

modusMail

Features (all versions)

Mail Server

The mail server component of modusMail allows your Windows 2000/2003 to receive, store and deliver Internet mail. The users of your system can then retrieve their individual email using the POP3 or IMAP4 messaging standards.

Domains, mailboxes and mailing lists can be created easily, and are further enhanced by powerful database integration. Its simplified user interface allows you to manage the integrated mail and web components from an easy-to-use administration console.

Mail receipt

- Understands Simple Mail Transfer Protocol (SMTP) and Extended SMTP (ESMTP).
- Incoming message size may be restricted.
- Uses efficient multithread worker-pool threading model for high-speed reception.
- Rewriting of From: addresses where appropriate.
- Optional reverse DNS lookup of host sending mail.
- Ability to block mail originating from certain hosts.

Local mail

- Supports the POP3 and IMAP4 protocols.
- Mailbox names can also be authenticated using RADIUS.
- Remote change password capability using Eudora protocol.
- Windows NT users can have their own mailboxes.
- Other named users may also have mailboxes.
- Mailbox names can be stored in a database.
- Per-mailbox quotas restrict the size of a mailbox.
- Per-mailbox expiration settings restrict how long mail is kept.
- Supports multiple mail domains - e.g. sales@abc.com and sales@xyz.com can be different users.
- Each virtual domain may have its own postmaster.
- Can automatically create user mailboxes.
- Hook for external processing of incoming messages
- Remote mailbox configuration

Out-of-office

- Leave a forwarding address.
- Auto-reply message capability.
- Single or multiple replies per sender.
- Message discard capability.

Mail routing

- Address alias feature allows mail re-routing.
- Uses the Domain Name System (DNS) for mail routing.
- Optional manual routing table.
- Configurable elapsed-time-based retry schedule.
- Configurable time-of-day-based retry schedule.
- Warning message if mail still undelivered after a specified time.
- Immediate mail delivery retries function.

Mail lists

- Support for regular and database mail lists.
- In Windows NT, NT groups can also be mail lists.
- Automatic subscribe and unsubscribe processing.
- Subscribe and unsubscribe can be independently moderated.
- Configurable messages prefixes and suffixes.
- Optionally store list membership in a text file.
- Optionally store list membership in a database.
- Four different levels of control for messages to the list.
- Moderation of messages through Web interface.
- Configurable options for handling error messages from bad addresses.
- Flexible message header processing.
- Hooks for external processing.
- Automatic Server wide or Domain wide lists are possible.

Configuration

- Configure machines remotely across a LAN.
- Immediate recognition of configuration changes.
- Service start/stop control.

Dialup Support

- Support for intermittently connected clients.
- Support for intermittent connectivity to the Internet.

Performance Monitors

- Interfaces to Performance Monitor.
- Five monitored entities.
- Total of 21 performance counters.

Logging

- Log to up to three separate file types: Text, Event Viewer and ODBC.
- 18 separate log sub-categories.
- Log files cycled daily.

Integration

- Integrates directly with the following membership/billing systems: Platypus, RODOPI, Emerald, EcoBuilder, Worldgroup.

Reliability

- Self-restarting services when running on Windows NT & 2000.

POP/IMAP Authentication

- Specify expiry of IP connection.
- Force extra validation of the email account.
- Cache successful POP/IMAP authentications.

Security

- Protocol filter
 - Filter messages at the protocol level.
 - Block messages based on the following header fields: from, helo, mailfrom, rcptto, received, subject, to, X-Advertisement.
 - Specify protocol filter from file.

- SMTP security
 - Enable full VRFY support.
 - Supports SMTP authentication.
 - Force SMTP authentication for suspect IP addresses.
 - Validate sender addresses and malformed addresses.
- Mail relaying
 - Limit mail relaying to trusted hosts or domains.
- Block scan attack
 - Limit the maximum number of recipients.
 - Slowdown or block IP addresses.
 - Cache connections by number of entries and lifetime.
- Reverse DNS lookup
 - Perform reverse DNS lookup for the SMTP host.
 - Cache DNS lookup results.
- Real-time blacklists
 - Lookup SMTP hosts in Real-Time Blacklist (RBL) hosts.
 - Administrator-specified RBL hosts.
 - Exclude trusted IP addresses from lookup.
 - Cache RBL lookup results.
- Connection limits
 - Limit connections for POP3 and IMAP4 protocols.
 - Limit connections by total number of connections to host.
 - Limit connections by simultaneous connections from single IP.
- Mail connections
 - Reject POP3 or IMAP4 connections from specified IP.
 - Reject all incoming mail from specified hosts or IP addresses.
- Whitelists
 - Administrator-specified list of IP addresses automatically bypass Block scan attack filter, reverse DNS lookup and RBL lookup.

Administration console

The ModusMail administration console is where all elements come together. The administration console was designed for flexibility and ease of use, and is organized in a coherent manner to assist with both day-to-day operations and in-depth system configuration.

Administration console – all versions

- “Find” feature allows system-wide user search.
- Properties regrouped for easy day-to-day administration.
- Intuitive delegation of parameters by system, domain or user.

Administration console – AS, AV & ASV versions

- Flexible quarantine interface for easy management.
- Integrated mail server, attachment, anti-spam and anti-virus administration tools, where applicable.
- Web-based administration – all versions
- Web-based administration tools.
- Interfaces directly with WebMail.
- End users can administer their own parameters, if wanted.

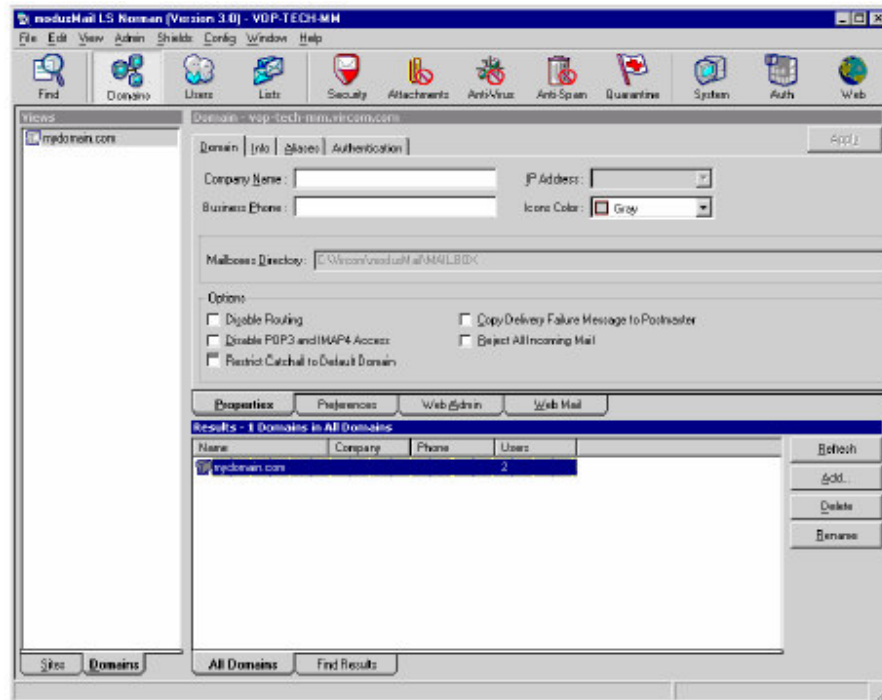


Figure 1: The administration console, modus ASV

Authority Delegation

Multi-level Preferences

For optimal flexibility, modusMail allows certain settings to be specified at three different levels: system-wide, per domain or per user. These settings are called **Preferences**, which can always be delegated.

There are three levels at which preferences can be set:

1. **Server-level:** affects all domains and users on the server. If you configure server-level settings and do not make any overrides, all users in all domains will inherit these preferences.
2. **Domain-level:** affects all users in a specified domain. When you configure domain-level settings, they override the server preferences, and will apply to all users in that domain.
3. **User-level:** affects only the user. When you set a user-level preference, it will override the domain and server settings.

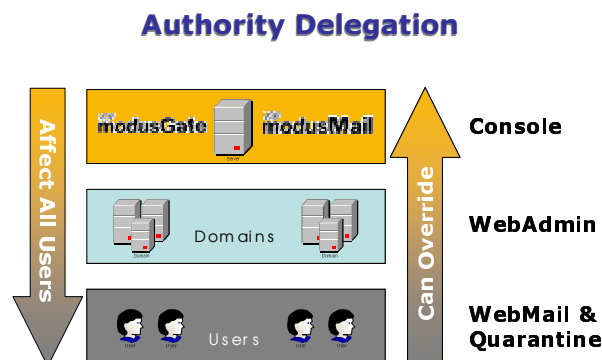


Figure 2: Delegation in modusMail

Multi-level Delegation

One powerful feature of modusMail 3.x is the ability to delegate all user-level and domain-level settings through a web administration console. All preferences can be delegated to either a domain administrator or to users.

There are three ways to do this within the administration console:

1. **System-wide settings:** You can delegate some preferences to all users on your system, regardless of their domain.
2. **Domain setting:** You can specify what preferences to delegate to all users within a specific domain.
3. **Users administrating domains:** Finally, you can grant administration privileges to certain users, allowing them to set specific preferences for all users within their domain, or for all domains in your system.

Multi-level Remote Settings

There are two different web-interfaces provided to change user/domain settings:

1. **WebAdmin:** Web interface given to domain administrators to manage their users and domains.
2. **WebMail:** Web interface that provides users with access to their POP/IMAP mailboxes from a web browser. WebMail has many advanced functions including folder support, spell checking, access to external POP accounts, as well as built-in access to mailbox preferences and settings.

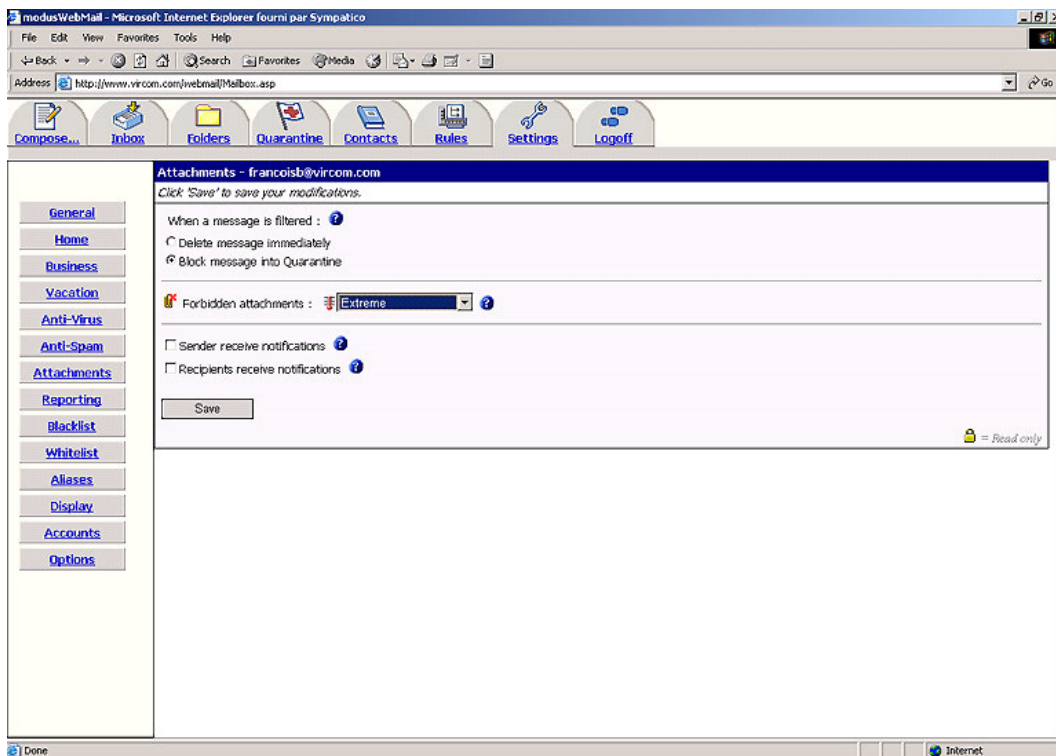


Figure 3: Attachment settings in WebMail

Anti-Spam & Sieve Filtering: AS & ASV versions

ModusMail AS and ASV versions include powerful and flexible anti-Spam tools that protect your system from abuse from unsolicited bulk email. These systems are 100% configurable to provide you the exact level of protection you need.

Attachment blocking (also available in the AV version)

- Explicitly block attachments by filename or extension.
- Use of wildcards in attachment blocking.
- Ability to send notification messages to both sender and recipient regarding potentially harmful content.

Whitelists

- Ensure that mail from specific domains and email addresses will always get through.
- Configurable at the server, domain and user levels.

Blacklists

- Block mail from specific domains and email addresses.
- Configurable at the server, domain and user levels.

Sequential Content Analyzer

- Performs advanced metrics analysis on message content.
- Determines whether message content is “good” or spam.
- Filters and processes messages according to your specifications, e.g. quarantine, delete or tag and deliver spam messages.
- Automatic updates of filter engine.

Sieve filters¹

- Enable Sieve filtering by system, domain or user.
- Create multiple complementary scripts.
- Cascade scripts for maximum flexibility.
- Sieve compiler verifies syntax of script.
- Color-coded script syntax for easy creation and modification.
- Supports regular expression (regex) and body purification extensions

Quarantine

- Quarantine interface integrated into administration console.
- Administrator-defined quotas for quarantine.
- Secure mail opening interface.
- Option to delete spam and messages containing forbidden attachments.
- Option to release messages to destination.
- Quarantine reports for end user management of contents.

Monitoring

- Top-10 domains/users that received/sent spams.

¹ In addition to these tools, ModusMail-AS and ASV offer you the full power of the Sieve filtering language, allowing you to build truly versatile custom spam filtering scripts. Sieve is a proposed standard for an Internet mail filtering scripting language. It can be used in a wide range of applications, and is particularly useful in defining spam filtering rules.

Sieve is defined under RFC 3028. For more information on Sieve, visit the following sites:

- <http://www.cyrusoft.com/sieve>
- <http://www.ietf.org/rfc/rfc3028.txt>

Anti-virus: ModusMail AV & ASV versions

Both ModusMail-AV & ASV include a powerful, built-in anti-virus engine. This engine is integrated to the core of the Internet mail server for optimal performance and reliability.

Anti-virus scan engine

- Award-winning 3rd-party anti-virus engine.
 - Catches all known viruses, as defined in Norman's or McAfee's virus definition files, including all known Bagle (.zip password-protected) viruses.
 - Includes Norman's anti-virus 'Sandbox' technology²
- Scan inbound and outbound messages.
- Scan messages when set as a relay.
- Specify anti-virus scanning by system, domain or user levels.

Auto-updates

- Download auto-updates directly from Vircom website.
- Download frequency is adjustable.
- Option to accept high-priority updates and bypass QA tests.
- Option to use HTTP-S to download updates.

Notifications

- Option to notify administrator-specified mailbox.
- Option to notify sender and recipient of detected virus.
- Administrator-specified alert messages.
- Plain text or HTML notifications.
- Specify alert from administrator-defined file.

Performance

- Cache last positive anti-virus identifications.
- Specify size and time limit of cache retention.
- Option to bypass large attachments.

Virus handling

- Option to delete the infected file or move to quarantine.
- New option to change the scanning order between Forbidden Attachments and Anti-Virus.

Quarantine

- Quarantine interface integrated into administration console.
- Administrator-defined quotas for quarantine.
- Secure mail opening interface.
- Option to delete infected files.
- Option to release virus to destination.
- Quarantine reports for end user management of contents.

Monitoring

- Top-10 domains/users that received/sent viruses.
- Top-10 viruses.

² For the SandBox technology, please refer to :
http://www.norman.com/News/Press_releases/11429/en
<http://www.norman.com/Virus/13927/en>