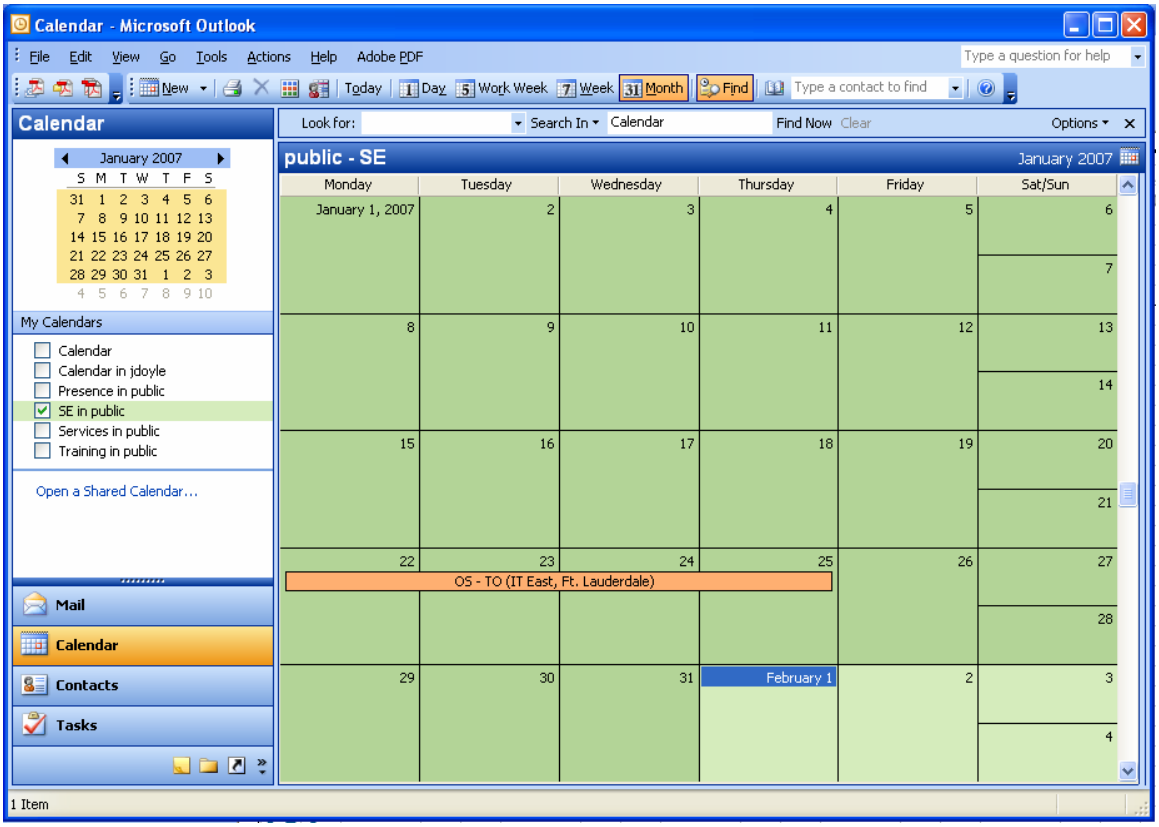
- Keep Outlook in "workgroup" mode, connecting via the MAPI interface,

- Access the same data via the full-featured WebMail client, or
- Choose any application supporting e-mail standards SMTP/POP/IMAP (such as Mozilla Thunderbird) and XMPP/SIP standards (such as Gaim) or calendaring standards iCAL/iTIP/iMIP (such as Mozilla Sunbird or Novell Evolution).

While you could always run Outlook with CommuniGate Pro in Internet mode - since the release of CommuniGate Pro v4.1 with Groupware, you can use Outlook in Corporate Workgroup mode, taking advantage of its advanced calendaring/tasks/etc functions in combination with Secure IM for Enterprises or global IMS/SIP/XMPP networks.

Utilizing Outlook in Corporate Workgroup mode against the CommuniGate Pro server requires the installation of the MAPI connector. This small piece of software translates the proprietary Microsoft language that Outlook uses to talk to Exchange (MAPI), into the language that CommuniGate Pro understands (IMAP). Additionally, the connection can be set to run in secure SSL mode (port 993) for sending and receiving mail in Outlook. This provides remote workers the flexibility to run Outlook without need of complex VPNs.

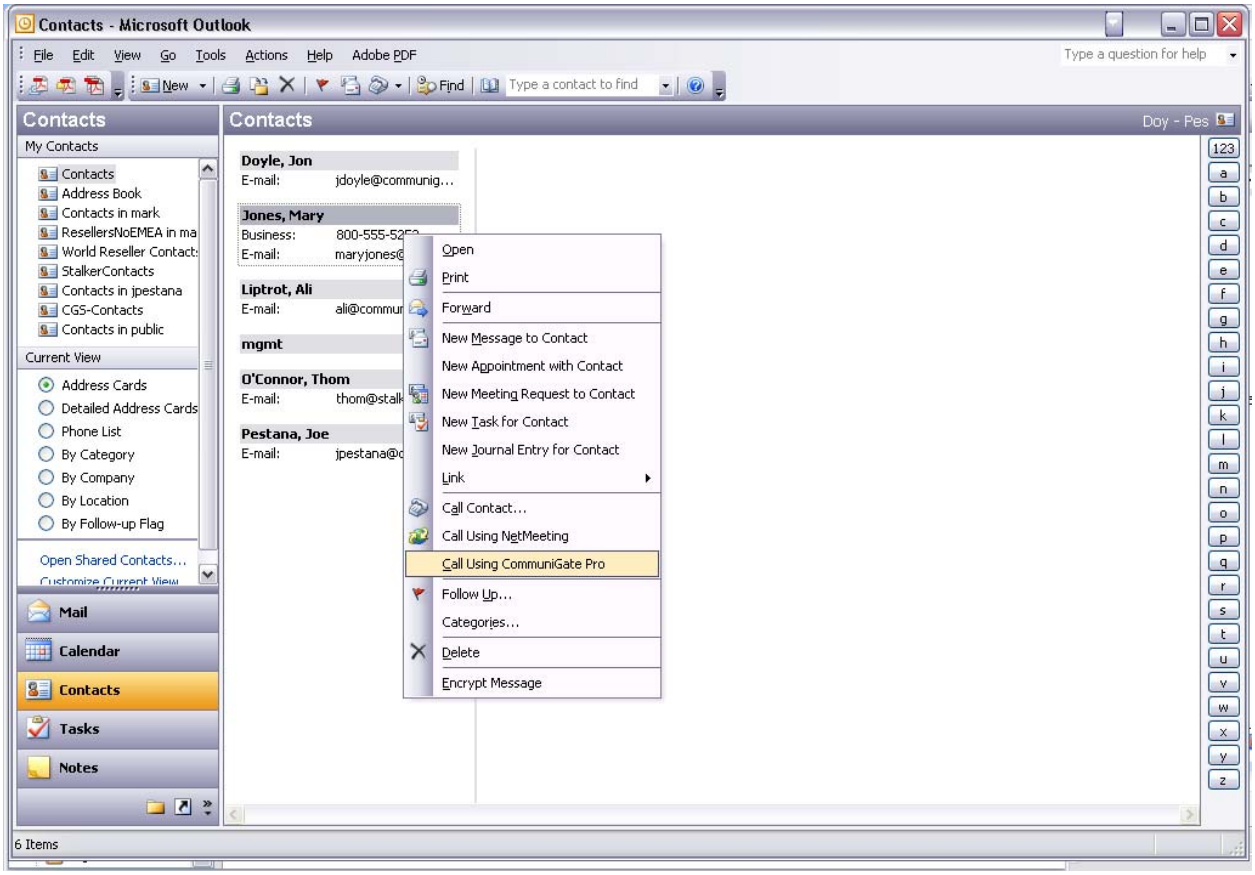
CommuniGate Pro with Groupware allows users to access the server through their existing Outlook clients (via the MAPI Connector), providing the same groupware functionality for Outlook users as if they were connected to a legacy MS Exchange server, but with enhanced reliability, speed, and mailbox sharing abilities.



Microsoft Outlook Groupware/Calendaring with CommuniGate Pro and the CommuniGate Pro Outlook Plugin (MAPI Connector).

2) Click-to-Call

Users in Outlook can now place VoIP calls directly from the Outlook address book, often called "Click-to-Call". This technology allows a softphone, or desktop SIP based phones that are registered to the user to be used rapidly from contact lists. Right-clicking on any phone number or e-mail address within Outlook:



Click-to-Call with Microsoft Outlook and CommuniGate Pro.

3) CommuniGate Pro Outlook Plugin ("MAPI Connector")

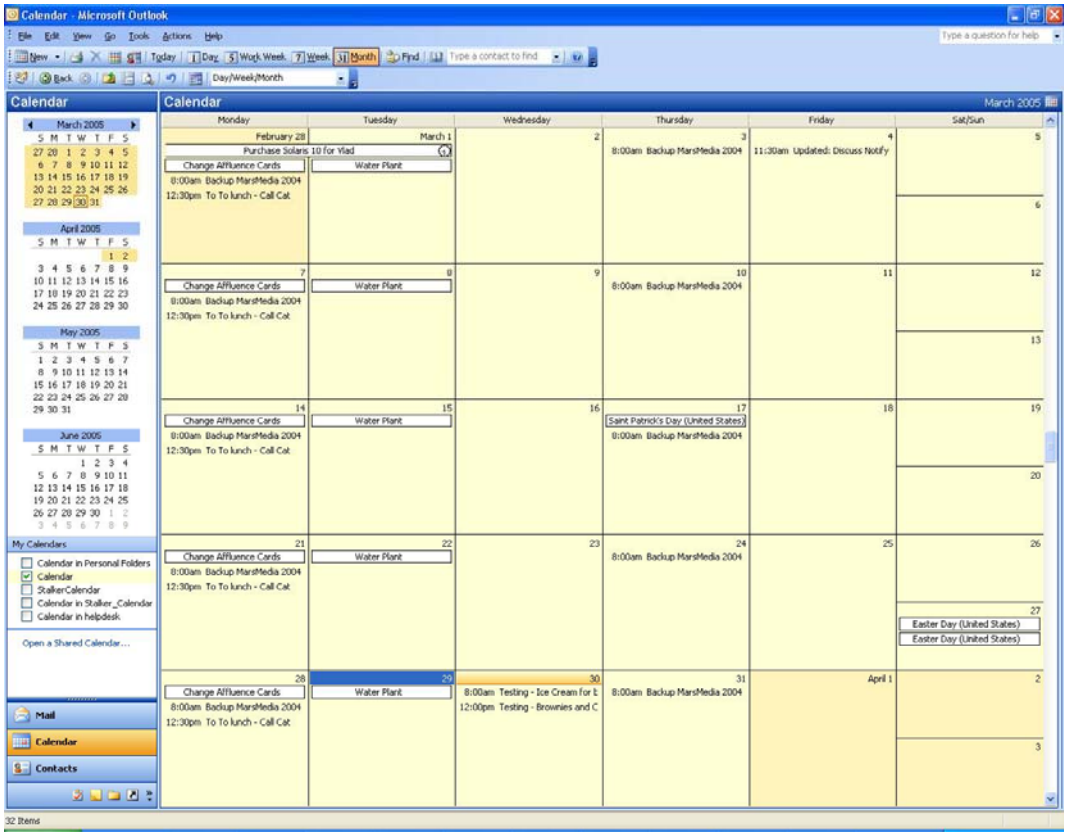
With CommuniGate Pro, Outlook provides virtually all Exchange functionality. CommuniGate Pro's Outlook Plugin (MAPI Connector) also provides advanced functions that Exchange does not offer, such as:

Placing VoIP calls from the contact lists. Click-to-Call allows a user to wear a headset and dial numbers, or simply speed the process of placing calls to an IP-based desk phone.

- The CommuniGate Pro MAPI Connector allows creation of "server-side" rules eliminating the need to re-create these on each copy of Outlook (desk/laptop) or in the WebMail. Rules can be for routing purposes; example, new mail with subject="emergency" gets redirected to my mobile, or mail from my old girlfriend is filed to "trash folder". Legacy Outlook environments do rules on the client, not the server which causes problems for multi-client use, or when desktops crash or laptops are lost.

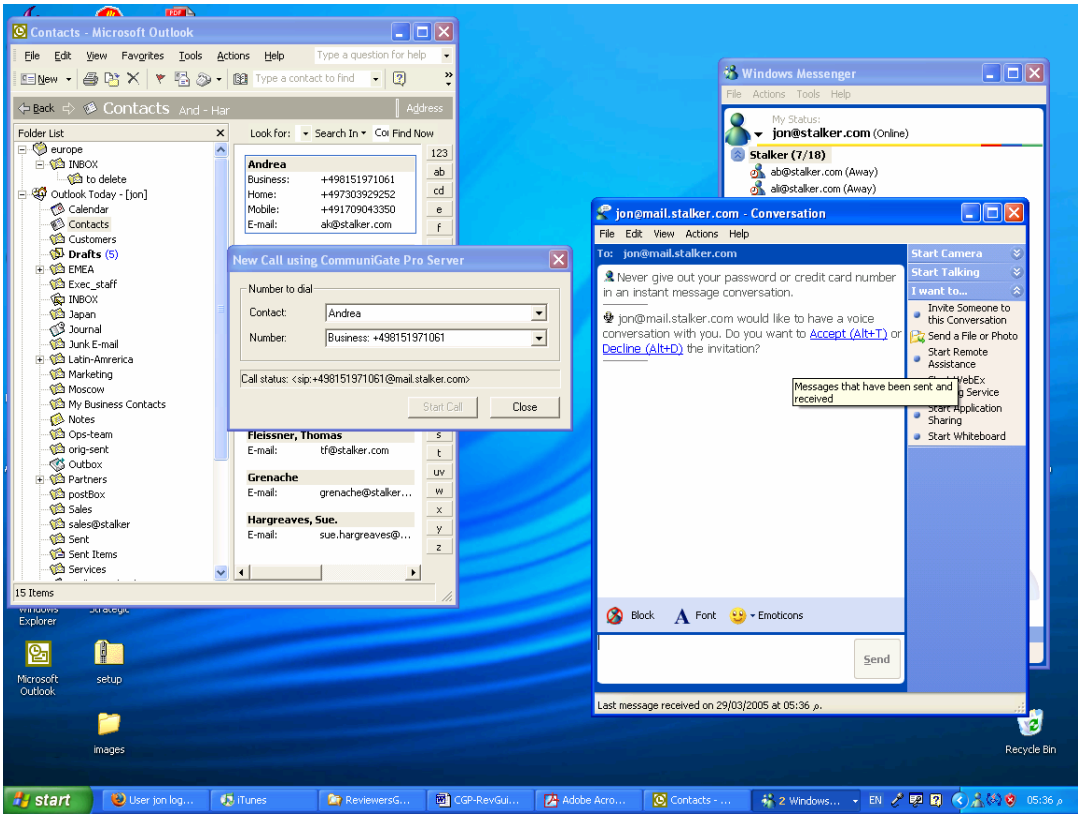
- Outlook with the CommuniGate Pro MAPI Connector can be run in secure mode for sending and receiving mail over SSL with secure authentication. This allows Outlook at home without VPN, or in remote sites. Kerberos/ Active Directory® single sign-on is supported.

- Multiple calendar application support is possible. WebMail users, or clients on the Apple platform, can mix various mail clients they personally use, depending upon their location or preference. Compatible applications including Mozilla Sunbird, Novell Evolution, KDE KOrganizer, and Microsoft Entourage.



Shared Calendars in Microsoft Outlook.

Below is a view of Microsoft Outlook running in full workgroup mode with the user placing a VoIP call through Windows Messenger.



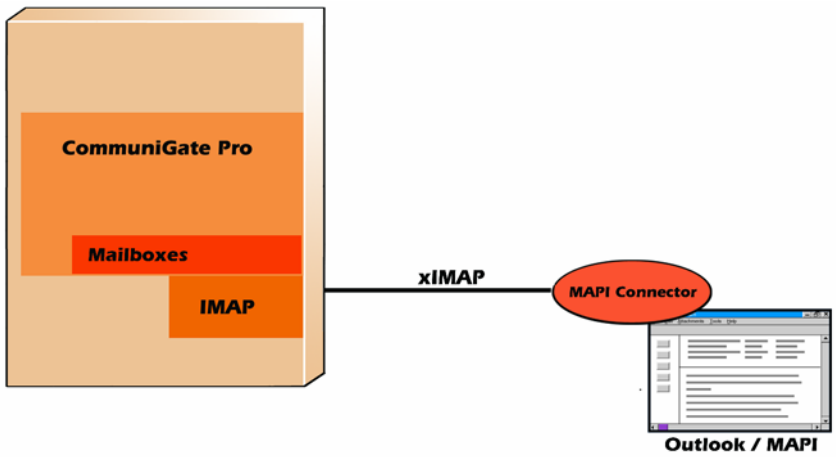
Click-to-Call with the CommuniGate Pro platform from Microsoft Outlook, calling using Microsoft Windows Messenger.

This would be the same case for an IP based phone, like SNOM or Cisco, which are registered to the user's Account:

- User right clicks on the contact, and selects, Call using CommuniGate Pro.
- CommuniGate Pro's Outlook Plugin (MAPI Connector) initiates an invitation to the SIP devices - in this case Windows Messenger 5.1 that a call is being placed. In the case of an IP phone, it would ring. Here we see Messenger sends a "pop" dialogue to the same user.
- The user either clicks "accept" or does an "ALT+T" and the recipient's phone (the "Callee") starts to ring. In the case of an IP-based phone - after the Calling user (the "Caller") picked up the receiver or answered - the line would begin to ring on the other end.

- The CommuniGate Pro client can be used in this fashion remotely, and the main CommuniGate Pro server will process the VoIP calls no matter where the user is. This is especially effective when the user is on the road in hotels, or in another country with a good hotel DSL connection, but would like to avoid the phone charges, or would like to arrange conference call with multiple people on the fly.

a) MAPI Connector Architecture Diagram



The CommuniGate Pro Outlook Plugin ("MAPI Connector") resides on the client-side desktop or laptop, and transparently translates Microsoft Windows proprietary "MAPI" protocol commands into secure IMAP.

b) MAPI Connector Technology Overview

The CommuniGate Pro Outlook Plugin (MAPI Connector) acts as a "MAPI provider". It accepts MAPI requests from Microsoft Outlook (Outlook 97, Outlook 2000, XP, and Outlook 2003) running in the Corporate Workgroup mode and from other Windows applications. The MAPI Connector then converts (translates) these requests into extended IMAP commands and sends them to the CommuniGate Pro Server.

When reading from mailboxes on the server, the CommuniGate Pro MAPI Connector converts (translates) messages back into the "MAPI object" format and passes the converted objects to the Windows MAPI libraries and applications (such as Outlook).

The CommuniGate Pro MAPI Connector contains two code parts (shared libraries). The main functionality is implemented on the server side. But, the second part of the Connector MUST be installed on the client, along with Outlook, to be able to effectively translate the data and connect to the CommuniGate Pro server.

c) WebMail Interface

CommuniGate Pro's groupware functionality is not limited solely to Outlook on the desktop. The integrated WebMail interface enables remote team members to access e-

mail, calendars, contacts, group scheduling, and electronic discussions while on the road.

d) Groupware Configuration with Other Applications

Standards-based groupware storage and processing ensures interoperability with any other systems using standard iCAL/iMIP/iTIP and vCAL/vCard data formats for information exchange - with Exchange™ and Lotus Notes™ servers, Apple's iCAL calendar clients, PALM™ calendaring applications, and many others.

CAP (Calendar Access Protocol) client applications can also use the CAP protocol supported with the CommuniGate Pro, and thus directly access and modify the same groupware data as the Outlook and WebMail clients.

Finally, WebDAV (which stands for "Web-based Distributed Authoring and Versioning") is a new protocol which uses a set of extensions to the HTTP protocol to allow users to collaboratively edit and manage files on remote web servers. WebDAV has been incorporated into CommuniGate Pro to allow for future integration with this emerging protocol, which promises to be a strong open-standard for collaboration and calendaring.

e) Options for Reviewing Groupware

To review the entire solution and take full advantage of the Groupware functionality, the CommuniGate Pro server must be installed and properly configured with user accounts. The server is available for download on all platforms from the CommuniGate Systems web site: http://www.communigate.com/download.html

The site also contains install and configuration documentation on-line for easy access: http://www.communigate.com/CommuniGatePro

If you want to test Outlook, in addition to preparing the server side you must install the MAPI connector on the clients you will be using to test. Please see the following section in this guide for instructions on installing and configuring the MAPI connector.

NOTE: If you download the CommuniGate Pro and MAPI connector trial software from the CommuniGate Systems Website, the default trial license restricts the number of users that can access the CommuniGate Pro server with Outlook via the MAPI connector. The trial license allows for 5 users. To request a larger trial license, please send a note to reviews@communigate.com.

NOTE: To access the WebMail client, you must install and configure the server with user accounts.

f) What Benefits Does CommuniGate Pro with Groupware Provide to its Customers?

Traditionally, corporations have had to settle for complex, high-maintenance messaging solutions in order to have groupware functionality. Now, CommuniGate Systems offers enterprises worldwide another option: support for e-mail, shared

folders, calendaring and group scheduling, with the robust and secure CommuniGate Pro messaging solution.

With Outlook's advanced functionality and a full-featured WebMail interface, users stay productive, accessing the same information in and out of the office. Adding the voice capabilities to the workgroup allows for more productive collaboration. The additional security and mobility aspects of CommuniGate Pro delivers to organizations an advanced platform with native SSL support that reduces costs and complexity by eliminating the need to provide expensive VPN solutions in order to communicate securely.

g) Affordable, Full-Featured Solution

CommuniGate Pro with Groupware provides an ideal option for organizations looking for calendaring and scheduling on the desktop, or those wanting to replace expensive and unreliable messaging environments without losing end user functionality. The CommuniGate Pro server is extremely easy to install and maintain, and supports tens of thousands of users on a single server, dramatically reducing overhead and administration costs typically associated with traditional enterprise solutions.

Administrators can consolidate Exchange back-ends while utilizing existing hardware – CommuniGate Pro supports over 35 operating system platforms today and can be clustered in many instances using multiple operating systems within a single cluster.

h) Advanced Outlook Functionality for End-Users

Users who prefer Outlook on the desktop can now take advantage of its advanced collaboration features. Working in Corporate Workgroup mode they receive e-mail, arrange meetings, share free/busy information and reply to requests in the familiar Outlook Interface. Users who previously ran Outlook in limited Internet mode can now fully utilize its calendaring and scheduling functionality. The CommuniGate Pro client product provides advanced voice and filter features greatly enhancing the control and power provided at the desktop.

i) Limited Disruption for End Users

While the e-mail server might change on the back-end, your end users should not be affected. For the end users who already have Outlook, the migration would be transparent; they keep using Outlook in same manner to which they have become accustomed.

There is no need to migrate all users at once. CommuniGate Pro can run alongside Microsoft Exchange or another solution, while you gradually migrate end-users.

j) Automatic Install and Upgrades

The MAPI connector can be installed across the network so administrators do not have to visit every desktop. The connector is self-updating and automatically checks for a new version every time it logs on to the CommuniGate Pro server. Management

systems and scripts can be used to provide large scale administration with versioning control and management.

k) Increased Productivity on the Road

Secure access to corporate information is crucial for communication in flexible work environments. Through the full-featured WebMail interface, users get mobile access to corporate e-mail and scheduling information from any browser. The capability to bring the office with the mobile worker increases ease for customers to communicate with that person, and reduce the IT complexity. SIP voice numbers can be used in any location where presence can be established. Example, users can bring their laptop, and now their +1-415-xxx-xxxx phone line with them also to Paris, Munich, or Sao Paulo. The user will continue to receive mail and phone calls in any location, but also make calls and send messages and schedule appointments. Thus, the office can now travel, not just the person.

l) Installing the MAPI Connector and Configuring Outlook

The following components are required to complete the installation:

- The CommuniGate Pro MAPI Connector installer.
- A full, licensed copy of Microsoft Outlook 97, 2000, XP or 2003.

The CommuniGate Pro MAPI connector installer is available for Microsoft Windows NT/2000/XP and 95/98/ME, and works with Outlook 97/2000/2003/XP. The MAPI Connector is available from the CommuniGate Systems download website:

http://www.communigate.com/download

m) Install the MAPI Connector

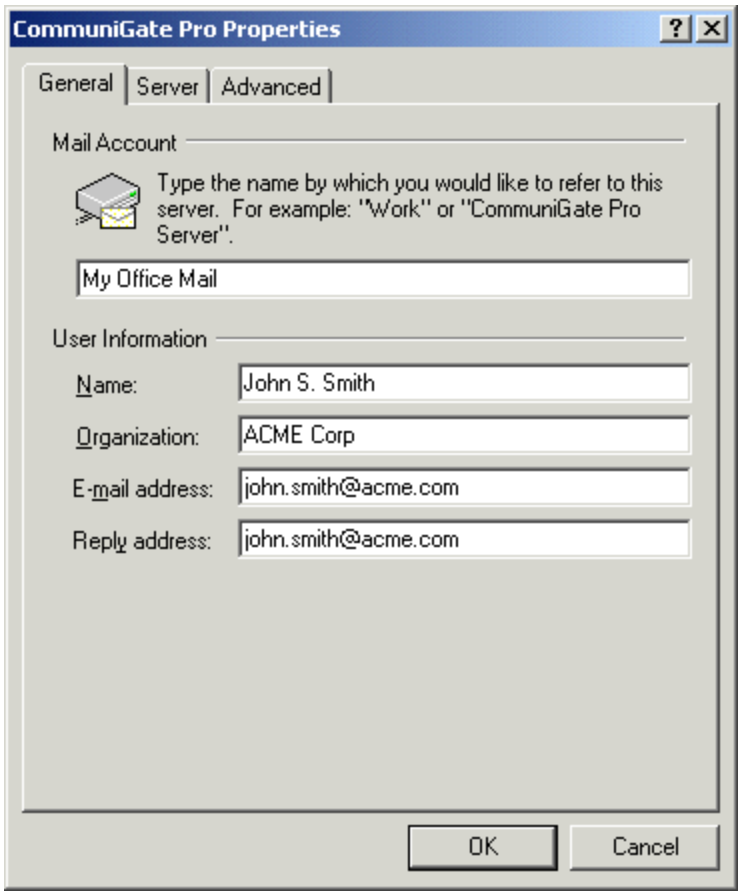
You need to install the CommuniGate Pro MAPI Connector shared library (.dll) on Microsoft Windows workstations. Download the CommuniGate Pro MAPI Connector archive and unpack it. The unpacked folder contains the Setup.exe file.

Start the unpacked Setup.exe application to install or update your CommuniGate Pro MAPI Connector software. After a successful install, the application may ask you to re-create your Mail Profile.

n) Create a Mail Profile

When the CommuniGate Pro MAPI Connector is installed on a client workstation, you can create a Mail Profile that will tell Outlook and other applications to use the CommuniGate Pro MAPI services.

If you use Outlook 98 or Outlook 2000 you should check that it is configured to run in the "groupware mode". Start Outlook, and select the Options item from the Tools menu. The Options dialog box appears. Select the Mail Services Tab and click the Reconfigure Mail Support button to open the E-mail Service Options dialog box. Check that the Corporate or Workgroup option is selected.



From your Windows Start menu, go to Control Panel then select "Mail". Once there, select the "Show Profiles" button. The list of Mail profiles appears. If the CommuniGate Pro MAPI Installer has instructed you to re-create your existing Profile, select the old Profile and click the Remove button.

If you do not have an existing Profile, click the Add button to create a new Profile. Depending on the version of the Outlook and the Mail control panel installed, you will see several dialog boxes. If you see a dialog box with the Additional Server Types option, select that option. Select CommuniGate Pro Server as the "service" or "additional server type". Create a name for your new profile such as "TestMAPI".

You can add other services into the same Profile.

o) Configure the MAPI Connector

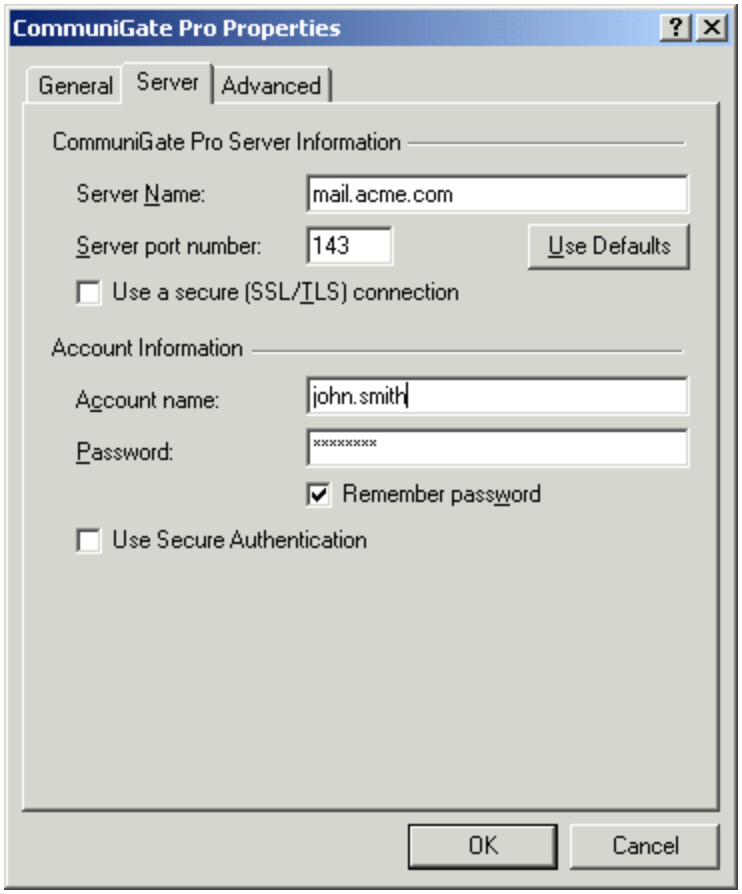
When the CommuniGate Pro service is added to a Mail Profile, the service settings can be configured. Later you can open the Mail control panel, open this Profile, and open the CommuniGate Pro Server settings. You can also use the Services item in the Outlook Tools menu to open the service settings.

The General panel allows you to specify the MAPI Account name and other general data. The Server panel allows you to specify the CommuniGate Pro Server and Account data:

Server Name

The name of your CommuniGate Pro Server. This should be a domain (DNS) name that has an A-record pointing to the network (IP) address of the server.

The MAPI Connector adds this name to the Account Name (see below) to send fully-qualified account names to the Server. This feature simplifies multi-domain support using a single IP address. Make sure that the specified name is either a name of some CommuniGate Pro Domain, or a name of some CommuniGate Pro Domain Alias, otherwise the Server will report the account has been moved to a remote system error.



Server Port

The network port the CommuniGate Pro Server uses for MAPI clients. This is the same port as the port used for IMAP clients.

Use a Secure (SSL/TLS) connection

This option is supported, the MAPI Connector establishes a network connection to the specified Server port, and uses the STARTTLS command to encrypt all data sent between the workstation and the Server. See the Security section for more details. It is usually a good idea to always select this option since it will allow secure communications.

Account Name

The name of the CommuniGate Pro Account to work with. This name can be a qualified name in the `accountName@domainName` form. If the simple name form is used (the name does not contain the @ symbol), the MAPI Connector adds the Server Name setting value to the specified account name.

Password

The password for the specified CommuniGate Pro Account.

Remember Password

If this option is not selected, the MAPI Connector will present a Login dialog box every time it needs to connect to the Server. If this option is selected, the supplied password is stored in the MAPI Connector settings data.

Use Secure Authentication

If this option is selected, the MAPI Connector sends passwords using secure (encoded) SASL CRAM-MD5 method. The secure method does not work if passwords are stored on the Server using a one-way encrypted method (see the Security section for more details). In this case this option should be disabled, and the MAPI Connector will send passwords in clear text.

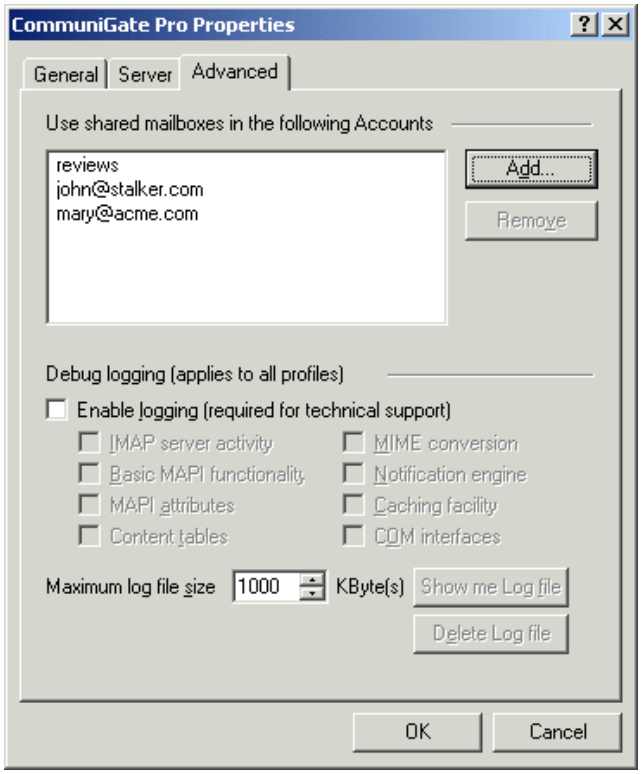
If you need to send passwords in clear text while connecting to the Server via public networks, enable the Use a Secure connection option, so all information is encrypted.

The Advanced panel allows you to specify other CommuniGate Pro Accounts you want to work with.

Use the Add and Remove buttons to specify the names of other CommuniGate Pro Accounts. If you want to access an Account in a different Domain, specify the full name: *accountName@domainName*.

The Account owners must grant you Mailbox Access Rights, otherwise you won't be able to see and open mailboxes in those Accounts.

NOTE: Outlook needs to have access to the Deleted Items mailbox in each foreign Account you try to open. Make sure that such a mailbox exists there and that the Account owner has granted you the Lookup, Read, Insert, and Delete rights for that mailbox.



Once you finish setting up your new profile, you are ready to begin exploring the extensive Outlook functionality enabled by the CommuniGate Pro MAPI connector. The following section explains how to set up various ways of sharing folder and calendar information. Begin by launching your Outlook client.

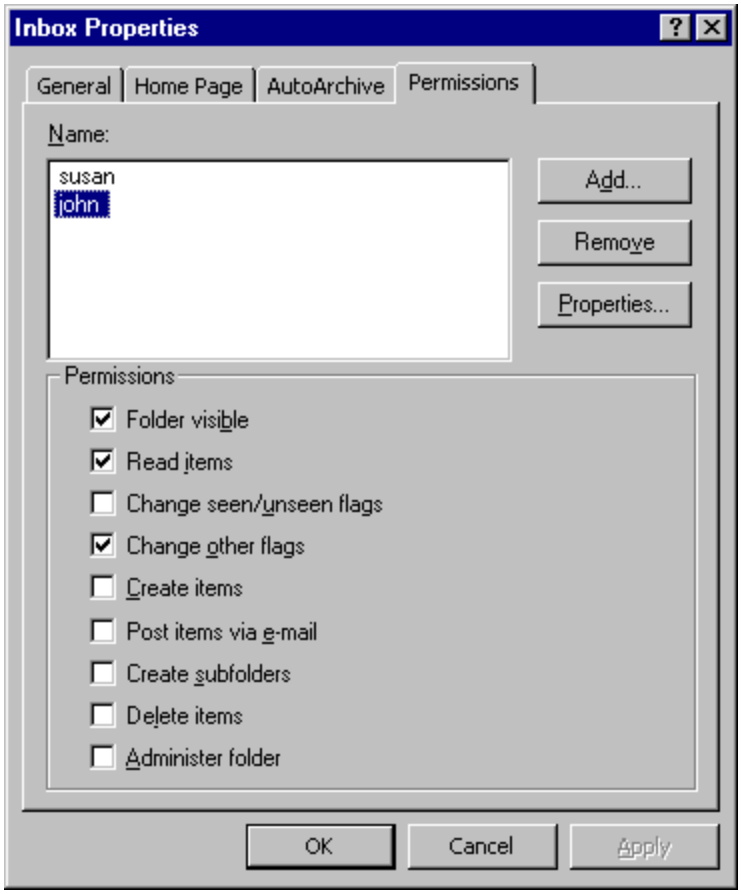
p) Enable Sharing of Folders

To share other users' mailboxes, tasks, contacts, etc., first ensure that you have specified the name of the account that owns the object you will be working with (see the Advanced panel section on the previous page.)

NOTE: Outlook needs to have access to the Deleted Items mailbox in each foreign Account you try to open. Make sure that such a mailbox exists there and that the Account owner has granted you the Lookup, Read, Insert, and Delete rights for that mailbox.

Then the account owner must set Access Control List for the shared folders to grant access to those folders to other CommuniGate Pro users.

To set access control for mailboxes, tasks, contacts, etc., select the object in the Outlook Folder List, and right click on it to open the Properties menu. From the Properties dialog box, open the Permissions panel:



Use the Add and remove buttons to specify the Accounts and other identifiers to specify those who should have access to this object.

Select an identifier in the list and use the checkboxes to grant required access rights to this identifier.

q) Calendar and Object Sharing

In this document, we have already covered the method used to share "Objects" (i.e., mailboxes, folders, calendars, tasks, notes, contacts) from Outlook to other users and visa versa. The sharing of objects in the system (calendar, addressbooks, etc...) is not

limited to this method. As all of these objects are basically "Mailboxes" - they can be shared and their access control can be managed by the users or administrators:

http://www.communigate.com/CommuniGatePro/Mailboxes.html

http://www.communigate.com/CommuniGatePro/MAPI.html#Sharing

There is another method available to configure access to a shared user's address book, calendar, or any object. It can be set from WebMail by the Administrator for all users in advance. This method is recommended for configuring group resources for all users. With regard to Outlook, users then see the objects they have access to on their next login. Here is how to do it:

- In this example the name of one account on the system is "public". The public account is sharing a Calendar with a user account named "john". John is a regular human user of the system.

- All of these settings are configured in WebMail and this can be done by the administrator for the users. We use here the "Basic" WebMail Interface "Skin" to describe the steps. Other WebMail skins have these features, but their interfaces may present them in different locations or with navigation methods. It is not necessary to deliver the ability to share and subscribe to these resources directly to the end user after the user is configured with the resources they need. You can customize skins or change account settings to hide the more complex or power user features.

  ### Step 1: Share The Object

  We first confirm that account public is sharing the Calendar in the public account to the account john. Start by logging into WebMail as the account name "public".

  #### i. Select the Calendar folder to be shared

  Optionally you can create a new Calendar object for public and give it any name you wish such as 'Travel-Schedule' as an example.

  #### ii. Folder Management

  Once you have selected or opened that object, either via the direct link or from the "Folders" page you will arrive at a view for this folder. Select the option that is "Folder Management". Some other skins call this option "View as Folder" and then "Folder Settings". We are attempting to navigate to the page where you can adjust the Access Control List (ACL) for this specific Address Book object.

Note: All Objects are IMAP Folders on the server side and the data contained in those folders tells the system how to display them. This is why sharing the Calendar is really sharing a folder to another user on the system.

iii. Access Control List (ACL)

Make sure ClientUser is listed as a client that can access this folder. Add their user name to the left hand side field and select the options you wish to grant permissions or access for:

Lookup	Post
Select	Create
Seen	Delete
Flags	Admin
Insert	

You can click help to find what privileges each of these options grant. These are the standard IMAP folder sharing ACLs.

iv. Permissions

Once the permissions are how you desire them to be, select update and log out of the public account.

Step 2: Subscribe to the Object (using the Folder Alias method)

v. Login to WebMail as "john"

Login to the WebMail of john and select Settings -> Folders

vi. Create a Folder Alias

You should create a folder Alias for the public Calendar by entering any alias name you prefer in the Alias Name like "Travel" and then enter the folder name as "~public/Travel-Schedule", in this example.

vii. Logout

Logout of WebMail for "john".

viii. Outlook

Open Outlook for "john" and the folder Alias should appear in Outlook after logging in – john should see the Calendar "Travel" available here – once clicked, it will provide the defined level of access to this Calendar – this could be "read/write" access, in the case of a "public" or Group Calendar. Outlook will need to download all of the information for that Calendar/folder on the first try – so please be patient - but after this initial access all following

accesses should be significantly faster, as they will only need to synchronize any additional changes to the Calendar.

This Folder Alias method works different from the shared folder method and may be easier to deploy for your environment because the configuration can be performed by the administrator for all users. However, it is also flexible enough for some users to configure.

Also worth noting in the case of CalendarData that you can view calendars you have permission to view with a link to the calendar data. Some calendar clients like SunBird on Windows or iCal on Apple use this method. If you try this with SunBird, the location of this (secure, by default) data is:

```
https://mail.example.com/CalendarData/~user/Calendar.ics
```

r) Set up Sharing of Free/Busy Information

The Free/Busy information is a file specifying when the person is busy, free, out of the office, etc. This information is usually made publicly available, so other users can access it when planning their meetings, scheduling appointments, etc. To compose the Free/Busy data, the groupware client application collects data from user Calendar(s), and merges it into one Free/Busy schedule.

s) Your Free/Busy Information

The MAPI Connector automatically stores your Free/Busy information in the Personal Web Site area. Publicly available information in the standard vCalendar format is stored as the freebusy.vfb file in the topmost directory of your Personal Web Site. The private-type information in the Microsoft Object data format is stored as the freebusy.eml file in the Personal Web Site private directory.

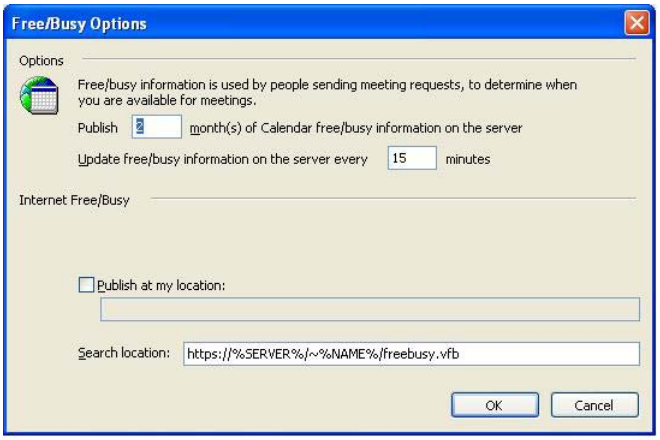
t) Accessing Free/Busy Information for Other Users

In order to process Appointments and Meetings, the Outlook application on the client machine should be able to access the Free/Busy information of other users. This operation is not implemented via the MAPI Connector and should be done by the Outlook application itself. To configure your Outlook application:

- Install the Microsoft Web Publishing Wizard (it can be downloaded from the www.microsoft.com Web site).
- Select Options from the Tools menu to open the Options dialog box.
- Click the Calendar Options button to open the Calendar Options dialog box.
- Click the Free/Busy Options button to open the Free/Busy Options dialog box.

- Enter the URL string into the "Search at this URL" field (please read all the notes below). Enter literally this exact string shown below– the entries "%SERVER%" and "~%NAME%/" are special variables in Microsoft Outlook.

```
https://%SERVER%/~%NAME%/freebusy.vfb
```



- Click the OK buttons to close all dialog boxes.

This option will be used by the Outlook application when it needs to retrieve the Free/Busy information for an e-mail user. The application substitutes the %SERVER% symbols with the domain part of the user e-mail, and the %NAME% symbols with the username part of the user e-mail, so for the e-mail address john@example.com the Outlook will use the http://mail.example.com/~john/freebusy.vfb URL to retrieve John's Free/Busy schedule.

Note: the suggested Search URL will work only if your CommuniGate Pro Server accepts WebUser Interface connections on the port 80 or 443. The CommuniGate Pro package is distributed only with ports 8100 and 9100 configured for WebMail HTTP and HTTPS ("WebUser Interface"). If it accepts them on the default port 8100, or on any other non-standard port, the Search URL must include that port:

```
https://%SERVER%:9100/~%NAME%/freebusy.vfb
```

Note: the suggested Search URL will work only if your CommuniGate Pro Domains have names that have "Domain Name System" [DNS] A-records pointing to the CommuniGate Pro server. Often, the DNS system does not contain any A-record for your example.com Domains, or those records point to a different system (company Web server), while the CommuniGate Pro Server addresses are specified as mail.example.com, or sip.example.com, or mx.example.com or similar DNS A-record(s).

Note: if your CommuniGate Pro server is serving only one Domain, then you can specify the Search URL as:

```
https://mail.example.com/~%NAME%/freebusy.vfb
```

where mail.example.com is the name of the CommuniGate Pro Domain or its alias, which has a DNS A-record pointing to the CommuniGate Pro Server.

In this case this Search URL will work correctly only for the users of the same CommuniGate Pro Server.

u) What You Can Do in Outlook

Once Outlook and the MAPI connector are configured on the desktop, here are some suggestions for reviewing the Outlook functionality:

- Compose, send and receive e-mail
- Schedule meetings, events and appointments
- Invite attendees, receive and respond to invitations
- Reschedule or make changes to appointments
- Set recurrences for appointments
- Share account free/busy and mailbox information
- Share folders, contacts and tasks
- Set up mailbox filters with the integrated wizard
- Search folders with integrated find utilities
- Work in off-line mode---synch when you re-connect

J. Working in the WebMail Interface

The exact same mailboxes, calendars, and sharing of both can be accessed through WebMail as with Outlook. Customizable skins in 14 languages are provided to match the look and feel of common messaging applications such as Outlook and Entourage.

1) E-mail

- Compose, send and receive e-mail
- Proofread work with integrated multi-language spell checker

2) Calendaring and Group Scheduling

- Schedule meetings, events and appointments
- Invite attendees, receive and respond to invitations
- Reschedule or make changes to appointments
- Share account free/busy and mailbox information

3) Address Book and Contact Management

- Access enterprise directories and personal address books

The new "address book" provides a "unified view" similar to Outlook's Address Books - i.e. it can retrieve data from our old "ACAP" address books, do the Directory/Directories, and to Contact-type folders (your own Contacts, as well as shared Contact folders in other accounts).

4) Collaboration

- Share folders, contacts and tasks

5) Self-Service and Call-Control Administration

- Define filtering rules and vacation messages
- Change (forgot) password
- Manage Call Control, access personal Call Logs
- Retrieve voicemail in e-mail

6) New Skins

With the release of CommuniGate Pro version 4.3, we have introduced the first three new WebMail Skins designed by CommuniGate Systems. These will provide the end-user with an "Outlook-like" experience, while maintaining all of the Groupware functionality to which they are accustomed.

K. WebMail

The WebMail Interface provided with CommuniGate Pro will always be the easiest to setup and use, because almost all users today are thoroughly comfortable with using a web browser and accessing their e-mail via a browser. CommuniGate Pro enhances this experience by bringing e-mail together with calendaring and shared folders into the WebMail environment.

WebMail users can access the WebMail Interface through many common browsers, with the most popular today being Internet Explorer™, Mozilla Firefox™, and Apple Safari™ browser, as well as the text-only web browser Lynx™.

The CommuniGate Pro WebMail Interface is accessed by default at either of the following URLs:

https://mail.example.com:9100

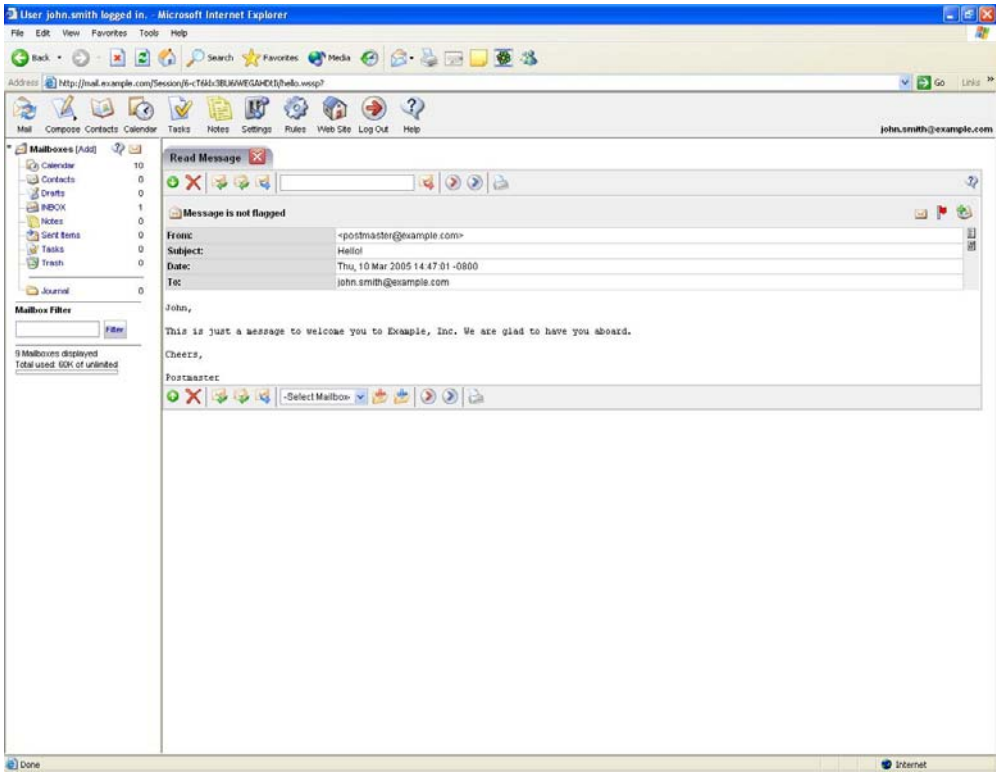
http://mail.example.com:8100

Most sites will install it on a server at the standard HTTP/HTTPS ports, like the following:

https://mail.example.com

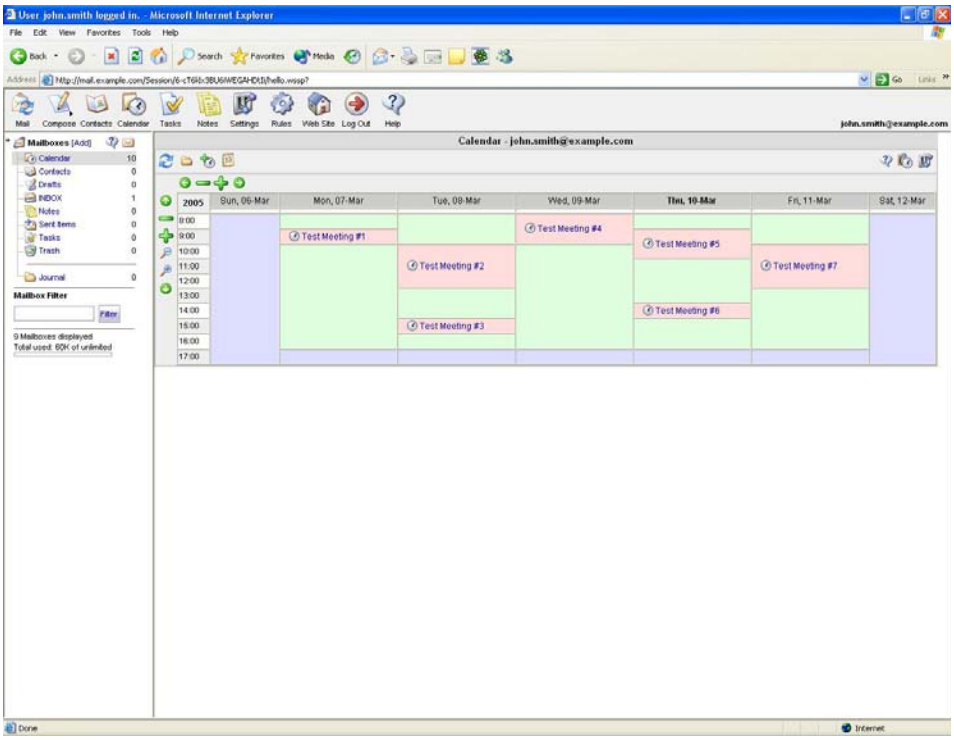
http://mail.example.com

The following page is a screenshot of a user's INBOX after logging into CommuniGate Pro using Microsoft's Internet Explorer:



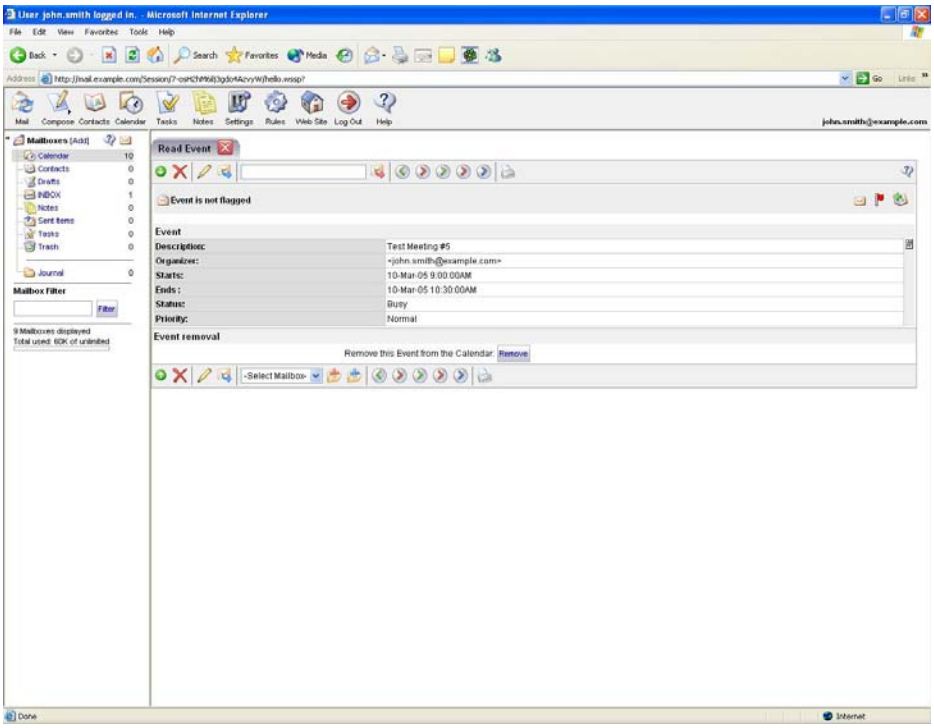
One of the many "WebMail Skins" included with CommuniGate Pro.

Once a user is logged in, they can also access their Calendar and Free/Busy information by clicking on the "Calendar" link in their Mailbox list:



Calendaring and Shared Calendaring through the CommuniGate Pro WebMail Interface.

Users can read and create new Calendar events, as well as invite other users to meetings:



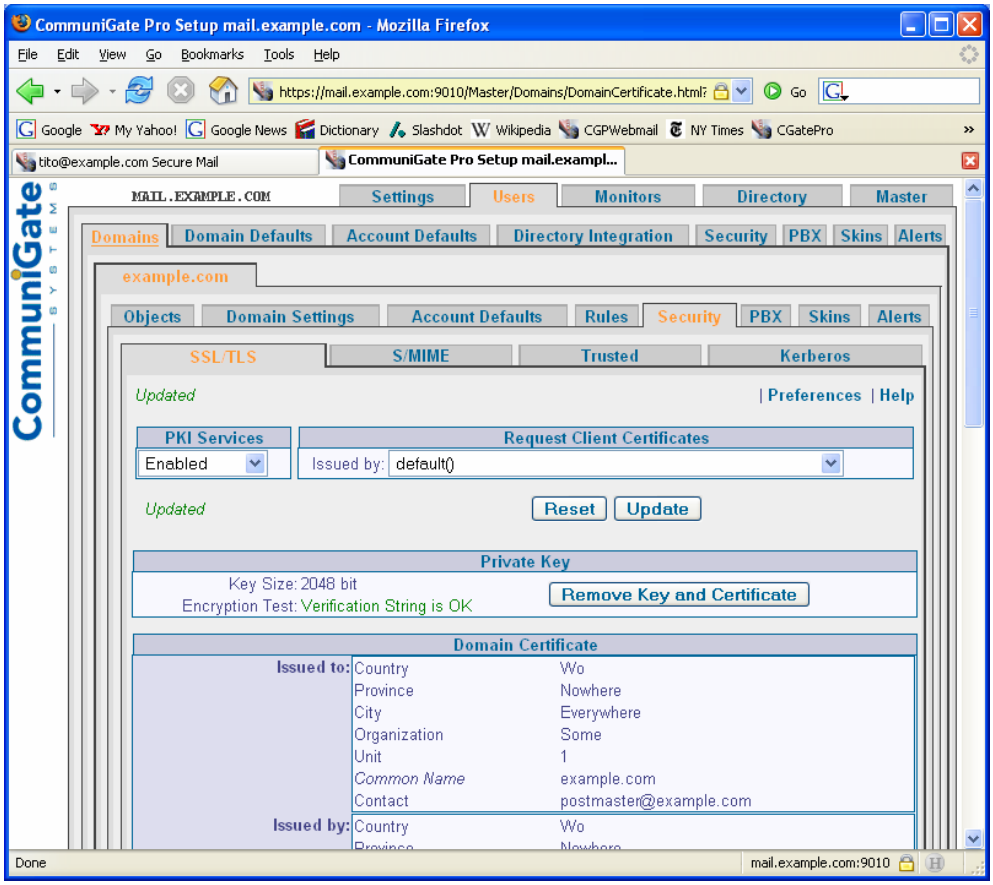
Creating or modifying Calendar events through the WebMail Interface – these Calendar invites generally interoperate easily with other collaboration systems such as Microsoft Exchange and Lotus Notes.

L. S/MIME

Brief Instructions on using S/MIME certificates with CommuniGate Pro.

1) Enable an SSL Certificate and an S/MIME Certificate

Please make sure you your System Administrator has first enabled a "certificate" for one or more domains on your CommuniGate Pro system [Users->(Select Domain)->Security]. For best results, use a "Signed Certificate" which has been signed by a "Certificate Authority" [CA] and which uses a Common Name: of all known server names for your domain (such as "example.com"). Or, you can have CommuniGate Pro create the certificates for you (using the "Generate Self-Signed" option). The domain must be "Enabled" for PKI Services to allow certificate creation.



Creating an SSL Certificate and S/MIME Certificate in the CommuniGate Pro WebAdmin Interface.

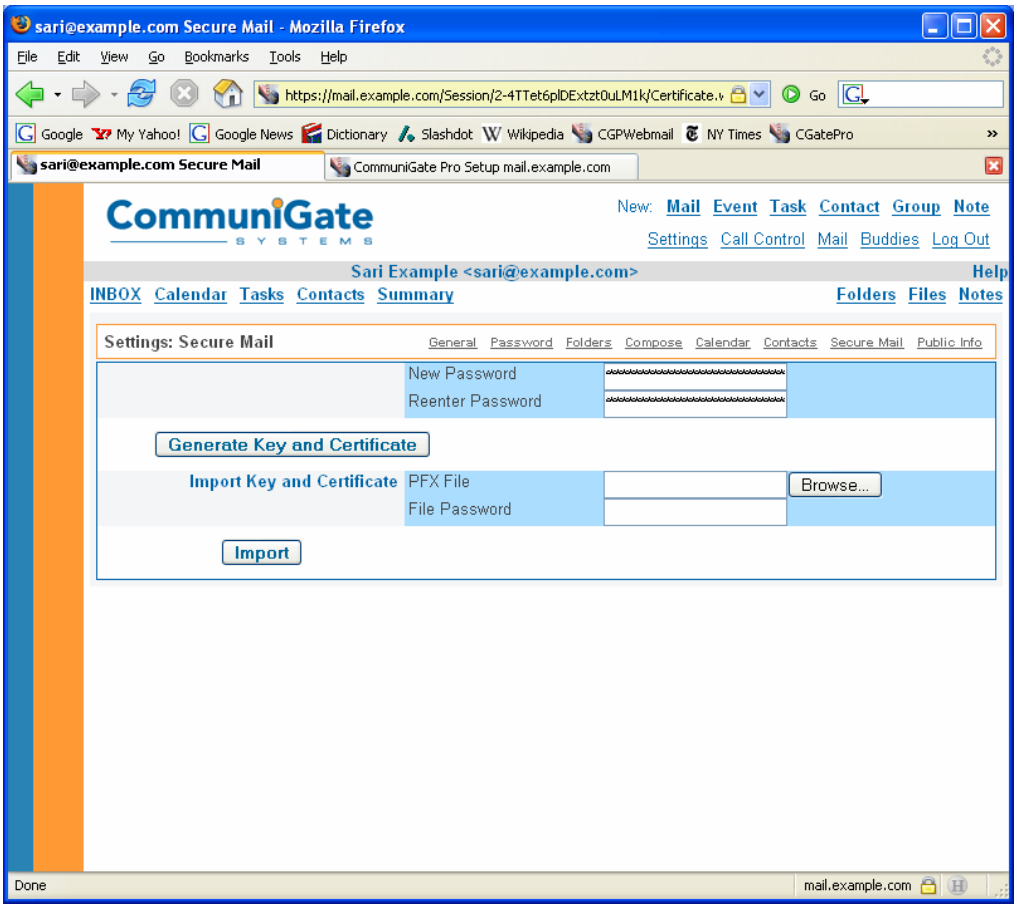
2) Create a New User S/MIME Certificate

This can be done by your System Administrator for you, or you can do it yourself. Here's how:

- Open up a web browser, and go to the WebMail login for your server. For example:

  https://mail.example.com

- Login. You may want to use the "Basic" (or ***) skin for this, as it occasionally has some features not available in other WebMail skins, though in this case many of the others should be fine too.
- Once logged into WebMail, select [Settings->"Secure Mail"]
- The first time you use this feature, you need to create a new "S/MIME certificate". Enter a secure password (it can be up to 256 characters long), such as a phrase or sentence that only you would know and which uses at least some digits and special characters such as ! $ % ^...whatever.
- Click "Generate Key and Certificate".



Creating the user's S/MIME Certificate in WebMail.

- Or, alternatively, Import your certificate from another source.
- Now that you have a personal S/MIME certificate created, you can use it in the WebMail Interface or Export it to other e-mail clients.

a) Using S/MIME in the WebMail/WebUser Interface:

- Please log in, go to "Secure Mail" in the [Settings->"Secure Mail"] location in WebMail.
- Once logged in, you now should see options to "Encrypt" any existing message in your INBOX or other mailboxes/folders.
- When composing a new message, you should also see an option to send messages "Encrypted" or "Signed". While we will not go into the details of PKI here, we can briefly document each:
  - Encrypted: a message for which the message body has been "scrambled" to make it unreadable without the secret password and/or key.
  - Signed: a message for which a "digital signature" (or cryptographic representation) which has been created using the message body in combination usually with a secret password and/or key.
- Signing messages has a particular benefit for sharing your "public key" or "public cert" with others. Once they have accepted this certificate for you, they are trusting that that public cert is a unique representation of your identity, and that it can be safely used to encrypt messages destined only for you.

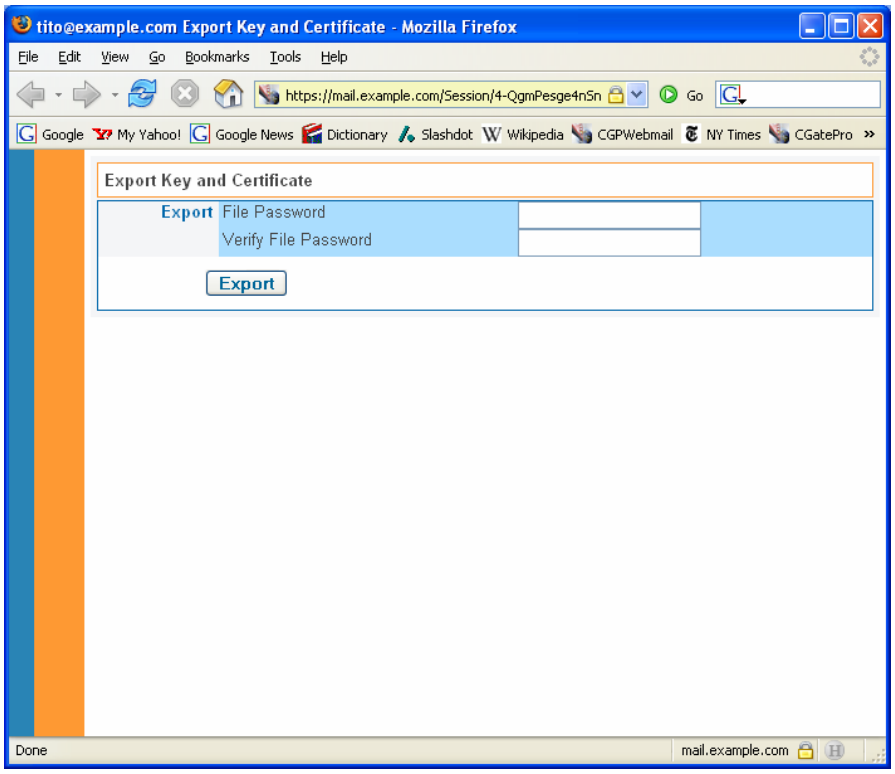
b) Export Key and Certificate

Many people prefer to use Message User Agents ("MUAs") or Clients such as Microsoft Outlook or Mozilla Thunderbird to send/receive e-mail. Your S/MIME certificate you just created can be Imported into these Clients (although we *must* say that this is likely to be far easier if your domain has a properly "Signed Certificate" signed by a registered Certificate Authority).

In the WebMail Interface, on the page:

Settings->Secure Mail

Once you've entered you're "Secure Mail Password" with the secret passphrase you created above, you should now see an option "Export Key and Certificate". Select it, and you'll see a page to Export your Key/Certificate to a file. Generally, you want to encrypt this Key/Certificate file itself, so it is recommended to at least use the same passphrase you used for your Key, and enter it twice here and hit the "Export" button.



Exporting the S/MIME Certificate created in the CommuniGate Pro WebMail Interface.

This should result in asking you to name the file to which you would like to save your Exported Certificate. Put this in as secure a location as you have.

c) [Possible Step] Import your Site Certificate into your Browser and Mail Reader

If you are not using a special "S/MIME Certificate" purchased from a Certificate Authority, you may need to Import your Domain/Site Certificate into your Client and assign a "Trust Level" which allows for the Trust of this Certificate as a valid e-mail identifier. Using Mozilla applications, you would do the following:

- Using a Browser, such as Mozilla Firefox, go to the main CommuniGate Pro WebMail Interface [WebUser Interface, HTTPU]:

For example:

https://mail.example.com

- Right-click on "Security Certificate", and select "Save Link As...". Save the Certificate.cer file to a known location.
- In your various Client applications, such as Mozilla Firefox and Thunderbird, go to:

Options->Privacy or Advanced->"View Certificates"->Web Sites

Then select "Import". Select the Certificate.cer file downloaded earlier.

You may also want to do this same process for the following tab, if your Signed Certificate is acting as an "Issuer" in generating new S/MIME certs through CommuniGate Pro.

Options->Privacy or Advanced->"View Certificates"->Authorities

Note: There are further details on this in the Official CommuniGate Pro Guide, here:

http://www.communigate.com/CommuniGatePro/PKI.html#SMIME

```
The CommuniGate Pro Server implements a Certificate
Server, issuing Certificates for its users.

A CommuniGate Domain can act as a Certificate
Authority for all its Accounts if:

* The Domain PKI Functions are Enabled.

* The Domain has a valid Private Key.

* The Domain has a valid generic Certificate or a
special S/MIME Certificate.

To specify Domain S/MIME settings, use the WebAdmin
Interface to open the Domain Settings pages. Open the
Security page and click the S/MIME link. If the Domain
has a valid Private Key, a page similar to those for
the generic Domain Certificate are displayed. These
fields can be used to enter a special S/MIME
certificate for the Domain. This Certificate is used
as the Issuer (Certificate Authority) for all S/MIME
Certificates requested by users in this Domain.

If the special S/MIME Certificate is not specified,
then the generic Domain Certificate is used as the
Issuer Certificate.
```

- Once Imported, you need to set the Trust level on this Certificate. Highlight the Certificate for your local domain, select "Edit", then select:

```
[X] Trust the authenticity of this Certificate.
```

- Also, select "Edit CA Trust", and be sure that this Certificate is completely Trusted, including:

```
[X] This certificate can identify web sites.
```

```
[X] This certificate can identify mail users.
[X] This certificate can identify software makers.
```

- Import Key/Certificate into another Application

i. Microsoft Outlook

Go to Tools->Options->Security->Import/Export...

```
[X] Import existing Digital ID from a file
 Import File:       [Browse]
 Password:
 Digital ID Name:
```

Fill out those fields correctly, and now you can Sign/Encrypt email from Microsoft Outlook. When you Compose new messages, the Security Settings option is on the "Options..." button under "Security Settings...". Inside here you can sign or encrypt outgoing messages. NOTE: remember, you must have someone else's "Public Key" in order to encrypt a message to them. You might be best off to attempt signing messages first, then moving on to encrypting.

ii. Mozilla Thunderbird

Go to Tools->Account Settings->(Select Account)->Security, then "Select" your Key for both Digital Signing and Encrypting.

When you send messages using Thunderbird, you will now use your "S/MIME" button (at the top of the Compose page with the little lock) for Signing or Encrypting messages. For Thunderbird, you may want to look at this page for Certificate issues:

http://kb.mozillazine.org/CA_certificate

M. Network Architecture and Ports

When installing CommuniGate Pro in your Organization's network environment, it is important to understand the ports required to access the many communications methods in CommuniGate Pro, as well as understand what ports are used "inter-cluster", when running a Dynamic Cluster or SIP Farm.

The following section details the usual ports configured for CommuniGate Pro.

1) Inbound Ports (Listeners/Services)

Firewall Note: Firewalls can be used which perform Port Restriction as well as Packet Inspection. However, if any packets are modified, this may cause Protocol Access to be affected or broken; therefore, disable any "Proxy" Services on the firewall, and if any packets are REJECTED, DISCARDED, or MODIFIED, then the CommuniGate Pro Administrator MUST be notified. If these packets are modified or discarded without notification, then very bad things may happen and

your access methods may not function properly. A "NAT method" of DMZ may be used with CommuniGate Pro; however, be sure that all "public ports" are properly mapped to "private ports" on the CommuniGate Pro Dynamic Cluster - also, please note that using "port re-mapping with NAT" will most likely NOT WORK at all, you must use standard and well-defined ports in order to provide standards-based Email and VoIP services. If using the NAT method of DMZ, then only IP re-mapping will work as expected, not port re-mapping.

Inbound Destination Port Number	Service [IP Protocol]
21	FTP [TCP]
25	SMTP [TCP]
53	DNS [UDP,TCP] (to DNS servers only)
69	TFTP [UDP] (may not be allowed for "Untrusted")
80	HTTP [TCP] (WebMail)
110	POP [TCP]
143	IMAP [TCP]
387	LDAP [TCP] (may not be allowed for "Untrusted")
443	HTTPS [TCP]
465	SMTP SSL [TCP] (Microsoft only)
587	SMTP MSP [TCP]
636	LDAPS [TCP]
674	ACAP [TCP] (may not be allowed for "Untrusted")
993	IMAPS [TCP]
995	POP3S [TCP]
5060	SIP [UDP,TCP]

5061	SIPS [TCP]
5222	XMPP [TCP] (Jabber)
5223	XMPP SSL [TCP] (Jabber old-style XMPP Encryption)
8010	WebAdmin Interface [TCP]
8021	FTP [TCP]
8100	WebUser Interface [TCP] (WebMail default)
9010	WebAdmin Interface Encrypted [TCP]
9100	WebUser Interface Encrypted [TCP] (WebMail default)
11024	XIMSS [TCP]
11025	XIMSS SSL [TCP]
60000-60099	RTP [UDP]

2) Outbound Ports

All "Source Ports" outbound should be allowed. Since MUAs (Mail User Agents) and SIP UAs (User Agents) can use a Source Port of any port, then outgoing packets should be allowed from the Cluster from any port to any port. All Outgoing Traffic should use a firewall method to "Keep State" on Outbound Packets, so that their Response Packets are safely allowed back in.

3) Inter-Cluster Ports

The CommuniGate Pro Dynamic Cluster communicates (by default) on these ports. **IMPORTANT NOTE:** Please keep the network as simple as possible between Cluster Nodes. This includes eliminating VIPs and firewalls ***between Cluster Nodes*** if at all possible, minimizing the chance of network failures - even short failures of less than 1 second can cause Cluster Nodes to separate from the Cluster if those TCP connections (on port 106) are broken.

Inter-Cluster Port Number	Service [IP Protocol]
21	FTP [TCP]

25	SMTP [TCP]
69	TFTP [UDP]
80	HTTP [TCP]
106	CGP CLI/API [TCP]
110	POP [TCP]
143	IMAP [TCP]
387	LDAP [TCP]
674	ACAP [TCP]
5060	SIP [UDP,TCP]
5222	XMPP [TCP]
8010	HTTP [TCP]
8021	FTP [TCP]
8100	HTTP [TCP]
9010	HTTPS [TCP]
9100	HTTPS [TCP]
11024	XIMSS [TCP]

N. Developing with XIMSS

The CommuniGate Pro Server implements the XML Interface to Messaging, Scheduling and Signaling (XIMSS) protocol. The XIMSS protocol is designed to give access to all modules within CommuniGate Pro (i.e., e-mail, calendaring, signaling, instant messaging, presence) via a standardized, published XML interface. Opening up all of CommuniGate Pro's communications methods to XML allows for the rapid development of rich XML applications and clients, by web application developers with XML development tools. In addition, XIMSS uses a server-driven event and access method allowing for hundreds to thousands of accounts to be handled efficiently through each TCP or TCP-SSL connection, providing huge scalability with a lightweight protocol. XML API clients should open clear-text or secure TCP connections to the CommuniGate Pro Server XML module. When a connection is established, both sides can send and receive messages. Each message is a text string

ending with a binary zero byte. Each message should be formatted as an XML document.

The XIMSS API is published here, and is open for third-party development:

http://www.communigate.com/CommuniGatePro/XMLAPI.html

For example, the following section demonstrates how XIMSS supports voice capabilities. Without knowing anything about the underlying (complex) protocols such as SIP and XMPP, a developer can easily create an application to drive it. In order to use the signalBind functions to have your program exchange the media, the application needs access to the audio resources on your client platform (often Windows or Mac).

Here is an example. CommuniGate Pro WebMail has a click to call feature where you can click a contact and the server calls your SIP address and then calls the contact. If you would like to create a very simple application that is an end user utility for 'Click-to- call' you can create one very fast that does not require the user to enter WebMail. You can choose to write the interface with flash, AJAX, j2me, widget or whichever development environment your project requires. You can test this example with netcat (nc), curl, telnet, or a perl tcp session manager script. You can telnet directly to the XIMSS port of 11024 or to the http port of your test CGP installation 8010 or 80 to test your XML messages. Please note that SSL and SASL options are also available, though these are not used in this example. If you test a direct connection, learn to type the null character, on a US keyboard it is control-@ or control-shift-2.

First your application must login. Have it take input for an example user "myuser@example.com" and password and send an XML message for login to the server:

```
<login id="x001" authData="myuser@example.com"
password="mypassword"/>
```

Your program sends the null character (ASCII 0) to complete that message and the server responds.

```
<session urlID="6-SESSIONYl02MWIhIwPsb"
userName="user@domain"/ >

<response id="x001" />
```

Once logged in your application can reuse the Session URL ID to offer many things to the user in the realm of Messaging, Signaling, and Scheduling. This simple example for Click-to-call has a single input, phone number or SIP address. The program we are creating changes the interface after successful login and presents an input field and a button control with the word 'Call'. If this is j2me on a mobile phone, I might have the application auto-login the user based on their phone SIM information and maybe only use a PIN number to confirm access making a kinder mobile phone user interface experience.

The user chooses to dial +52 (55) 5350 4672. The program we are creating reformats that number into a SIP URL for our server and connects the user to that number. First we call the user account from the server:

```
<callStart id="x001" callLeg="4444"
peer="user@domain;services=no">

<sdp ip="[IP_OF_CGP]" origUser="-" sessionID="7777777"
sessionVersion="9999" originIP="[IP_OF_CGP]">

<media media="audio" ip="[IP_OF_CGP]:16398"
protocol="RTP/AVP" direction="sendrecv">

<codec id="0" name="PCMU/8000" />

<codec id="4" name="G723/8000" />

<codec id="8" name="PCMA/8000" />

<codec id="101" name="telephone-event/8000" format="0-
15"/>

</media>

</sdp>

</callStart>

Program sends the null character and the server responds:

<response id="x001" />

<callConnected callLeg="4444">

<sdp ip="[IP_OF_CGP]" origIP="[IP_OF_SOFTPHONE]"
origUser="-" sessionID="10837624"
sessionVersion="10837666" subject="eyeBeam">

<media direction="sendrecv" ip="[IP_OF_SOFTPHONE]: 9242"
media="audio" protocol="RTP/AVP">

<codec id="0" name="PCMU/ 8000" /><codec id="8"
name="PCMA/8000" />

<codec format="0-15" id="101" name="telephone-
event/8000" />

</media>

</sdp>

</callConnected>
```

This calls your end user. Note that the end user accepts the call with the Eyebeam softphone. The Server response returns information you can have your program parse and act on if you wish. You can read about all of those XML message options in the XML API link above. Note that your user can have their CGP preferences set to forward their calls to a mobile phone. This is very handy if you are in a country where inbound mobile calls are not charged by the minute. Even if the call is billed per minute, it is very convenient for a mobile user to establish calls in this manner without worrying about having their softphone or IP phone registered. This callStart can go anywhere based on the user's preferences on the server.

I now have a connected the server's call to the end user. I wish to connect them to +52 (55) 5350 4672. I can use the callLeg I defined to do this with a call transfer.

```
<callTransfer id="x001" callLeg="4444"
peer="011525553504672@domain"/>
```

Send the null character.

Server says:

```
<response id="x001" />
<callDisconnected callLeg="4444"/>
```

A few things happened here. The program we are creating knows that my server expects international calls from the US to begin with 011, so the program replaces the international long distance symbol of '+' and replaces this with 011. You can accept the '+' on your server if you wish, this is simply a routing rule in CGP. The reformatted destination number is then sent to the server as a SIP address where CGP has a gateway configured to handle the call. The Gateway can be a physical box with SIP routing capabilities or an account on a service that supports SIP standards for routing calls. CGP connects the user with their destination number and disconnects the call leg that it had established directly with the end user. We can end our session if we want our program to do that now.

```
<bye id="x001" /> //send null
```

Note that in this same session I could have added a calendar item or a completed task to serve as an end user record of the call. I could have also sent instant messages from the server to the user via XMPP or SIP notifying the user of the call progress. After the program we are creating works, it can be refined to add pre-recorded audio prompts for the user and/or the destination. "Please hold while I connect your call" "Call Connected" "Sorry I could not connect your call press 1 to retry or 2 to hang up" ", etc...

Instead of just Click-to-call we could have created a Podcasting application supported by some CG/PL that calls the end user prompts them for their Podcast recording and records the audio. It is then possible to programmatically generate the XML for the RSS feed that the podcast requires and post that to the user's blog.

VI. PRICING

CommuniGate Pro Server pricing is available for single and multiple server configurations on the CommuniGate website:

http://www.communigate.com/CommuniGatePro/Licensing.html

A CommuniGate Pro Dynamic Cluster license starts at 500 users – licenses for greater numbers of users, as well as OEM licenses, for voicemail and other application uses are also available.

CommuniGate also provides Services for installation, configuration, customization, and migration, as well as Training and Technical Support.

About CommuniGate Systems

Since 1991, our company's mission is to create the most scalable, feature-rich solutions for Internet Communications based on open standards.

Headquartered in Mill Valley, California, CommuniGate Systems has over 10,000 customer sites worldwide, ranging from the largest broadband, wireless and wire line service providers to enterprises and universities. Over 125 million end users including 45 million voice customers rely upon CommuniGate Systems' products for their voice and data communication needs.

Today, CommuniGate Systems delivers applications based on the unique field-proven Dynamic Cluster technology for the mature e-mail messaging and collaboration market, as well as for the emerging VoIP market. CommuniGate Pro provides the only fully integrated and clustered carrier-class solution for email, VoIP, IP/hosted PBX, messaging and collaboration, and session border control. OEM partners worldwide. CommuniGate Systems maintains the highest customer satisfaction level in the industry and has won more awards than any other IP Communications platform. CommuniGate Systems provides performance, scalability, with the benchmark proven architecture that remains un-challenged in the industry. Our open development environment with simple APIs delivers extensibility with a unique clustering technology for 99.999% uptime for the most demanding application environments.

CommuniGate Systems has over 175 members in its partner network worldwide. Download your copy of CommuniGate Pro today and join the global initiative to help SIPify and convert nearly 2 billion e-mail accounts to a single identity for all forms of IP communications.

For more information about CommuniGate Systems and its products and services, please contact us at (800) 262-4722 or (415) 383-7164 by fax at (415) 383-7461; or E-mail at sales@communigate.com. Visit the CommuniGate website at the following URL: http:// www.communigate.com