SmarterMail

Help Documentation

SmarterMail Help

Welcome to the SmarterMail Online Help System.

The tree menu on the left offers links to various pages that can help guide you through a better understanding of what SmarterMail is and how it works. This documentation is also broken down by role, and has pages that correspond to sections within the SmarterMail web client. Reviewing these pages will help you use SmarterMail more effectively, and each page is linked from within SmarterMail itself: either by clicking on any ? icons on modal windows, or using the "Online Help" link that appears when you click on your avatar. Whichever method you use, you'll be taken to the page in help that directly corresponds to the page you're on.

At the top of each help page, there are links that will allow you to do various things: visit the SmarterTools Community, browse the knowledge base, search through the help documentation, print the page you're on, translate the page you're on, or view the entire help as a PDF file.

If you need assistance beyond what's available in this documentation, feel free to contact customer service . We also offer paid support options , or you can visit the self-help options available from our portal : the knowledge base and the SmarterTools Community.

Common Help Topics for Users

- Logging in to my email account
- Sending messages
- Reading messages
- Marketplace for Users

Common Help Topics for Domain Administrators

- Adding new users
- Adding email aliases
- Add shared resources (shared calendars, conference rooms, etc.)
- Configuring spam filtering
- Marketplace for Domain Administrators

Common Help Topics for System Administrators

- Adding new domains
- DNS configuration for a mail server
- Locking down your server
- Sending your first email to test your setup
- Marketplace for System Administrators

Getting Started

Now that you have SmarterMail installed, it's time to get things set up. Below is a quick walkthrough that shows you how to add a new domain, how to add a new account to that domain, then how to send a test message between users. After that, there are some helpful links to additional help topics for things like adding new domains and users, configuring antispam, DNS configuration, and more.

Free Installation Available!

If you're not quite to the point of getting SmarterMail installed, that's okay: SmarterTools offers complimentary installation of any new license purchase! You should have seen that as an option when you placed your order but if not, just email us at sales@@smartertools.com and we can help get you scheduled. In addition, SmarterTools offers paid training to help get you on your way to expert mail server management.

A Quick Walkthrough

With SmarterMail installed, it's time to set up a domain and send your first email. Note: Until you have DNS set up, any mail sent from SmarterMail will be sent locally. (I.e., You can only email yourself — nothing is sent or received from outside the SmarterMail server.)

Adding Your First Domain

- Log in to SmarterMail using your system administrator username and password.
- Make sure you're on the Manage tab. (This tab generally opens by default.)
- In the left tree menu, select Domains .
- As we're adding a new domain, you'll want to use the New button in the content pane. the Domain modal opens:• Fill out the information on the Domain modal:

Domain   ?

Name *

|

Hostname *

mail.

Folder *

/var/lib/smartermail/Domains/

Primary Domain Administrator Username *

Primary Domain Administrator Password *

Confirm Password *

The new password must meet the following guidelines:

Contain one UPPERCASE letter
Contain one lowercase letter
Does not match your username
Contain any number 0 through 9
Is at least 8 characters long

Cancel   Save

• Name - This is the domain name, plus extension, you want to add to SmarterMail. For example, "example.com".

• Hostname - This will be set up automatically using "mail." as the domain prefix for your SmarterMail webmail login URL. Using "example.com", our hostname is "mail.example.com"

and the webmail login would become "http://mail.example.com". This can be edited as needed, but it's recommended that you leave this as the default.

• Folder - This, too, is set up automatically using the default path for the Domains folder. Again, this can be changed as needed, but it's recommended that you leave this as the default.

• Primary Domain Administrator Username - As a system administrator, you need to add a primary domain administrator for each domain you set up in SmarterMail. If you're also going to be a user of the domain, you can use your own account as the primary domain administrator and use SmarterMail just as everyone else does, you'll just have some additional Settings that others won't. (Name, you'll have access to Domain Reports and Domain Settings.) If this is one of many domains you're adding, you can use a generic username such as "domainadmin" or, for the sake of brevity, "dadmin".

• Primary Domain Administrator Password / Confirmation - This is, of course, the password to use for the username created above.

At the bottom of the modal you'll see the password requirements set up for the domain administrator passwords. Once you start filling out a password, these requirements will change from red to green, which lets you know you've achieved each requirement.

• Once you've completed this and met all requirements, be sure to Save the changes you've made in the modal.

Congratulations! You've added your first domain in SmarterMail. Your Domains page should now show something like this:
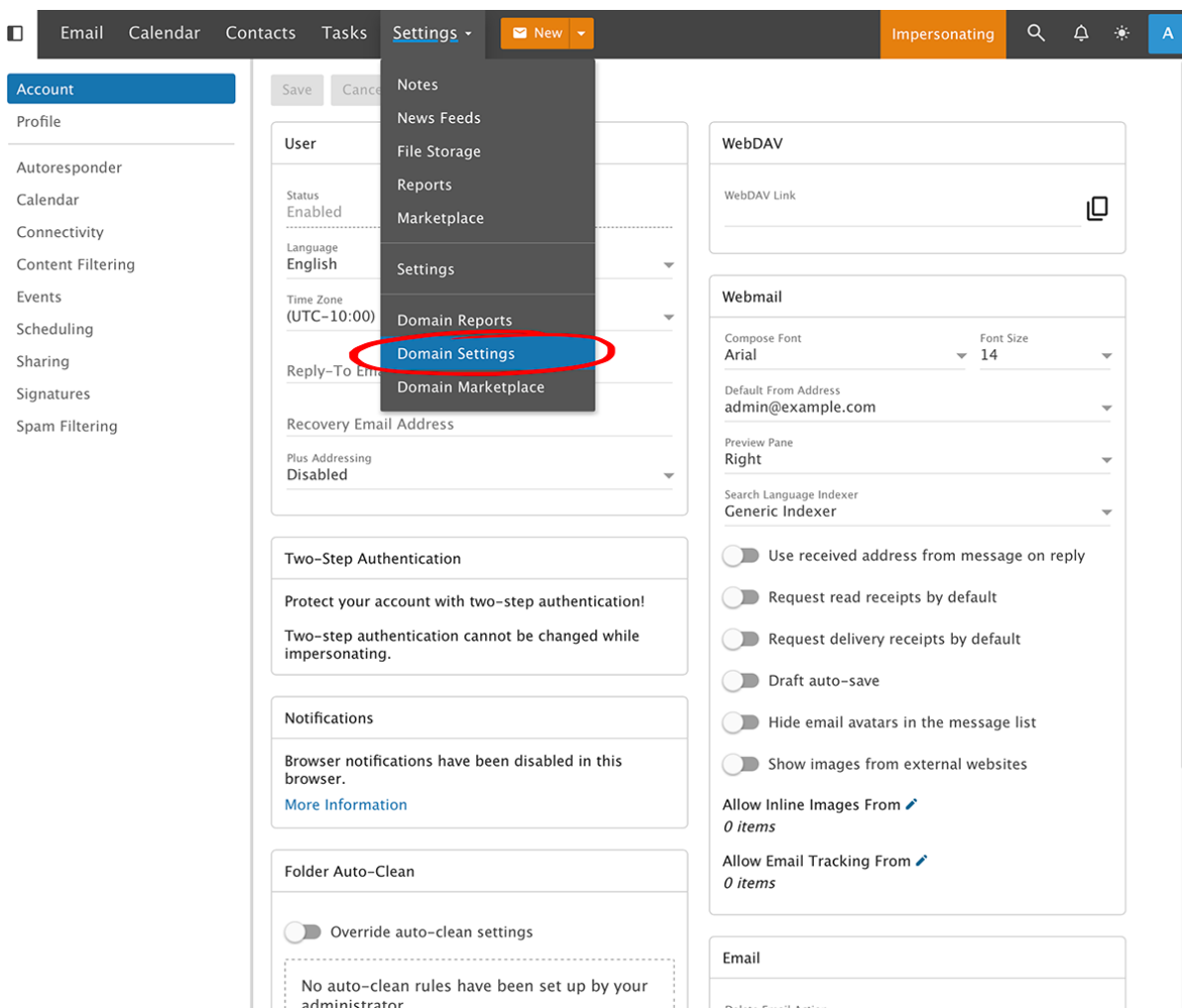

Logging In To Your First Domain

Now that you've added your domain, you can log into it as the domain administrator. As your DNS may or may not be set up yet, the easiest way to login as the domain administrator for the new domain is this:

• Staying on the Domains area, select the domain you just added to open its details.

• Using the Accounts tab, right-click the domain administrator account you just created and select Impersonate User from the menu. This will log you in as that user on the domain you just added to SmarterMail.• You will initially be logged in to that domain administrator's account settings. However, what we'll do next requires you to be in that domain's settings, not the domain administrator's settings. So:

• Use the Settings menu at the top of the page and select Domain Settings from the dropdown.• Once selected, the Accounts page will be opened, and you'll see the domain administrator account listed on the Accounts tab. From here, we'll add a new account, then send a test email.

Adding a New User to Your Domain

Since we're already on the Accounts tab in the domain's settings, adding a new account isn't much different than adding in the domain administrator account you set up. You just need to do the following:

> • Use the New button to open the New User modal.• As you can see, the information necessary is not much different than what was used to set up the initial domain administrator account. For now, you just need to add the following:

New User   ?

Username *

Password *

Confirm Password *

The new password must meet the following guidelines:

Contain one UPPERCASE letter
Contain one lowercase letter
Does not match your username
Contain any number 0 through 9
Is at least 8 characters long

☐   Force password change at next login

Cancel   Save

New User

?

Username *

John.smith

Password *

●●●●●●●●

Confirm Password *

●●●●●●●●

The new password must meet the following guidelines:

Contain one UPPERCASE letter
Contain one lowercase letter
Does not match your username
Contain any number 0 through 9
Is at least 8 characters long

☑ Force password change at next login

Cancel   **Save**

• Username - This is what forms the email address for the user you're adding. So, if "Dave Jansen" is the user you're adding, their username may be something like "djansen" or "Dan.Jansen".

• Password / Confirm Password - Yeah, this is pretty much what you think it is. The difference here, though is that there are some basic, default password requirements you'll need to follow. These are listed in red on the modal. System administrators can set default password requirements for all users on the server, then domain administrators can add on to those requirements if they so desire. Again, that's a bit advanced for right now, but you can read more on that once you get into SmarterMail a bit deeper.

• Force password change at next login - You can check this box if you want the user you're creating to change their password when they initially log in to the SmarterMail web client.

Once you're satisfied with the user information, be sure to Save your changes. When you do, you'll be taken to the new user's Account settings. Here, you can modify their account as needed, or you can let them edit their own settings when they initially log in to the SmarterMail web client. However, if you select Accounts from the tree menu, you'll see both accounts you've created listed on the Users tab.

Now, let's complete our final Getting Started task:

Sending a Test Email From One User to Another

Now that we have 2 new users set up — the domain administrator and another user — let's try sending a test message from one to the other. As mentioned earlier, since DNS may not be set up yet, sending this message will stay local to the domain, meaning it won't travel outside of the SmarterMail server. However, this will also get you familiar with the SmarterMail web client.

To send a test email, do the following:

• As you're already impersonating the domain administrator account you created, simply select Email from the top menu. This will take you to the Email section of SmarterMail.
• By default, you'll arrive at your Inbox . Chances are there's nothing in there, but there will be soon.
• To create a new message, use the orange New button. This will open SmarterMail's email compose window. This should look very familiar as it's just what the name implies: a way to compose a new message that can be sent to anyone you choose.
• Start typing the username of the new user you just created in the To: field. You should notice that SmarterMail already anticipates who the recipient of the message is using its autocomplete

functionality. You can select the suggested name or simply keep typing out the address.

• Next, fill out the Subject of the message, then start typing in the message area.• Once you're satisfied with your message, use the Send button to send it on its way.

• After the message is sent, you can impersonate the new account, just as you did when you impersonated the domain administrator account.

• Briefly, you go to the Accounts tab for the domain, right-click on the username of the account you want to impersonate, and select Impersonate User from the menu. This will open up that user's mailbox in a new tab.

• Hopefully you notice a few things:

• There's a red 1 on that user's Email menu. That denotes there's 1 unread message. (The one you just sent!)

• When selecting Email from the menu, you'll see that user's Inbox . It, too, will show a 1 to the right of its name in the tree menu.

• You'll see the message you sent in that user's Inbox. It should be selected by default and its contents show in the content pane.• That's it! You've successfully sent and received your first email.
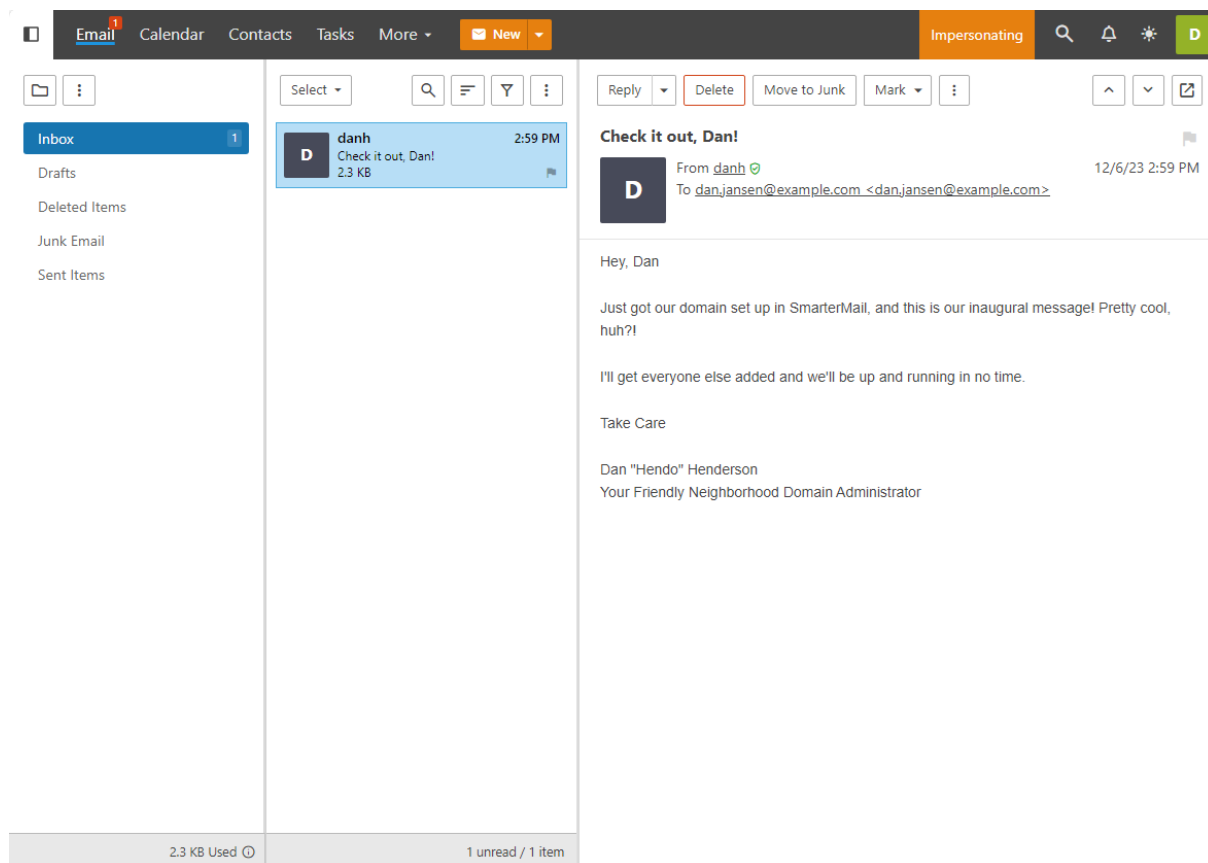
Of course, this is just the tip of the iceberg! There is much more you can do with SmarterMail, but this at least gets you started. Take a look at the additional help topics listed below and start your journey towards successful SmarterMail server administration.

Additional Helpful Links

Adding New Domains

As a system administrator, it's easy to add new domains, whether using custom configurations or default settings for every domain you add.

- Adding a New Domain
- Domain Configuration
- Domain Defaults

Adding New Users

As a domain administrator, adding users is quick and easy, whether using custom configurations or default settings for every user you add.

- Adding a New User
- User Configuration
- User Defaults

Configuring Antispam

SmarterMail offers a number of antispam options, free of charge, right out of the box. Setting them up helps protect your users and your server.

- Antispam Options
- Spam Checks
- RBLs and URIBLs

General Security Settings

After Antispam, configuring user password requirements, system events and some other important security features is a great next step to securing your server.

- Password Requirements
- System Events
- IDS Rules
- There are additional precautions you can take as well.

DNS Configuration for a Mail Server

Before a mail server is ready to be put in service, some DNS configuration is necessary for the domain(s) on the server so that mail can be sent and received.

- DNS Configuration for a Mail Server

Sending Your First Email

Once everything is set up, it's time to test things by sending your first email.

- Sending Your First Email

Ports

A mail server also requires specific ports to be opened to the outside world. Therefore, if you have a firewall sitting in front of your network, or your mail server, you'll want to open the following ports:

- 25 - Commonly used for SMTP traffic.
- 53 - DNS Resolution. Note: Port 53 is used for DNS only. If DNS is not run on the SmarterMail server, this port does not need to be open.
- 80 - Used to access SmarterMail's web client. Also used by EAS.
- 110 - Used for POP connections made to the server.
- 143 - Used for IMAP connections made to the server.
- 389 - Used for LDAP connections to the server.
- 443 - Used to access SmarterMail's web client over SSL. Also used by EAS.

• 465 - SSL/TLS SMTP Port.

• 587 - Submission Port - Commonly used as an alternative port number for SMTP traffic (supports SSL/TLS).

• 993 - SSL/TLS IMAP Port.

• 995 - SSL/TLS POP Port.

• 50099 - Used for XMPP (live chat) connections.

General Information

What is SmarterMail?

SmarterMail is an award-winning email, collaboration and group chat server that easily meets the needs of any sized business, from the individual proprietor to large corporations and enterprise organizations.

Features include:

- A rich, modern webmail interface optimized for desktops, tablets and smartphones.
- An integrated chat system that can be used right from the web interface or integrated with third-party chat clients.
- Integrated online meetings that include group chat, inline file sharing, and audio/video conferencing.
- Full collaboration features such as personal shared contacts, calendars, tasks and notes.
- Domain collaboration shares for things like calendars, notes, tasks, and contacts.
- Support for advanced features like delegation, contact groups, to-do lists, etc.
- Sender verification shield that shows the validity of a sender using various antispam checks (SPF, DKIM, etc.).
- Integrated file storage plus the ability to use OneDrive and Dropbox for file storage.
- Detailed reporting at the mailbox, domain and system levels.
- Email and chat archiving, ideal for compliance requirements.
- Integrated intrusion detection and DDoS protection.
- Advanced synchronization with third-party desktop and mobile email clients (Apple Mail, Windows Mail, eM Client, Android, iOS, etc.).
- The only server-side support for complete integration with Microsoft Outlook, providing features just like you get when using Outlook with Microsoft Exchange.
- Structured and multi-layered antispam and antivirus tools included at no additional charge.
- Optional add-ons such as EAS (Microsoft Exchange ActiveSync), MAPI/EWS, Cyren Premium Antispam, Message Sniffer, and other antivirus/antispam products.
- Incoming/outgoing gateway support.
- Failover functionality.
- Much, much, more!

With lower hardware requirements, superior stability and reduced maintenance costs, SmarterMail has significantly lower total cost of ownership and is the best-in-class Microsoft Exchange alternative for businesses and hosting companies.

SmarterMail Edition Explanation

Enterprise Edition

SmarterMail Enterprise has everything in the Professional Edition plus additional tools and features a business needs to bring an entire organization together. With the MAPI & EWS and EAS add-ons, SmarterMail Enterprise is truly a complete and affordable alternative to Microsoft Exchange. It's perfect for businesses looking for enterprise features, web hosting companies, ISPs and other service providers who want to offer a collaborative messaging platform.

Some additional features that set Enterprise apart from Professional include:

- Online Meetings
- Live chat
- Failover functionality
- Ability to mark a domain as hosted externally
- LDAP support
- Active directory authentication
- Email and chat archiving for SOX, HIPAA or other regulatory requirements
- The ability to purchase and integrate one, or both, of the following licensed add-ons:

- EAS for mobile (e.g., Outlook Mobile) synchronization
- MAPI & EWS for Microsoft Outlook 2016 and above on Windows (MAPI), plus Apple desktop client synchronization (Outlook for Mac, Apple Mail) and eM Client on Windows (EWS).

SmarterMail Professional

SmarterMail Professional is a complete and feature-rich mail server. It offers the essentials: email, calendaring, contact lists, tasks and notes and the ability to share and collaborate on all of these features. It's the ideal solution for a business or organization that focuses on using primarily webmail for their day-to-day operations and includes the ability to sync mobile and desktop clients using IMAP, POP, CalDAV and CardDAV. SmarterMail Professional is a great solution for a number of small businesses or for individual users.

SmarterMail Free

SmarterMail Free contains much of the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users. This is to give you an opportunity to try all the features out before making a decision on what product to purchase.

SmarterMail Edition Comparison

You can also refer to the following edition comparison chart for more information about each edition.

Features	1 Free	Pro	Enterprise
Migration and Converters			
Mail server converters for a wide variety of competitors	•	•	•
Mailbox migration for email, calendar, contacts and tasks	•	•	•
Automation using (Web Services/ REST)			
Compatible with wide variety of control panel companies	•	•	•
Add/edit domains and users	•	•	•
Add/edit calendars, tasks and notes	•	•	•
Add/edit RSS feeds	•	•	•
Retrieve user and domain statistics via Web services 2	•	•	•
Collaboration			
Scheduling (Replace services like Harmonizely)	•		•
Public Folders	•	•	•
CalDAV and CardDAV support	•		•
Outlook Scheduling Assistant support (requires MAPI & EWS add-on)	•		•
Microsoft Outlook 2007 and higher synchronization	•		•
eM Client synchronization	•		•
Apple Mail, Contacts, Calendar synchronization	•		•
Mozilla Thunderbird and Lightning synchronization	•		•
Webmail reminders system	•	•	•

Webmail availability of attendees	•	•	•
Webmail personal contacts	•	•	•
Webmail Global Address List (GAL)	•		•
Webmail personal calendars, tasks and notes	•	•	•
Shared calendars, contacts, tasks and notes	•	•	•
Delegation (Available in clients using supported protocols such as MAPI & EWS)	•	•	•
Chat and Online Meetings			
XMPP server	•		•
Chat (Audio, video, and text between individuals)	•		•
Online Meetings (Audio, video, and text for groups)	•		•
File upload support for Chat and Online Meetings	•	•	•
Search, view and print archived chats	•		•
Compatible with XMPP-supported chat clients	•		•
Mail Server Protocols			
MAPI & EWS support (Native support for desktop clients: Microsoft Outlook, eM Client)			Add-on
EAS support (Native support for mobile clients and apps)			Add-on
SMTP	•	•	•
IMAP 4 and IMAP IDLE	•	•	•
POP3	•	•	•
LDAP	•		•
Message retrieval via POP and IMAP	•	•	•
Antispam Measures			

Default and custom RBL support	•	•	•
Default and custom URIBL support	•	•	•
Message Sniffer available		Add-on	Add-on
Cyren Premium Antispam available (Includes Cyren IP Reputation Management)		Add-on	Add-on
Inbound and outbound spam checking	•	•	•
Spam quarantine (outgoing messages only)	•	•	•
Spam checking on POP3 message retrieval	•	•	•
Outgoing spammer detection and limiting	•	•	•
SpamAssassin-based Pattern Matching Engine	•	•	•
Support for distributed SpamAssassin servers (Linux or Windows)	•	•	•
Support for remote Rspamd servers	•	•	•
SPF record checking	•	•	•
DKIM Mail Signing	•	•	•
DMARC support	•	•	•
RBL listing detection	•	•	•
Reverse DNS checking	•	•	•
Greylisting (based on IP, sender location, spam weight, etc.)	•	•	•
Configurable spam weights for system, domain and users	•	•	•
Configurable spam headers	•	•	•
Trusted senders	•	•	•
Requiring SMTP authentication for outgoing messages	•	•	•

Support for Declude	•	•	•
Antivirus			
Cyren Zero-hour Antivirus		Add-on	Add-on
Out-of-the-box ClamAV	•	•	•
Support for third-party real-time antivirus solutions	•	•	•
Support for third-party command-line antivirus solutions	•	•	•
Support for a remote ClamAV server (Linux or Windows)	•	•	•
Virus quarantine (outgoing messages only)	•	•	•
Security/Attack Prevention			
Inbound and outbound TLS	•	•	•
Inbound and outbound SSL	•	•	•
SSL/TLS Automation	•	•	•
Server Name Identification (SNI)	•	•	•
Block Authentication by Country	•	•	•
IDS Blocks by Class C	•	•	•
Active Directory Authentication (ADX)	•		•
Two-Step Authentication (2FA - users and administrators)	•		•
Optional alternate SMTP port	•	•	•
SMTP authentication by domain	•	•	•
Restrict administrator access via IP	•	•	•
Brute force detection for Webmail	•	•	•
Manual and automatic IP whitelisting/blacklisting	•	•	•

Automatic harvest attack prevention	•	•	•
Automatic denial of service prevention	•	•	•
Malicious script filtering in webmail	•	•	•
Throttle user and domain activity	•	•	•
Throttle incoming bounces to prevent saturation	•	•	•
Reporting			
Real-time performance dashboards (traffic stats)	•	•	•
Basic reports (disk usage, file storage, etc.)	•	•	•
Advanced summary/trend reports (connections, traffic, spam, virus, etc.)	•	•	•
Data drill down for summary reports	•	•	•
Reporting statistics exposed as PerfMon counters	•		•
Export reports to CSV and tab formats	•	•	•
Events and Notifications			
Event-driven architecture	•	•	•
Notification profiles	•	•	•
Configurable system, domain and user events	•	•	•
Assign actions to events (e.g. command-line, notifications, etc.)	•	•	•
Default notification to all users when disk quotas are reached	•	•	•
Message Archiving			
Sarbanes-Oxley compliance 3	•		•
Enable message archiving by domain	•		•

Messages .ZIP compressed to reduce space necessary	•		•
Search, view and print archived messages	•		•
Messages stored in .EML format	•		•
Administration			
Mark a domain as hosted externally	•		•
Remote wipe of mobile devices (requires EAS add-on)			•
Support for auto-discovery	•	•	•
Performance counters (POP threads, POP connections, message sent/received, etc.)	•	•	•
Two-Step Authentication (2FA)	•	•	•
Failover functionality			•
Administration from a Web browser	•	•	•
Login Customization	•	•	•
Multiple system administrator accounts	•	•	•
Review and download log files from interface	•	•	•
Users can be limited to specific protocols (IMAP, POP, SMTP)	•	•	•
Mass propagation of settings for domains/users	•	•	•
Mass messaging to some or all users and domain administrators	•	•	•
Prioritize SMTP based on message type, domain or user	•		•
Spool functionality that allows third-party integration	•	•	•

Configurable outbound SMTP IP addresses	•	•	•
Multiple spools (smart spooling)	•	•	•
Manage all connections	•	•	•
Manage current blocks	•	•	•
Immediate blacklisting of connections and sessions	•	•	•
Configurable user password strength requirements	•	•	•
Configurable user settings by domain	•	•	•
Configurable logging for all protocols	•	•	•
Password compliance reporting and enforcement	•	•	•
Folder auto-clean to enforce user quotas	•	•	•
Domain-wide and system-wide footers	•	•	•
SmarterMail search indexing	•	•	•
Web Interface (Webmail)			
Multi-language compatible	•	•	•
Sender Verification Shield	•	•	•
Easily unsubscribe from mailing lists	•	•	•
Block email trackers	•	•	•
Optimized web-based performance	•	•	•
Compatible with mobile devices	•	•	•
Preview message attachments	•	•	•
New message notifications from anywhere in interface	•	•	•
Thumbnails for image file attachments	•	•	•

Download all attachments as .ZIP	•	•	•
Upload attachments in the background	•	•	•
File storage	•	•	•
Automatic save as draft	•	•	•
Click-to-map, click-to-call and click-to-mail functionality	•	•	•
Follow-up flagging	•	•	•
Linked emails and tasks	•	•	•
Advanced content filtering	•	•	•
Advanced spam filtering rules	•	•	•
User-level auto-clean	•	•	•
Support for multiple languages	•	•	•
Email address auto-complete similar to Microsoft Outlook	•	•	•
Import and export contacts	•	•	•
Support for user and domain aliases	•	•	•
Multiple signatures support	•	•	•
Multiple identity/SMTP support	•	•	•
Mailing Lists			
Bounce detection	•	•	•
Automatic removal of subscribers on bounces	•	•	•
Optional double opt-in	•	•	•
Subscriber custom fields	•	•	•
Friendly unsubscribe links in messages	•	•	•
Common subscriber database for all mailing lists	•	•	•

	•	•	•
Merge variables and custom fields into messages (mail merge)	•	•	•
Enable auto-generated response to mailing list commands	•	•	•
Enhanced mailing list compose with attachments	•	•	•
Customized command messages	•	•	•
Mail logging per subscriber	•	•	•
Message prioritization of mailing list	•	•	•
Throttling of mailing lists	•	•	•
Gateways			
Round robin or by domain	•	•	•
Use as SmartHost or inbound gateway	•	•	•
Use as backup MX server	•	•	•
Use as outbound gateway	•	•	•
User authentication and SSL/TLS support for outbound gateways	•	•	•
Gateway authentication with other SmarterMail servers	•	•	•
Gateway can have domain exceptions	•	•	•
Spam checking available on gateways	•	•	•
Greylisting available on gateways	•	•	•

1 SmarterMail Free contains much of the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users. This is to give you an opportunity to try all the features out before making a decision on what product to purchase.

2 For more information about using Web services with SmarterMail, see Automation with Web Services .

3 Consult your compliance professional to determine applicability to your organization.

For further assistance choosing the right edition, please contact the sales department by emailing sales@@smartertools.com . During business hours you can also start a live chat or call us at 1.877.357.6278.

How SmarterMail Works

Webmail Client

SmarterMail's webmail client is really the only thing system administrators, domain administrators, and standard users need! With support for any desktop or mobile browser:

> • Standard users have a versatile, yet lightweight, method of managing their accounts as well as sending/receiving email, managing their calendars and contacts, and more.
> • Domain administrators have access to their own mailbox as well as domain settings for things like adding users, propagating settings changes, adding domain shares, reviewing domain-level reports, and more.
> • System administrators can manage domains, set domain defaults and propagate those defaults, manage antispam and antivirus, set password requirements, administer IDS and other security protections, review domain and system-level reports, and more.

Regardless of what role you play, all of this is done through the same interface, using any browser from anywhere in the world - it simply adjusts based on the login used. That said, and as functional as the webmail client is, users can also opt to add their accounts to their favorite mobile and/or desktop email client. (Though domain and system administration is handled solely via the webmail client.)

Roles in SmarterMail

Generally, there are 3 major roles in SmarterMail:

> • System Administrators - System administrators are responsible for all aspects of running a safe, secure and high-performing mail server. That includes having solid antispam and antivirus solutions and rules in place, ensuring mail flows into and out of the spool, monitoring server memory and disk space usage, managing overall performance of the mail server and much, much more.
> • Domain Administrators - Domain administrators are responsible for managing the domain as a whole. That means creating users, watching users' disk space usage, managing spam and virus controls for users, managing mailing lists, reviewing domain and user reports, and much more.

• End Users - End users are the lifeblood of SmarterMail. They use webmail all day, make calendar appointments, sync their mailbox, calendar and contacts to a variety of mobile and desktop devices and clients, and so much more. Users keep domain and system administrators on their toes, and are sure to let someone know if something isn't working correctly.

These various roles are hierarchical as well. The system administrator manages the entire SmarterMail installation, overseeing all domains and users on the server, imposing limits and making judgements about which features domain administrators can control for their users. The domain administrator manages just the domain they're part of, and, therefore, defers to the judgement and settings propagated by the system administrator for their domain. Domain administrators may have the ability to manage some settings, but these options are granted to them by the system administrator. Finally, users abide by the rules and settings imposed by the domain administrator. Users may have some control over their own accounts, but this flexibility is dictated by the domain administrator. The diagram, below, shows the "Order of Operations" of the various Roles within SmarterMail and, really, almost any other email server:

System
Administrators

Domain
Administrators

End
Users
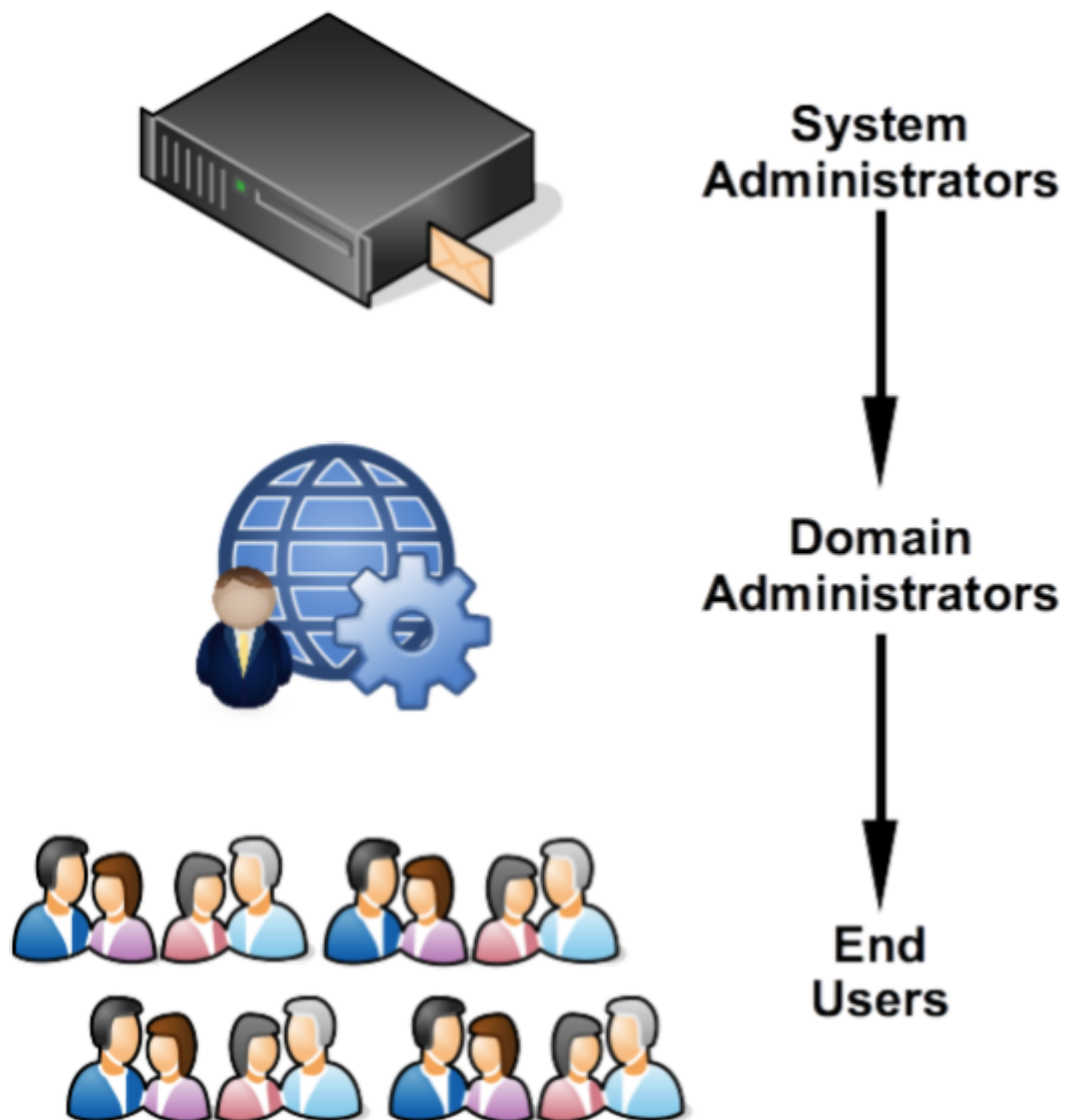
Installation and Deployment

Browser Requirements

Desktop

SmarterMail is fully supported by any modern and updated desktop browser. Minimum versions supported:

- Google Chrome
- FireFox
- Microsoft Edge
- Safari
- Opera
- Brave Note: Any browser you use with SmarterMail should also support WebRTC to ensure video conferencing works for you and any participants. In addition, using any versions of the above browsers that are over a year old may lead to poor performance of the webmail interface.

Mobile

In addition to working with most mobile email clients, not to mention third-party calendar and/or contact apps, SmarterMail offers the same robust webmail experience on mobile as it does on the desktop. As long as the mobile browser you use supports CSS, JavaScript and other modern scripting platforms, accessing the SmarterMail webmail interface is not a problem. This includes:

- Mobile Safari
- Chrome (iOS/Android)
- Firefox (iOS/Android)
- Brave (iOS/Android)
- Edge (iOS/Android)

Online Meetings

Just as with SmarterMail in general, online meeting functionality was built to accommodate any modern, up-to-date browser. The reason for this is due to the requirements for audio, video and screen sharing and the WebRTC protocols used on the back end. WebRTC makes real-time communication possible within applications and is used by virtually all of the most popular web-based conferencing solutions on the market. As such, any recent browser will support online meetings, and in many cases at least one or two previous versions of browsers are supported as well. That said, there are some limitations:

- Chrome and Firefox on iOS do not support WebRTC at this time. (Safari does.)

- WebRTC support was introduced in Safari 11. Previous versions are not supported.

- Legacy versions of Microsoft Edge may support WebRTC. The more recent releases of Edge (beginning with Edge 79) definitely support WebRTC.

SmarterMail System Requirements

SmarterMail was designed to operate efficiently with multiple applications on the same server. Below are the minimum system requirements solely for SmarterMail. If SmarterMail is running on a server with other applications, those need to be taken into consideration and may add to the requirements listed below. In addition, high-load / high-volume servers may need to adjust the requirements as needed:

Supported Operating Systems

- Windows Server 2016, 2019, 2022, 2025 or higher
- Linux

- Debian-based: Debian 11+, Ubuntu 20.04+
- Red Hat-based: RHEL 8+, Fedora 40+, CentOS Stream 9+, AlmaLinux 8.10+, Rocky Linux 8.10+
- Docker with Docker Compose

Minimum Hardware Requirements

- 4GB RAM
- 2-core CPU
- 1GB disk space for installation, not including mail data, file storage, etc.
- Dedicated IP address
- Dedicated domain name (subwebs and/or virtual directories are not supported)
- Active internet connection

Can SmarterMail Be Installed "In the Cloud"? (I.e., on Azure, Amazon AWS, etc.)

SmarterMail can be installed in the cloud or on your own dedicated hardware. When using a cloud service like Azure or Google Cloud, we recommend a full VM (e.g., Compute Engine on Google, which is extremely efficient when running SmarterMail for Linux) and not serverless installs (like Cloud Run or App Engine). This is because SmarterMail will use whatever hardware you give it for caching and performance, and services that dynamically scale automatically may cost you more money.

Services like Azure and Amazon's platforms, as well as other cloud providers, have some things to consider when determining how well any mail server will run. For example, some cloud services don't offer static IP addresses, instead rotating the IP addresses that are used. This can cause issues with items like DNS records, (MX records, A records, etc.) and affect mail delivery. As such, a static, public IP address is required for any mail server running in the cloud.

In addition, some providers lock down the ports necessary to run a mail server in order to prevent spamming. Check to ensure you can get permission to allow Port 25 as most don't allow it by defult. However, legitimate customers can bypass this restriction for their accounts, though it may take some time. Note: Each installation and environment is unique. Extra load caused by excessive messages or email accounts and/or other factors may require more disk space, memory, CPUs and/or CPU cores, database allocation, etc. SmarterTools recommends that system administrators slowly add domains to the server and watch how they impact the server. In addition, email patterns indicate that the number of email messages per account are increasing by approximately 60% every two years. It is important to keep this growth in mind when planning your rollout.

Installation and Upgrade

Installation and Upgrade

SmarterMail comes as a single installation file that contains everything necessary to run the product and get it set up on your server, regardless of the Edition that you intend to use. The features available are based on the license used during the activation process; if no license is entered, the Free Version will be installed. SmarterMail installers are available on the SmarterMail Downloads page of our website.

Jump to:

- Installing SmarterMail for the First Time
- Upgrading SmarterMail
- Things to Know
- Upgrade Process
- Upgrading Failover Servers
- Steps for Upgrading Legacy Versions

Installing SmarterMail for the First Time

Once you've downloaded the installation file from the SmarterTools website, it's time to actually install the product. SmarterMail starts by installing its mail service. This includes setting up all folders and directories needed to run SmarterMail. Therefore, it's just like any standard program installation:

• On the first page, you select the path for the installation and accept the license terms.

• Next, you'll input any licensing and activation information:

• Free Edition - Select this if you're going to test out SmarterMail. The Free Edition is essentially SmarterMail Enterprise (with some limitations) and works for a single domain and up to 10 email accounts.

• Enter a license key - If you have purchased SmarterMail, select this: you'll then be prompted to enter the license key so the product can be activated.

• Manual activation provided by support - In some systems, those locked behind strict network security policies for example, SmarterMail is used for internal purposes only. In these cases a "manual activation" of the product is necessary. These are provided by the SmarterTools support team.

• Once the activation information is provided, you'll see an overview of the SmarterMail version and mailbox allocation.

• Next, you provide some information about how SmarterMail appears in IIS: the Site Name, a Hostname, IP and Port (if these are needed — by default, SmarterMail binds to localhost on all IPs over port 9998). You can also change where SmarterMail installs by modifying the default File Path. Note: IF installing SmarterMail on new hardware with the intention of migrating domains and users from another SmarterMail server, it's best to ensure you're installing using the same File Path as your previous server to ensure migrated data and settings are preserved.

• Finally, you're given an overall summary of the installation. Clicking Install will install SmarterMail. Note: On Windows servers using IIS, the SmarterMail installation process modifies some IIS system settings for Application Request Routing (ARR). If you have anything else installed on the SmarterMail server that uses ARR, those will need to be reviewed to ensure they are still working properly.

• On new systems, that haven't had SmarterMail installed, the installation process takes care of any additional set up and configuration that's necessary: setting up SmarterMail in IIS with an application pool and website, setting the proper permissions on both, etc.

• After the installation completes, you'll be presented with the Welcome to SmarterMail screen. called Welcome to SmarterMail or Setup Wizard and then just link it from these pages. *@

Welcome to SmarterMail

After SmarterMail is installed, a window opens in your default browser that takes you to the web interface for your installation. The URL used will match what was configured during the setup process, and if nothing was changed (e.g., no changes to the hostname or port), your browser will open localhost:9998/interface/setup#/ .

On this Welcome page, you'll set up a few pieces of information to get started using SmarterMail:

• You'll create the primary system administrator account

• You'll set the default base path for storing all SmarterMail data. This includes domain data, spool, log files, and POP and IMAP retrieval data, etc. By default, this path is C:\SmarterMail\

Once you have set up this information, you will be redirected to the webmail interface and automatically logged in to SmarterMail using the system administrator you created. From there, you can add in your first domain , then add users to that domain , you can modify your default domain template , adjust the security settings as needed, and more.

Upgrading SmarterMail

Upgrading SmarterMail is a very simple process: you simply uninstall SmarterMail using Add Remove Programs, then run the installer you download from the SmarterTools website. Yep, it's really that simple. For those worried about uninstalling first, when you use Add Remove Programs, only SmarterMail's program files are removed: NONE of the data files are touched. So all of your users, domains, settings — all of it — is perfectly preserved and ready to use after you install the new version you want to run.

Things to Know

While the installation of SmarterMail is quick and easy, there are a few things to be aware of, especially if you're upgrading from a Legacy version of SmarterMail (SmarterMail 16.x or earlier) to a new Build:

• Due to significant back-end changes in recent versions of SmarterMail, it is not possible to roll back to a version earlier than Build 8495 (April 5, 2023).

• When performing an upgrade from a legacy version to the most recent current Build, all domains will go through a conversion process and all users will be re-indexed . The re-indexing of users is handled in batches, so it can take time to complete, especially if you have a lot of users on the server.

• This conversion process should go smoothly, and it can be tracked by going to https://your-smartermail-domain/interface/convert-status. You will need to log in with the system administrator account, but that page will list every domain on the server and its status as the conversion happens.

• If you run into errors at any point during the conversion process, please contact the SmarterTools Support Department. Be sure to provide a screenshot of the errors you're seeing in the SmarterMail interface as well as the conversion.log file from your SmarterMail Logs folder. (The default path is c:\SmarterMail\Logs .) Please send the full log file or copy and paste the snippet of text containing the domains showing an error.

• Legacy Versions of any product can be downloaded from your Account area. Simply log in to

your account, and from the Account dropdown icon, select "Legacy Versions". Here you'll have access to any current Build plus the most recent release of any Legacy product.

• The Release Notes for all major and minor versions of SmarterMail, as well as Release Notes for all current Builds, are available on the SmarterMail Release Notes page of our website. It's a great idea to familiarize yourself with all the changes that have been made to SmarterMail between the version you're on and the version you'll BE on once you've upgraded.

• To ensure that the upgrade maintains the integrity of your data, settings, users, file structure, etc. it's important to keep any default settings "as is" during the installation of the upgrade. Only change default settings if they were changed for the version you're upgrading from. File paths, etc. should match exactly. For reference, the default installation file path for SmarterMail is C:\Program Files (x86)\SmarterTools\SmarterMail .

• If you are upgrading an installation that utilizes a license key, you WILL need to re-activate that key once the upgrade completes. Please be aware that license keys pertain to the version of SmarterMail you're running as well as the maximum version of SmarterMail you CAN run — you cannot activate a key on a more recent version of SmarterMail if your key does not support that version. However, all license keys are retroactive for previous versions.

• Choose to use the same IIS site that was used previously. If IIS was not previously configured, create a new site. Note: An IIS site is required in order to access the SmarterMail web interface. An IIS site can be configured after installation; however, you will not be able to access the setup wizard or web interface in the meantime. If you choose to configure the site later, you can access the IIS Configuration Tool by navigating to its default location at C:\Program Files (x86)\SmarterTools\SmarterMail\IIS Tool.

• If you are running SmarterMail as an IIS site, IF NEEDED, change the .NET version of the Application Pool to .NET 4.0 and restart IIS.

Upgrade Process

To upgrade SmarterMail, do the following:

• First, back up your current SmarterMail installation or take a snapshot of your VM. This will give you something to fall back on should something happen during the upgrade.

• Stop the SmarterMail website and associated Application Pool in IIS.• Next, download the latest version of SmarterMail from our website .

• Uninstall the current version using Add or Remove Programs . This will only remove the SmarterMail program files — no data or system files are touched. This is an important step and should not be skipped, especially if you're upgrading from an older version. Newer versions may not require this step, but it doesn't hurt.• Run the installer.• Upgrading is essentially like installing for the first time. The difference is that most fields will simply carry over based on your existing installation. So you'll walk through the installation just as you did when first

installing the product but things like your paths, etc. will already be filled in. The upgrade process even finds the existing SmarterMail site in IIS! .NET 9 is required for installation.
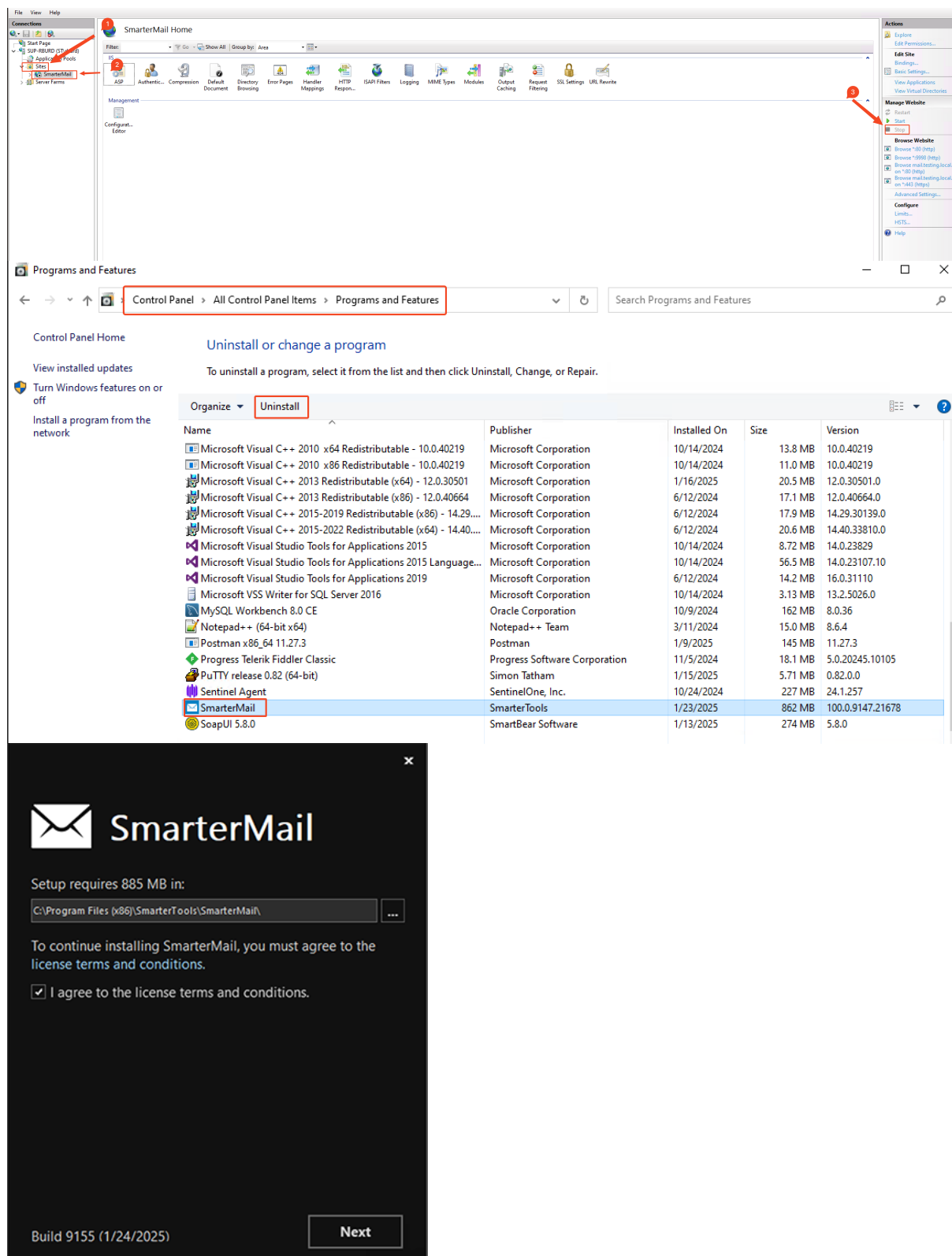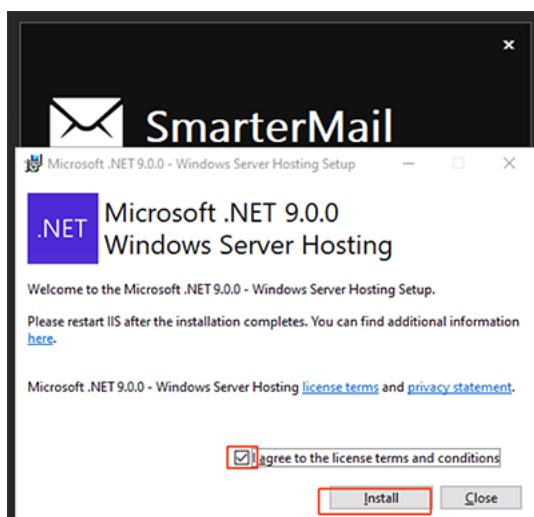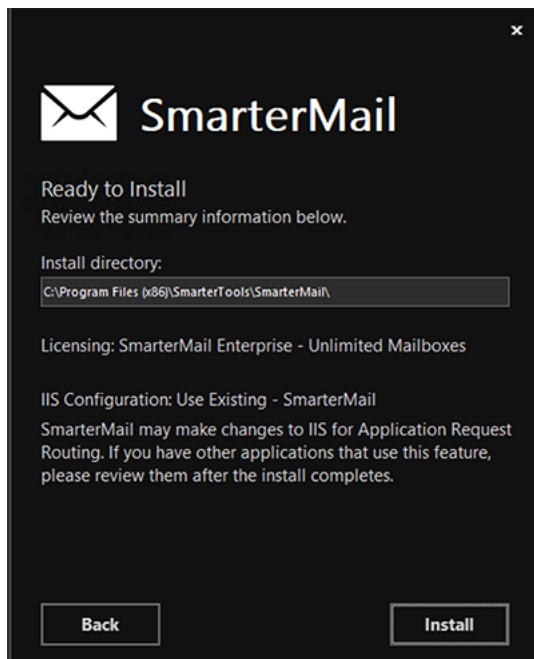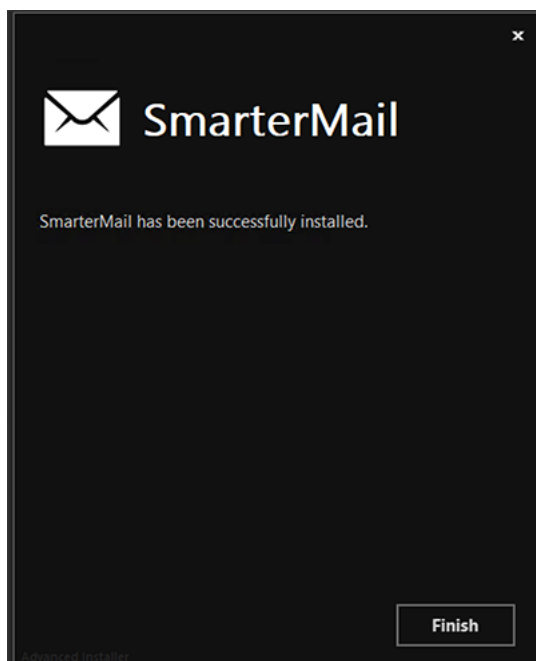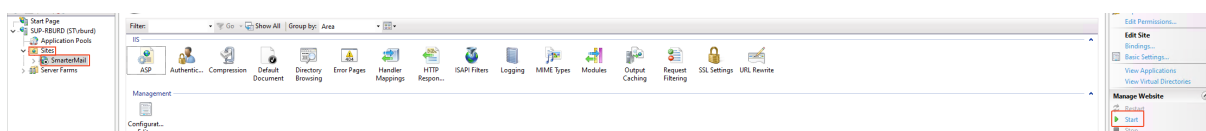
• Start the SmarterMail IIS Site - Verify everything is loading and working correctly.

• After the upgrade finishes, you're taken right to the SmarterMail login page where you can log in with your existing system administrator account.

Upgrading Failover Servers

For organizations running SmarterMail Enterprise in a failover configuration — that is, 2 SmarterMail front ends that share the domain, user and data via a network share or NAS — the upgrade process is a bit more complex. This is because the SmarterMail installer itself generally doesn't have access to the shared drive or NAS device. Therefore, it's not possible to make any modifications to the folders and/or data that is shared on those types of storage solutions. While an upgrade may not need to change any of those pieces, SmarterMail's upgrade process does still need access to them. Therefore, each server needs to be upgraded separately, with some files and folders moved temporarily during the upgrade.

Upgrading the Primary Server

For the purposes of this upgrade process, the "Primary Server" acts as the default SmarterMail server and manages the licensing of the server cluster whereas the other is considered the "Secondary Server" that remains connected to the cluster and is available as a "hot standby".

> • Stop the SmarterMail Service on both the Primary and Secondary servers. The rest of these actions should be performed on the Primary Server.

- Uninstall the old version of SmarterMail via Add/Remove Programs.
- Install the new version of SmarterMail.
- Stop the SmarterMail Service again. (It will restart after the installation).
- Right-click on the SmarterMail Service and go to the Log On tab. Make sure the account being used has the proper permissions/credentials for accessing the shared directory.
- Start the SmarterMail Service. The old "failoverConfig.xml" on the shared drive should be converted to failover.json, which is saved in the Service\Settings directory.
- Verify that the domains loaded properly.

Upgrading the Secondary Server

Upgrading the Secondary Servers is a bit easier as you don't need to move files between the two servers.

- Stop the SmarterMail Service on both the Primary and Secondary servers. The rest of these actions should be performed on the Secondary Server.
- Uninstall the old version of SmarterMail via Add/Remove Programs.
- Install the new version of SmarterMail.
- Stop the SmarterMail Service again. (It will restart after the installation).
- Right-click on the SmarterMail Service and go to the Log On tab. Make sure the account being used has the proper permissions/credentials for accessing the shared directory.
- Start the SmarterMail Service. The old failoverConfig.xml on the shared drive should be converted to failover.json, which is saved in the Service\Settings directory.
- Stop the SmarterMail Service one more time.
- Edit the failover.json file to match the failover.json on the Primary Mail Server.
- Start the mailservice on BOTH the Primary and Secondary Servers.
- Verify that the domains loaded on the Secondary Server match the Primary Server.

After both servers have been upgraded, it's best to perform some tests to ensure that the failover acts as expected and that any backups being performed are working.

Steps for Upgrading Legacy Versions

When upgrading a legacy version of SmarterMail, such as SmarterMail 16.x or earlier, it's very important to understand the current version and how much different it will be than the version you're upgrading from. SmarterMail has not only improved greatly from legacy versions, but it's gone through a few interface changes along the way. This is especially noticeable if you're upgrading from particularly older versions of SmarterMail to a current Build.

In addition, we've previously recommended that customers upgrade in steps when coming from SmarterMail 14.x or earlier. However, this is no longer the case: the latest installers accommodate for

all of the back end changes we've made since those versions, so it's no longer necessary to step up to SmarterMail 7.x, then SmarterMail 15.x, then on to the latest Build. In fact, it's NOT a good idea to upgrade in steps as you can carry forward any types of corruption or issues you may be having — even if you don't notice them. There can be back end file issues that you don't see, but that break an installation if you step through upgrades. Doing a standard upgrade to the latest Build should account for any of those issues and account for them in some way: either by fixing the issues or preventing those issues from corrupting any domains or users once the upgrade is complete.

That said, if you're at a point where you're upgrading from SmarterMail 15.x or earlier, we'd be happy to help you out: simply contact our Sales or Support Department and we can help test the upgrade for you, BEFORE you actually start through the process. Doing this will allow us to troubleshoot any issues you may encounter during the upgrade, and either fix them for you or help set your expectations of what you'll see once the upgrade completes.

Installation and Upgrade (Linux)

SmarterMail comes as a single installation file that will automatically download and install the appropriate operating system components required to run SmarterMail on your server. The features available are based on the license used during the activation process; if no license is entered, the Free Version will be installed.

Jump to:

- Installing SmarterMail on Linux
- Upgrading SmarterMail
- Uninstalling SmarterMail
- Manually Installing SmarterMail
- Things to Know
- Welcome to SmarterMail

Installing SmarterMail on Linux

Run the following in bash command to download and run the SmarterMail installer, which will download and install the current SmarterMail build. Replace the XXXX with the build number you wish to install (a full list of versions is available on the SmarterMail Release Notes page):

```
wget https://downloads.smartertools.com/smartermail/100.0.XXXX/smartermail_XXXX \
&& chmod +x smartermail_XXXX \
&& sudo ./smartermail_XXXX install Copy
```

This bash command will download and run the SmarterMail installer. This includes setting up all folders and directories needed to run SmarterMail. Therefore, it's just like any standard program installation.

Upgrading SmarterMail

To upgrade SmarterMail, first, backup your SmarterMail installation or take a snapshot of your VM.

Run the following in bash command to download and run the SmarterMail installer, which will download and upgrade the current SmarterMail build. Replacing the XXXX with the build number you wish to install. Yes, this is the same exact bash command that you use to install SmarterMail originally.

```
wget https://downloads.smartertools.com/smartermail/100.0.XXXX/smartermail_XXXX \
&& chmod +x smartermail_XXXX \
&& sudo ./smartermail_XXXX install Copy
```

Uninstalling SmarterMail

To uninstall SmarterMail, run the following in bash command, in the folder where you downloaded the SmarterMail installer. If you do not have the installer still, you can download it again using the wget and chmod commands in the installation section above.

```
sudo ./smartermail_XXXX uninstall Copy
```

Manually Installing SmarterMail

To manually install SmarterMail — generally when automating the installation process or installing via scripts — do the following:

• First, you want to download the installer:

```
wget --timeout=6000
https://downloads.smartertools.com/smartermail/100.0.XXXX/smartermail_XXXX
```

• Next, download the ZIP package, which contains all of the files necessary to install SmarterMail:

```
wget --timeout=6000
https://downloads.smartertools.com/smartermail/100.0.XXXX/smartermail_XXXX.zip
```

• Create a folder called "sm-install-data"

```
mkdir sm-install-data
```

• Then, you'll want to move and rename the ZIP file you downloaded to that new folder:

```
mv smartermail_XXXX.zip sm-install-data/sm.zip
```

• Now you can run the installer:

```
sudo ./smartermail_XXXX install
```

• The last step is cleaning up your downloads, otherwise the next upgrade may fail:

```
sudo rm -rf sm-install-data
rm -f smartermail_*
```

That should do it. SmarterMail is installed and ready for any future upgrade/update.

Things to Know

By default, files are stored in the following locations:

> • System Configuration Files - /etc/smartermail
> • SmarterMail Data Files - /var/lib/smartermail

Additionally:

> • The Release Notes for all major and minor versions of SmarterMail, as well as Release Notes
> for all current Builds, are available on the SmarterMail Release Notes page of our website. It's a
> great idea to familiarize yourself with all the changes that have been made to SmarterMail
> between the version you're on and the version you'll BE on once you've upgraded.
> • If you are upgrading an installation that utilizes a license key, you WILL need to re-activate
> that key once the upgrade completes. Please be aware that license keys pertain to the version of
> SmarterMail you're running as well as the maximum version of SmarterMail you CAN run —
> you cannot activate a key on a more recent version of SmarterMail if your key does not support
> that version. However, all license keys are retroactive for previous versions.

Welcome to SmarterMail

After SmarterMail is installed, a window opens in your default browser that takes you to the web
interface for your installation. The URL used will match what was configured during the setup
process, and if nothing was changed (e.g., no changes to the hostname or port), your browser will open
localhost:9998/interface/setup#/.

On this Welcome page, you'll set up a few pieces of information to get started using SmarterMail:

> • You'll create the primary system administrator account
> • You'll set the default base path for storing all SmarterMail data. This includes domain data,
> spool, log files, and POP and IMAP retrieval data, etc. By default, this path is
> /var/lib/smartermail

Once you have set up this information, you will be redirected to the webmail interface and automatically logged in to SmarterMail using the system administrator you created. From there, you can add in your first domain , then add users to that domain , you can modify your default domain template , adjust the security settings as needed, and more. function GenerateCodeBlocks() { let elements = document.getElementsByName("install_code"); elements.forEach(element => { element.innerHTML = GetInstallScript(); }); elements = document.getElementsByName("uninstall_code"); elements.forEach(element => { element.innerHTML = GetUninstallScript(); }); } function GetInstallScript() { let version = "XXXX"; let text = `wget https://downloads.smartertools.com/smartermail/100.0.${version}/smartermail_${version} \\ \n` + ` && chmod +x smartermail_${version} \\ \n` + ` && sudo ./smartermail_${version} install`; return text; } function GetUninstallScript() { let version = "XXXX"; let text = `sudo ./smartermail_${version} uninstall`; return text; } document.addEventListener('DOMContentLoaded', GenerateCodeBlocks);

Installation and Upgrade (Docker)

SmarterMail comes as a single docker file that contains everything necessary to run the product and get it set up on your server, regardless of the Edition that you intend to use. The features available are based on the license used during the activation process; if no license is entered, the Free Version will be installed.

This guide will help you get started with running SmarterMail using Docker Compose.

Prerequisites

- Docker installed on your system.
- Docker Compose installed.

Docker Compose File

First, create a docker-compose.yml using the information below. NOTE: you will want to replace or edit the following lines:

- <fill in web port> - Here you'll add or edit the port numbers you want to make available to SmarterMail.
- <Path on host> - These are the appropriate paths on your host system for storing data and system files.
- TZ - This should be updated to your desired server timezone. A full list of time zones can be found at Wikipedia's List of tz database time zones

```
version: '3.8' services: smartermail: image:
smartertools/smartermail:latest container_name: smartermail environment: -
TZ=America/Phoenix ports: - "<fill in web port>:80" - "<fill in web
port>:443" - "<fill in web port>:443/udp" - "25:25" - "110:110" - "143:143"
- "465:465" - "587:587" - "993:993" - "995:995" - "5222:5222" volumes: -
<Path on host>:/app/Data - <Path on host>:/app/SystemData restart: unless-
stopped
```

Firewall Configuration

Before starting the container, ensure the necessary firewall ports are open. If you have any custom ports configured, these should be added as well.

```
sudo ufw allow 80,443/tcp comment 'SmarterMail: Web-tcp' sudo ufw allow
443/udp comment 'SmarterMail: Web-udp' sudo ufw allow 25,465,587 comment
'SmarterMail: SMTP' sudo ufw allow 143,993 comment 'SmarterMail: IMAP' sudo
ufw allow 110,995 comment 'SmarterMail: POP3' sudo ufw allow 5222 comment
'SmarterMail: XMPP'
```

Starting SmarterMail

To start SmarterMail, use the following commands:

```
docker-compose up -d
```

You can access the webmail interface using the port(s) specified in your docker-compose.yml file. You'll use the webmail interface for configuring SmarterMail. (E.g., adding domains, configuring antispam, etc.)

Updating SmarterMail

In order to upgrade SmarterMail to the most recent release, use the following commands:

```
docker-compose down docker-compose pull docker-compose up -d docker image
prune -af
```

Useful Commands

Below is a list of commands that may be useful when managing your SmarterMail container.

- Get the container IP: docker inspect --format '{{ .NetworkSettings.IPAddress }}' smartermail
- View container logs: docker logs smartermail
- Access the container's shell: docker exec -it smartermail /bin/bash

Installing SmarterMail without Docker Compose

Below is an example command to run SmarterMail directly.

You will want to replace the following to match your particular installation, just as you would change them when creating your docker-compose.yml file:

- <fill in web port> - the port numbers you want to make available to SmarterMail.
- <Path on host> - The appropriate paths on your host system for storing data and system files.
- TZ - Your desired server timezone. A full list of time zones can be found at Wikipedia's List of tz database time zones

```
docker run -d --name smartermail -e TZ=America/Phoenix -p 80:80 -p 443:443
-p 443:443/udp -p 25:25 -p 110:110 -p 143:143 -p 465:465 -p 587:587 -p
993:993 -p 995:995 -p 5222:5222 -v /path/to/data:/app/Data -v
/path/to/systemdata:/app/SystemData smartertools/smartermail:latest
```

Licensing and Activation

During the installation process for SmarterMail, you're asked to input a license key, which defines the Edition and mailbox count that is activated once the installation completes. If you so desire, you can install SmarterMail as the Free Edition, which is good for use with 1 domain and up to 10 mailboxes.

To upgrade to a paid version and unlock additional mailboxes and/or gain access to use purchased SmarterMail Add-ons , a license key must be activated. Furthermore, if the SmarterMail installation is moved to another server or upgraded to a different version or product level, the product will need to be activated again. System administrators can use the Licensing section to activate SmarterMail or view current licensing information and limits. Note: Activation of a license key requires the server to contact SmarterTools over port 443 (HTTPS). Please ensure that any firewall or internet security software you have installed allows an outgoing TCP port 443 request. If the server cannot connect for security reasons or due to internet connectivity, please contact sales@@smartertools.com to request steps for a manual activation. A manual activation requires the server's hostname, which can be found by entering 'hostname' into the server's command prompt.

When accessing Licensing , the current licensing details for SmarterMail and its add-ons will be displayed, including the license key, license level information, status of the license or subscriptions, the number of items used out of the total limit, and an indication of whether an add-on trial is available. A license's current Maintenance and Support status is listed as well as it's expiration date. (This includes the status of any add-ons as well as SmarterTools' licenses.)

The following actions can be taken:

- Activate - Select this option to activate a new SmarterMail license key. Activating a paid license requires authentication by verifying the SmarterTools account login credentials. Trial license keys do not require authentication to be activated.

- Reactivate - Select this option to refresh the limits of the SmarterMail installation. This will cause SmarterMail to call back to the SmarterTools servers to refresh the limits of the license key and should be used after purchasing an add-on, upgrading to the Enterprise edition or increasing the mailbox limit. Reactivating is immediate and does not require authentication with the SmarterTools account credentials.

- Purchase - Select this option to be taken to the SmarterTools website where you can purchase a new license key or add-on.

- Start Trial - If an add-on trial is available, a Start Trial button will appear on its card. This allows the system administrator to test the functionality for up to 30 days. A trial can only be activated one time. To continue using the service after the trial, the add-on must be purchased. In addition, trials are not available on Free Editions of SmarterMail. Note: The ActiveSync trial

is limited to 25 Mailboxes. Note: If you are running a trial version of SmarterMail, it will automatically revert to SmarterMail Free when the trial expires.

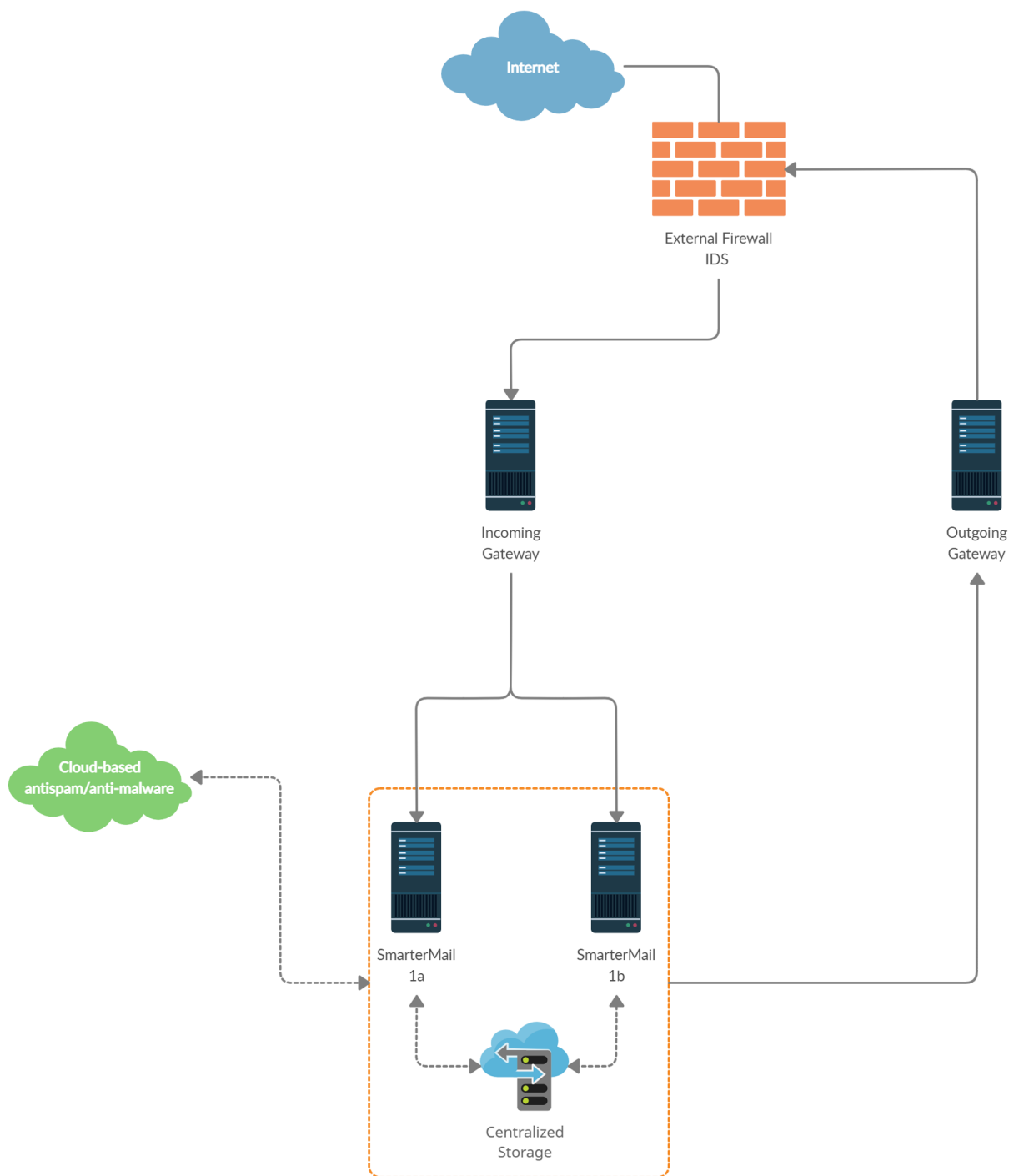# Configuring SmarterMail for Failover (Windows Only)

This feature is only available in SmarterMail Enterprise for Windows.

Who Should Use This

This document is intended for use by administrators deploying SmarterMail in high-volume environments and/or for organizations that want to ensure maximum uptime. It provides minimal system requirements and considerations for deploying SmarterMail in a failover environment. Note: Failover requires activation of SmarterMail Enterprise. For licensing information for this product, contact the SmarterTools Sales Department .

Failover Overview

SmarterMail Enterprise allows organizations to decrease the likelihood of service interruptions and virtually eliminate downtime by installing SmarterMail on a standby server that is available should the primary mail server suffer a service interruption. For businesses that use their mail server as a mission-critical part of their operations, failover functionality ensures that the business continues to communicate and that productivity remains at the highest levels possible, even if there is a primary server failure.

Understanding How Failover Works

The main components of failover functionality are; a primary server that acts as the default SmarterMail server and manages the licensing of the server cluster, and a secondary server that remains connected and available in a "hot standby" mode until the primary server experiences problems with network access or system hardware. It's considered a "hot standby" because the server is "hot", in that it's powered on, but the SmarterMail service (and possibly the web server) are inactive/disabled.

If the primary server fails, SmarterMail can be configured to automatically enable services on the secondary server. When this occurs, the secondary server then takes over responsibility for processing background threads and supporting all email functionality. This server will remain in active status until another failure occurs or the primary mail server comes back online.

The initial set up of SmarterMail's failover functionality entails system administrators manually disabling both the node and SmarterMail service on the primary server and then starting the node and SmarterMail service on the standby. However, system administrators can easily use third-party monitoring systems and script an automated failover and recovery strategy as needed. An example of this is provided at the end of this document.

Minimal System Requirements

• A minimum of two servers running Microsoft Windows Server 2019 64-bit. (Windows Server Core is not currently supported).

• Three IP addresses

• Both servers must have their server times synchronized

• A domain account or local system User or Group account with bidirectional authentication. Note: SmarterMail can NOT be run using Local System, Local Service or Network Service in a failover configuration.

• NFS/SMB share for mail and system files. We recommend that the share is running on a NAS/SAN that is configured as RAID 10

Adding Network Load Balancing to Your Servers Note: This needs to be performed on each server that will be used in the failover environment.

• Open the server manager console

• Right click on Features in the tree view and select Add Features

• Check the box next to Network Load Balancing and select Next

• Click Install

• Once the installation finishes, click Close

Configuring the Load Balanced Cluster for Use with Failover

• Navigate to Start → Administrative Tools → Network Load Balancing Manager

• Click the Cluster menu item and select New

• In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New

• When the Interface Name and Interface IP appear, select the Interface Name and click Next

• Since this is the primary node, ensure the host Priority is set to 1

• In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are

correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines. Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.

• Click Next

• In the New Cluster: Cluster IP Addresses window, click Add and enter in your cluster IP address and the same subnet mask as in Step 6

• Select Next

• In the New Cluster: Cluster Parameters window, confirm the IP address and subnet mask, then enter a Full Internet Name , though this is optional

• Ensure the cluster operation mode is set to Multicast

• Click Next

• In the New Cluster: Port Rules window, click Edit

• If you want you can restrict the cluster IP to work on an individual port or across a port range. You can also simply allow the cluster IP to work across all ports on the server

• Ensure your port rules are set to Single Host in the Filtering Mode section

• Click OK

• Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

• From the secondary server navigate to Start → Administrative Tools → Network Load Balancing Manager

• Click the Cluster menu item and select Connect to Existing . Note: the existing cluster will need to be running before a secondary node can be added

• In the Connect to Existing: Connect window, enter the IP address of your existing cluster as the Host and click Connect

• Select the existing cluster that appears in the Clusters section and click Finish

• In the main Network Load Balancing Manager , expand Network Load Balancing Clusters and right-click on your Cluster (it may be the IP address of your cluster) and select Add Host to Cluster

• In the Add Host to Cluster: Connect window, enter the IP address of the secondary server in the Host: section and click Connect

• When the Interface Name and Interface IP appear, select the Interface Name and click Next

• In the Add Host to Cluster: Host Parameters window, confirm the IP address and subnet mask and ensure the Initial Host State is set to Stopped . As this is the second node you're adding to

your cluster, the Priority should be set at 2

• Click Next

• Just as with the primary node, in the Add Host to Cluster: Port Rules window you have the ability to set this node to respond via specific ports or a port range. If you wish to set these rules, click Edit . Otherwise, click Finish to complete the setup

• Wait for the nodes to converge and, if necessary, stop the secondary sever by right-clicking the second server's name, select Control Host → Stop

Configure a Shared Service Directory

• Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. Note: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.

• Inside that new SmarterMail folder, create a Settings folder

• Configure your permissions accordingly. The SmarterMail service needs to run as a domain account or a local account with bidirectional authentication. You can configure this within the Windows Services console. When running SmarterMail with failover, Local System, Local Service and Network Service users are not allowed. Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

• Manually install and configure a primary SmarterMail server using the .MSI file available from the SmarterMail downloads page . Then, stop the service on this primary installation.

• Manually install another SmarterMail Enterprise instance on a second server. This new installation will be your standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.

• Stop the SmarterMail service on the standby

• Edit the failover.json file in the primary server's Settings folder as follows.

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer

• IsEnabled - Set this to True

• SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this (this example is for a Windows server):

```
{ "NodeId": "a51eba87-c8c6-49e3-812f-84e46ab617e7", "FailoverIPAddress":
"122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath":
"\\\\serverName\\SmarterMail\\Service\\Settings" } The code should look
like the above: casing, proper escaping of paths, etc. in order for the
JSON to be read properly.
```

```
• Save this file, then copy it to the standby's Settings folder, replacing
the existing failover.json
• Copy over all folders and files from SmarterMail's Settings folder to the
Settings folder in the shared service directory you created.
• Start the service on the standby server and verify that the paths are
pointing to the network shared paths
• Activate your Enterprise key on the standby by logging into SmarterMail's
management interface as the system administrator and going to the
activation section. Then stop the SmarterMail service on the server
• Start the service on the primary server, then reactivate your Enterprise
license key in the SmarterMail management interface
• After re-activating the license, go to IP Addresses and bind all the
ports to the load balancer's IP address and make sure no other IPs have any
ports bound to them
• Both servers are now set up for failover. To verify this, log into the
primary server as the system administrator and go to Gateways / Failover .
The servers that are part of the failover cluster will be displayed on the
Failover Servers tab.
```

Adding Failover to an Existing Installation of SmarterMail Note: You will need to configure both servers for Network Load Balancing and set up a shared service directory. See the steps outlined in the Adding Network Load Balancing to Your Servers , Configuring the Load Balanced Cluster for Use with Failover , Joining Additional Nodes to the Cluster and Configure a Shared Service Directory sections earlier in this document for more information.

• Ensure the primary server is running the latest version of SmarterMail and that it is also configured as an IIS site. Ensure the IIS binding is pointing to your cluster IP address

• Install SmarterMail on a standby and configure it as an IIS site. Ensure the cluster node is stopped on the standby and ensure the IIS binding is also pointing to the cluster IP

• Stop the SmarterMail service on the standby

• Copy all of your mail data (located in C:\SmarterMail\ by default) to your shared service directory. If possible, use robocopy to do this because it will not result in any downtime for the mail service

• Once robocopy finishes, run it one more time. This second pass will only copy any new data

• Stop the SmarterMail service on the primary server

• Edit the failover.json file in the primary server's Settings folder as follows:

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer

• IsEnabled - Set this to True

• SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this:

{ "NodeId": "a51eba87-c8c6-49e3-812f-84e46ab617e7", "FailoverIPAddress": "122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath": "\\\\\serverName\\SmarterMail\\Service\\Settings" } The code should look like the above: casing, proper escaping of paths, etc. in order for the JSON to be read properly. Also, due to size limitations, in the sample above the SharedSystemFilesPath is split across 2 lines -- that should be ONE line.

• Copy that failover.json file, after you've edited it, and move it to the same location on the standby. You should replace the file on the standby, if it already exists.

• Run the robocopy one more time to copy over any modified files and remaining spool emails

• Copy over all folders and files from the SmarterMail service's Settings folder to the Settings folder in the shared service directory you created.

• Edit the domains.json file in the shared Settings folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)

• Edit the settings.json file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on E:\SmarterMail, you would then perform a find and replace for all instances of E:\SmarterMail to \\NAS01\SmarterMail).

• On the primary server, go to Start → Administrative Tools → Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node

• Start the SmarterMail service on the standby

• Access SmarterMail's web interface at the cluster IP and sign in as the system administrator

• Activate your Enterprise key on the standby by logging into SmarterMail's management interface as the system administrator and going to the Licensing section.

• Verify that the data and settings are being picked up from the shared Service directory

• Stop the SmarterMail service on the standby and stop the secondary cluster node

• Start the cluster node and the SmarterMail service on the primary server

• Sign into the web interface on the primary server and re-activate the Enterprise license key by going to the Licensing section.

• Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

Below is an example of a PowerShell script that can be created to automate the SmarterMail failover process. You can utilize a third party monitoring product such as PRTG or SolarWinds (though there are many others) to execute this script when a failure is detected.

Prepping PowerShell on the Servers

The servers will need to be configured to run remote scripts and accept remote PowerShell sessions. Therefore, on each server, run the following commands within an elevated PowerShell console:

- Set-ExecutionPolicy RemoteSigned - Press Y to accept
- Enable-PSRemoting -force

Sample Script - Stop a Primary Server and Start the Hot Standby

In the scripts below, replace the "WAN" variable called in the –hostname parameter with the name of your interface. This can be obtained by opening a PowerShell console on the server and typing Get-NlbClusterNodeNetworkInterface . Also replace Server01 and Server02 with the NetBIOS names of your servers.

```
$StopPrimary = New-PSSession -ComputerName Server01 Invoke-Command -Session
$StopPrimary -ScriptBlock { Import-Module NetworkLoadBalancingClusters ;
Stop-nlbclusternode -HostName Server01 -InterfaceName "WAN" ; import-module
WebAdministration ; stop-webapppool SmarterMail; set-service -computerName
Server01 -name mailservice -status stopped ; remove-pssession Server01}

$StartSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StartSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; set-service -computerName Server02 -name mailservice
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-pssession Server02 }
```

Sample Script - Stop the Hot Standby and Re-start the Primary Server

These scripts can be used to bring the primary server back online and stop the standby after your monitoring software issues an all-clear.

```
$StopSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StopSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool
SmarterMail; set-service -computerName Server02 -name mailservice -status
stopped ; remove-pssession Server02}
```

```
$StartPrimary = New-PSSession -ComputerName Server01 Invoke-Command -
Session $StartPrimary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server01 -
InterfaceName "WAN" ; set-service -computerName Server01 -name mailservice
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-pssession Server01 }
```

SmarterMail Add-ons

SmarterTools' add-on licensing system allows users to enhance the functionality of SmarterTools products. Information about the add-ons available for your installation, purchasing and/or activating add-ons can be found on the Licensing and Activate page of this online help.

The following add-ons are available for SmarterMail:

- EAS
- MAPI / EWS
- Message Sniffer
- Cyren Premium Antispam and IP Reputation
- Cyren Zero-hour Outbreak Detection

EAS

EAS is a data synchronization protocol that syncs email, calendars, tasks, and notes to virtually any iOS or Android mobile device. Some desktop applications, such as Windows Mail, People, and Calendar, which initially came with Windows 10 installations, also support EAS. However, these products are being phased out by Microsoft in favor of the "New Outlook". Therefore, EAS is most useful for email clients on mobile phones and tablets to sync to email accounts.

MAPI/EWS

MAPI provides users with native Microsoft Outlook synchronization and functionality at the server level. Available for Outlook 2016 and above, MAPI offers standard functionality such as syncing emails, calendars, contacts, tasks and notes, but also additional functionality that is available when connecting Outlook to Microsoft Exchange. This includes advanced features such as delegation, contact groups, Public Folders, and more.

EWS seamlessly syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients, including Apple Mail for MacOS and eM Client for Windows and MacOS. EWS allows for fast communication between an email client and the mail server and also supports advanced features such as delegation, contact groups, etc.

Message Sniffer

Message Sniffer complements SmarterMail's built-in antispam functionality and accurately captures more spam, viruses, and malware when combined with SmarterMail's "out of the box" protection. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks.

This add-on can be purchased directly from the SmarterTools website by logging into your account and adding it to any SmarterMail license.

Cyren Premium Antispam and IP Reputation

The Cyren Premium Antispam add-on is a service that uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time as messages are mass-distributed over the internet. Rather than evaluating the content of messages, the Cyren Detection Center analyzes large volumes of internet traffic in real time, recognizing and protecting against spam outbreaks the moment they emerge.

In addition, the Cyren Premium Antispam add-on includes, at no extra cost, Cyren IP Reputation checks. Cyren IP Reputation builds upon what existing RBLs and URIBLs provide by handling the vast gray area of IPs and IP sources that have little or no information. For example, machines that are hijacked and used by botnets that dynamically use, and abuse, the innocuous IP addresses on those hijacked machines. Cyren analyzes hundreds of millions of messages every day, so they are able to classify (and re-classify), in real-time, the reputation of each IP source.

This add-on can be purchased directly from the SmarterTools website by logging into your account and adding it to any SmarterMail license.

Cyren Zero-hour Outbreak Detection

The Cyren Zero-hour Outbreak Detection add-on is a service that identifies new, "zero hour" viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology, protecting in the earliest moments of malware outbreaks and continuing protection as each new variant emerges. It's worth noting that Cyren Zero-hour works best in conjunction with other antivirus products, like the native implementation of ClamAV.

This add-on can be purchased directly from the SmarterTools website by logging into your account and adding it to any SmarterMail license.

Antispam and Antivirus Integration

Powerful antispam and antivirus functionality is included with every copy of SmarterMail. However, some users may need extra protection or have fixed infrastructures. The solutions listed on this page have been tested with SmarterMail, but you can integrate almost any command-line scanner or real-time scanner with SmarterMail.

Message Sniffer

Message Sniffer complements SmarterMail's built-in antispam and antivirus features and accurately captures more than 99% of spam, viruses, and malware right out of the box. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks. The Message Sniffer solution is available as an integrated add-on to SmarterMail from the SmarterTools website and authorized SmarterTools resellers.

- Learn more about MessageSniffer

Cyren Premium Antispam

When coupled with SmarterMail, Cyren Premium Spam protection delivers upwards of 99% spam protection. Cyren technology complements SmarterMail's out-of-the-box antispam features by adding email transmission pattern recognition. The Cyren Premium Antispam solution is available as an optional add-on to SmarterMail from the SmarterTools website and authorized SmarterTools resellers.

- Learn more about Cyren Premium Antispam

Cyren Zero-hour Outbreak Detection

The Cyren Zero-hour Outbreak Detection uses Recurrent Pattern Detection to identify viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology. Cyren Zero-hour Outbreak Detection is available as an optional add-on to SmarterMail through the SmarterTools website and authorized SmarterTools resellers.

- Learn more about Cyren Zero-hour Outbreak Detection

Microsoft Defender (Windows Only)

Microsoft Defender (formerly Windows Defender) uses machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices (or endpoints) in an

organization. It comes pre-installed on most versions of Windows desktop and Windows Server. For integration instructions, please search the SmarterTools Knowledge Base .

- Learn more about Microsoft Defender

ClamAV

ClamAV is an open-source project that provides mail servers with decent protection from viruses at no cost. SmarterTools has found ClamAV to be a valuable scanner to use, especially in lower-volume environments. For integration instructions, please search the SmarterTools Knowledge Base .

- Lean more about ClamAV Declude

Control Panels

SmarterTools has spent considerable effort into providing a solid Web services implementation in its products in order to facilitate automation systems. As a result, more and more control panel providers are finding it easy to tie our products into their interfaces.

Plesk (7.5 or higher)

The integration of SmarterMail with Plesk is fully embedded within the Plesk product. No additional downloads are necessary to complete the integration.

- Learn more

WebSitePanel

The integration of SmarterMail with WebSitePanel is fully embedded within the WebSitePanel product. No additional downloads are necessary to complete the integration.

- Learn more

WHMCS

The integration of SmarterMail with WHMCS is available as a free add-on, which can be downloaded from the WHMCS App Store. Two modules are available: an admin area module for basic SmarterMail management, and a provisioning module that allows for multiple SmarterMail servers, adding domains, webmail log in and more.

- Learn more

HostingController

The integration of SmarterMail with HostingController is fully embedded within the HostingController product. No additional downloads are necessary to complete the integration.

• Learn more

Automation with Web Services

SmarterMail was built with custom configuration in mind. In addition to being able to customize the look and feel of SmarterMail, developers and/or system administrators have the ability to code to the SmarterMail application using its extensive and comprehensive APIs. Virtually every aspect of SmarterMail is exposed via web services, allowing developers and/or system administrators to automate a variety of different things: add domains to SmarterMail on the fly, grab domain-specific bandwidth usage for billing purposes, set details on a specific domain or server, update domain information, and more. note: The current API is JSON-based. Previous iterations of the API used SOAP calls. As such, any discussion of the "SmarterMail API" will refer to the current version and not the legacy version of the API. Code samples are based on the current API as well. In addition, current/new functionality built into SmarterMail will not have any legacy API calls as that functionality is not available in older/previous/legacy versions of SmarterMail.

For the most up-to-date API information, including all calls and examples, system administrators should navigate to their Settings , then click API Documentation in the navigation pane. This will open the current API documentation in its own window. It's also possible to view the SmarterMail documentation for the SmarterTools installation, which is always up-to-date: SmarterTools Web Services documentation .

Web services are intended for use by high-volume and automated business environments as well as hosting companies and ISPs as they develop procedures to manage their SmarterMail system and workflow. It's assumed that a basic understanding of Web service technologies and ASP.NET programming when working with our APIs. Important Note: SmarterMail will occasionally update our API documentation as well as deprecate calls as they become outdated or are no longer used. However, legacy calls for legacy products are not updated. The API documentation is included with each update released by SmarterTools, and is also reflected in the link to the API documentation included above. API documentation for any legacy products is not, and can not be, supported.

Integrations

SmarterMail for WHMCS

Overall Description

SmarterMail for WHMCS consists of two complementary open-source modules: one for setting up a server for use within WHMCS, and one for provisioning "plans" or "products" that can be sold within WHMCS. The provisioning module includes the ability to create packages based off specific

SmarterMail features such as mailbox counts, disk space allocations, etc. It also offers domain administrators and end users some management capabilities. For example, domain administrators can add users, add aliases, and more while end users can see some basic information about their accounts as well as log directly in to SmarterMail.

These were developed by SmarterTools as replacements for the two previous WHMCS modules that were available. As a result, anyone transitioning to the new modules will need to create new products within WHMCS. Customers who use products configured using the older module can coexist with customers created using the new modules, but for the sake of consistency we recommend those customers be moved over to new products created using this newly developed solution. Note: As both modules work together, they both need to be installed even if only using the features in one or the other.

Skip to:

- • Prerequisites
- • Installing the Modules
- • Configuring the Addon Module
- • Configuring Your Server(s)
- • Configuring Your Product(s)/Service(s)
- • Configurable Options
- • Custom Fields
- • Enabling Debug Logging

Goals

The primary goals of the integration of SmarterMail are twofold:

- • Allow businesses to create email packages based off configurable options within SmarterMail, such as individual mailbox size, the ability to synchronize to email clients and mobile devices with Exchange-like features, etc., and
- • Reduce both domain and server administrator labor. With the module installed, the process of setting up a SmarterMail server, then managing domains and accounts on the server, is automated through WHMCS.

The integration provides the following services:

Admin Area Features

- • Create Domains
- • Suspend Domains
- • Unsuspend Domains

• Terminate Domains

• Upgrade Packages

• Add Configurable Options for complementing Products/Services

• Add/manage Configurable Options

• Add/manage Custom Fields

• Change Passwords

Client Area Features (i.e., Domain Administration)

• Manage Mailboxes: Add, delete, modify settings, change passwords

• Manage User Aliases: add/delete

• Manage Domain Aliases

• Login to the SmarterMail webmail interface

• Upgrade/Downgrade Products

• Upgrade/Downgrade Options

Prerequisites

• Existing installation of WHMCS.

• Existing installation of WHM/CPanel. (If used.)

• Licensed installation of SmarterMail Build 100.0.8580 or later .

Installing the Modules

Installing the SmarterMail module is no different than installing any modules within WHMCS.

• Extract the zip file that contains the SmarterMail module and add-on.

• Rename the smartermail_addonmodule folder to "smartermail" and place it in "WHMCS\modules\addons".

• Rename the smartermail_provisioning folder to "smartermail" and place it in "WHMCS\modules\servers".

Configuring the Addon Module

• Login to the admin side of your WHMCS installation.

• Go to System Settings → Addon Modules

• Click "Activate" next to "SmarterMail Module"

• Click "Configure" next to "SmarterMail Module" and set it up as per your usual module configurations. Be sure to set the appropriate Access Control permissions as well.

Next, you will want to set up the actual SmarterMail server.

Configuring You Server(s)

Once the SmarterMail module is installed, you can begin adding new mail servers to your WHMCS installation and begin provisioning domains and mailboxes within SmarterMail.

Creating a Group

While this step is optional, creating Groups for servers you set up in WHMCS is a great way to help keep things organized. Therefore, it's recommended that you set up a group for your SmarterMail server(s).

- On the Servers page, click the "Create New Group" button.
- Set a group name. (E.g., Mail Servers)
- Fill Type is purely optional and based on preference.
- In the "Selected Servers" box, choose your SmarterMail Server(s).
- Click the "Add" link to move the server(s) from the left to the right box.
- Be sure to "Save Changes".

Adding a Server

- Click on "Servers" under the Products/Services on the left menu. Alternatively, select "Servers" from the System Settings area.
- Click "Add New Server"
- When presented with the Add Server info, click the blue "Go to Advanced Mode" button as this gives you more options.
- Fill in the following settings:

- Name - The friendly name for your SmarterMail server within WHMCS
- Hostname - The hostname for your server. (E.g., mail.your_domain.com)
- IP Address - The primary IP address for your SmarterMail server.
- Assigned IP Addresses - Re-enter the primary IP as well as any other IP addresses used by your SmarterMail server.
- Module - Select "SmarterMail" from the dropdown.
- Username/Password - The username and password of the primary system administrator set up on the server.
- Secure - Ideally, you WILL want to use SSL for the connection, so check this box.
- Be sure to Save Changes.

If you experience problems, and Module Logging is enabled, you can go to http(s)://your_WHMCS_hostname.com/admin/addonmodules.php?module=smartermail to check the error logs

Configure Your Product(s)/Service(s)

Now that the modules have been installed and the SmarterMail server(s) configured, you now can configure individual Product\Service packages within WHMCS based on SmarterMail.

As with Servers, you can create groups of products/services to help keep things better organized. Again, this is recommended, though purely optional. For the sake of this section, we will create a "SmarterMail" group, then add products to that group.

Create a Product Group

- If not already, login to the admin side of WHMCS.
- Go to System Settings → Products/Services. (Alternatively, if you're already in an administrative area of WHMCS, select "Products/Services" from the left navigation menu.)
- Click the "Create New Group" button.
- Set your "Product Group Name". (E.g., SmarterMail)
- Add in any additional information as you see fit, such as the Group Headline, Tagline, and Features. You can also select an Order Form Template that customers will use to order the product(s).
- Be sure to save your changes.

Create a Product

- Click the "Create New Product" button.
- Select the product type.
- For "Product Group", select the group you created above.
- Set the "Product Name". (E.g., Basic Email.)
- For the "Module", select SmarterMail from the dropdown.
- Click the "Continue" button. Once this is done, you'll be presented with a number of tabs detailing various aspects of your new product. For example, the Product Details, Pricing, Configurable Options, etc.
- Once everything is configured, be sure to "Save Changes".

A Note About Module Settings

The SmarterMail module gives providers the ability to configure various features of SmarterMail based on the product that is created. The idea, here, is that service provider can create email "packages" based on the features available. For example, a basic email plan may offer email a minimal number of users, aliases, mailbox size, and domain disk space. Then, a more robust product can be created that increases things like disk space and mailbox size, then adds mailing lists, automated forwarding, live chat, and file storage.

Configurable Options

A new feature of the module is the ability to create "email plans" that offer base limits for things like account size, domain disk space, and more. However, there are times when users may require more allocations for these things than they were originally provided, or they require additional features that aren't part of their actual hosting plan. The ability to sync their account to their mobile device, for example, using EAS.

In these cases, configurable options can be used to create "Add Ons" for existing products you've created. A Configurable Option will essentially override the standard settings used to initially create the products within WHMCS. Users can then include these options prior to checkout, or they can be added to a user's plan on an as needed basis. Each option can have its own pricing, thereby creating additional revenue opportunities.

WHMCS will pass information to SmarterMail when you set up configurable options using the following format: <variable size> | <friendly text>. (Where "variable size" requires numerical values only.)

For example, to add and options for adding EAS accounts, you would create a configurable option like this: 5 | 5 EAS Accounts = 5 EAS Accounts 10 | 10 EAS Accounts = 10 EAS Accounts

Adding the friendly text makes the options more descriptive, so users know exactly what they're getting.

The following are available as Configurable Options, with the associated, internal variable name in parentheses:

- Users (users) - The number of users supported by the domain. (E.g., 10 | Additional Users)
- Mailbox Size (mailbox_size) – Size, in MB, to set the mailbox size for each user. (E.g., 1000 | 1 GB)
- Domain Size (domain_size) – Total size, in MB, allowed for the domain. (E.g., 10000 | 10 GB)
- Aliases (aliases) – Number of user aliases. (E.g., 100 | 100 Aliases)
- Domain Aliases (domain_aliases)– Number of domain aliases. (E.g., 10 | 10 Domain Aliases)
- EAS Accounts (accounts_eas) – Allowed number of EAS devices/users. (E.g., 20 | 20 EAS Accounts)
- MAPI & EWS Accounts (accounts_mapiews- Allowed number of EWS/MAPI users. (E.g., 20 | 20 MAPI & EWS Accounts)
- Exchange Accounts (accounts_exchange) – Combines both MAPI & EWS Accounts and EAS Accounts into one option so you don't have to set each item individually. (E.g., 20 | 20 Exchange Accounts)

Create a Group

• If not already, login to the admin side of WHMCS.

• Go to System Settings → Configurable Options. (Alternatively, if you're already in an administrative area of WHMCS, select "Configurable Options" from the left navigation menu.)

• Click the "Create a New Group" button.

• Set your options, such as Group Name, Description, and select the Assigned Products.

• Save your changes.

Configurable Option Groups

Manage Group

Group Name	SmarterMail Options
Description	These modify your SmarterMail package as desired.
Assigned Products	Email Hosting - SmarterMail 50 Users Email Hosting - SmarterMail 500 Users Email Hosting - SmarterMail Enterprise Email Hosting - SmarterMail Basic

Configurable Options

Add New Configurable Option

Option	Sort Order	Hidden		
mailbox_size | Mailbox Size	0	☐		
domain_size | Domain Quota Upgrade	0	☐		
aliases | User Aliases	0	☐		
accounts_eas | EAS Device Quota	0	☐		
accounts_mapiews | MAPI/EWS Device Quota	0	☐		
domain_aliases | Domain Alias Quota	0	☐		

Save Changes   Back to Groups List

Create Options

• Click the "Add New Configurable Option" button. Set the Option Name and the Option Type. For many options, the Dropdown type will suffice as it allows you to create multiple "upgrades" based on counts. (E.g.,

• Disk Space increases.)

• Continue adding Options to the group until finished. NOTE: it IS possible to add multiple options to ONE group.)

• Be sure to save your changes, the close the Configurable Options window.

• Save your changes on the Configurable Option Groups page.

This is what the option would look like for adding disk space for a domain:

Custom Fields

Custom fields allow for some customization of product creation and can help automate things like setting up domains and users within SmarterMail. "Username" is a perfect example of a custom field as it can be used to set the username for a user that essentially becomes their email address.

To add Custom Fields, do the following:

- Click Wrench/Settings → System Settings → Products/Services
- Select the desired Product.
- Field names use the following format: <variable name> | <friendly text>
- You can use Regex in the validation field as all the supported fields use Text boxes. For example: Ask for a username/password combo to create the domain admin account, "sm_username|Username" and "sm_password|Password"

The variables available for Custom Fields are as follows:

- sm_hostname - Sets a custom hostname for the domain. By default, SmarterMail creates the hostname as "mail.{domain}". Using this Custom Field allows you to use a different hostname.
- sm_username - Initial username that is appended to the "@@domain" for the email address. If this is left blank, it defaults to the first 8 characters of the domain name.
- sm_password - Initial user password. If this is left blank, a 10-character password is automatically generated.

Enabling Debug Logging

There is debug logging available in the module, but it's not turned on by default. To turn it on do the following:

- Open modules\addons\smartermail2\smartermail2_functions.php
- Find line 630
- Uncomment the line (logActivity($msf, $num);
- Save your changes

The file can be edited while WHMCS is running, so no need to stop/restart. The log is saved to the "System Logs" and can be accessed from the WHMCS admin area.

Odin APS (Automated Provisioning System) Package for SmarterMail

Package Description

The SmarterMail APS package is designed to integrate SmarterTools' SmarterMail email server software within the Parallels Operations Automation system. SmarterMail can then be used as the mail server of choice for Odin administrators when creating hosting plans for resale, when adding domains that require email services and more.

Package Goals

The goal of the SmarterMail APS package was to provide a means of easily managing domains, mailboxes, mailings lists and aliases. To those ends, services provided include:

- Domain Services

- Add / Remove Domains
- Add / Edit / Remove Domain Aliases
- Add / Edit / Remove User Aliases
- Domain Disk Space Reporting
- Mailbox Services

- Add / Edit / Remove Mailboxes
- Configure Email Forwarding Settings
- Configure Auto-responder Settings
- Mail List Services

- Add / Edit / Remove Mailing Lists
- Add / Edit / Remove Mailing List Subscribers

Prerequisites

This goes over the list of requirements that are needed before installing, configuring and using the SmarterMail APS package. These requirements are as follows:

- Existing installation of Parallels Operations Automation (PoA)
- Existing, licensed installation of SmarterMail 9.x or above
- Required knowledge in the following areas:

- Application Manager

- APS catalog
- Importing packages
- Provisioning Manager

- Resource templates
- Service templates
- Customer Manager

- Creating of customers
- System director

- Task manager

Installation

This covers getting the APS package set up with the PoA system. There are two ways to install the SmarterMail APS package within PoA using the Application Manager: from Applications or the APS Catalog

- • Applications

- • Expand Service Director
- • Expand Application Manager
- • Select Applications
- • Click on "Import Package"
- • Select "local file" option and click "Choose File"
- • Provide the path to the SmarterMail APS
- • Check "Enabled" option
- • Finally, click "Submit" and the package will be scheduled for importing
- • APS Catalog

- • Expand Service Director
- • Expand Application Manager
- • Select APS Catalog
- • Select the "Application" field and search for 'SmarterMail*'
- • 'SmarterMailAPS' package should appear in the list
- • Check the box next to the Application column and click "Import Package"
- • On the next screen click "Import Packages" and the package will be scheduled for importing

Configuration

This covers the configuration of the SmarterMail APS package after it has been installed/imported into the PoA system.

Resource Types

Resource Types are used to define activation parameters, which are:

- • General package settings
- • Global settings
- • Default settings
- • Services

Creating an Application

The application resource is the crucial part of setting up the SmarterMail APS package. This defines the global settings that are used by each application service.

- Expand Service Director
- Expand Application Manager
- Select Applications
- Select the "Application" field and search for 'SmarterMail*'
- The results should yield the 'SmarterMailAPS' package that was installed prior (where applicable)
- Select the 'SmarterMailAPS' package
- Click the "Resource Type" tab
- Click "Create"

- Select Application from the Resource Class list
- Give it a name (Ex: SmarterMail App) & Description, click "Next"
- Fill in the following fields under the "Global application settings" section:

- SmarterMail public site URL
- SmarterMail installation host
- SmarterMail installation IP
- Primary System Administrator Login
- Primary System Administrator Password
- Primary MX
- Click "Next"
- Uncheck "Automatically provision application," click "Next"
- Check "External Provisioning," click "Next"
- Click "Finish"

Creating an Application Service

The application service is what defines the defaults for each service that used by the SmarterMail APS package (domains, mailboxes, etc.) .An application service will have to be created for each service that you want to provide.

- Navigate to the "Resource Types" section of the SmarterMail APS package. Follow the same steps when creating an application resource to get to this section.
- Click "Create"

- Select Application Service from the Resource Class List
- Give it a name (Ex: SmarterMail App Domain Service) & Description, click "Next"

- Select from the list of services the application service will be (Ex: SmarterMail Domain Service)
- Provide default values for this resource, then click "Next"
- Priority can be any number, so let's go with 1, Click "Next"
- Click "Finish"

Again, these steps must be repeated for each application service that is offered with the package.

Service Templates

This covers the creation of service templates for the package. A service template defines both subscription limits as well as what services are provided when using the package.

Creating a Service Template

- Expand Service Director
- Expand Provisioning Manager
- Select Service Templates
- Click "Add New Service Template"

- Provide a name & description
- Uncheck "Autoprovisioning"
- Set "Type" to Custom
- Click "Next"
- A list of available Resources will be shown

- Select the Resource Application that was created earlier as well as any of the Resource Application Services that were just created. For example, "SmarterMail App" and "SmarterMail App Domain Service"
- Click "Next"
- Set the limits of the service template

- Check Unlimited for the Resource Application (Ex: SmarterMail App), Application Backup and Application User
- Resource Application Services (Ex: SmarterMail App Domain Service) can be either set to unlimited or can have a limit applied to them
- Home Visibility is an optional field that can be checked, if desired, that provides usage information for the user when they log in
- Click "Next"
- Review your settings, then click "Finish"

Subscriptions

This covers the how to apply subscriptions to customers using the service template that was created early.

Creating a Subscription

- Expand Service Director
- Expand Provisioning Manager
- Select Service Templates
- Select the "Service Template" field and search for, then select, the service that was created prior
- Click "Activate" under the General section of the service template (the service template must be activated prior to adding a subscription)
- Click "Subscriptions" tab
- Click "Create New Subscription"
- Select the "Company" field and search for the company that will be subscribing to this template, then select the company from the search results
- Set additional resource limits for the subscription if desired (subscriptions will inherit the values from the service template by default)
- Click "Next"
- Review the settings and click "Finish"

The company selected now has the ability to use the SmarterMail APS package.

Package Setup and Usage

This covers the steps required before provisioning and usage of the package can be conducted.

Setup

Creating a Domain

- Expand Operations Director
- Expand Customer Manager
- Select Customers
- Select the "Company" field and search for a company, then select the company from the search results
- Click the Resources tab
- Click "Add New Domain"

- Provide a domain name (e.g., example.com)
- Check "Set Registrar Status to Ready"

- Select the SmarterMail APS subscription from the "Subscription" dropdown
- Click "Next"
- Click "Next" again
- Review the settings and click "Finish"

A domain is required to be associated with the package so the domain can be properly added with the package. After a domain has been added, the package can start being used.

Usage

This covers an example usage of using the package by creating a domain as a customer.

Login

- Expand Operations Director
- Expand Customer Manager
- Select Customers
- Select the "Company" field and search for the company, then select the company from the search results
- Click "General" tab
- Click "Staff Members" and a list of staff members will be shown
- Click "Login as Customer"

Configure

- Click the "SmarterMailAPS" link towards the bottom of the page
- Click "Add New"
- Fill in the following fields:

- Display Name
- Check "Login in existing domain"
- Fill in the user name
- Fill in the password (Generate New Password can be used to generate a random password for this account)
- Click "Next"
- If "Display Name" was supplied from the previous step, the system administrator's first & last name will be filled in. If not, it is optional to provide a first & last name
- Click "Next"
- Review the settings and click "Finish"
- The account and the domain will be scheduled for provisioning

The steps when configuring each service are the same for each service the package provides. Simply fill out the required fields for each service and follow through each wizard.

Website Panel Module for SmarterMail

Package Description

WebsitePanel (WSP) is a multi-tenant, enterprise hosting automation tool with support for private cloud servers. It enables you to centralize the management of your hosting infrastructure and share resources across multiple customer accounts. This product can be used with SmarterMail and SmarterStats to deploy users and domains\sites from a single interface.

Package Goals

The SmarterMail WebsitePanel module allows the administrator to create, remove, and manage domains, users, mailing lists, and aliases. User settings that can be modified include the ability to change mailbox size, manage passwords, set domain admins, manage autoresponders and mail forwarding. Advanced settings and server settings are managed from within the SmarterMail domain and / or system administrator logins in SmarterMail itself. Server defaults will want to be configured prior to integrating with WSP.

The SmarterStats WebsitePanel module allows site and user creation, and allows the ability to link directly to the site to view reports as a particular user. Server and site/domain settings will need to be managed on the server itself.

Prerequisites

- You will need to be registered with WebsitePanel in order to access the download links
- Microsoft.NET framework 4.0 (ensure this is registered within IIS)
- IIS 6.0 or higher
- Microsoft SQL Server, installed locally or hosted remotely
- Licensed install of SmarterMail 9.x or higher and / or SmarterStats 7.x or higher

Configuration

Once all of the prerequisites are met, configuring the modules is fairly straightforward. The steps below cover adding a new server to your environment, creating a hosting plan, and creating a customer account to utlize the server resource that was set up.

Adding a Server

When you're ready to add a new server, ensure the server password is configured in the Website Panel installer.

• Navigate to Configuration → Servers

• Click Add Server

• Enter the Server Name, the URL, and Server Password (this is configured in the WebsitePanel installer)

• Server URL: http://127.0.0.1:9003 (default)

• Enter the password configured during the initial setup

• Ensure "Check for installed software" is selected

• SmarterMail and SmarterStats should be picked up during the installed software check. These services will need to be configured separately, however. Navigate to Configuration → Servers. You should see your server, and the services associated.

• Click on SmarterMail 10.x +

• Set the SmarterMail web services URL

• Select a public IP address

• Set the Admin Login

• Configure any additional options

• Click Update

• You should be back in the server configuration page.

• To configure SmarterStats, scroll down and Click SmarterStats 5.x +. Otherwise, skip to step 5

• Set the SmarterStats web service URL

• Specify admin credentials

• Select the SmarterStats server

• Click Update

• You should now have a server set up for the particular service resource.

Creating a Hosting Plan

Below you will find the steps for creating a hosting plan that uses the particular server and service resource you've created.

• Navigate to Account Home

• Click on Hosting Plans in the left hand menu

• Click Create Hosting Plan

• Set the Plan Name

• Set the target server to your desired server with the particular service resource attached

• Set your quotas

- Check System, then set desired options

- Check Websites (Only necessary for SmarterStats) , then set desired options

- Check Mail, then set desired options

- Check Statistics, then set desired options

- Click Save

- You should now have a hosting plan set up that uses the particular service resource.

Creating a Customer Account

Below are the instructions for creating a customer account that will utilize the resource and hosting plan created.

- Navigate to Account Home
- Select Customers from the left hand menu
- Click Create User

- Enter a Username and Password
- Fill in all other required information
- Click Create
- It will bring you to a new window with an option to create a new hosting space. Click Create hosting space to begin the process

- Select your hosting plan that this will apply to, fill out required fields and select Create Space
- After the space has been created you will need to create a domain for your users within SmarterMail

- Sign into WSP with the newly created user
- Navigate to Domains, and select Add Domain
- Set the domain name, ensure create website is checked (for SmarterStats)
- Leave the other checkboxes un-ticked
- Click Add Domain
- Using the hosting space menu on the left, navigate to Mail → Accounts, and select Create Mail Account

- Fill in the email address, and select the domain that was created in step 6
- Enter a Password
- Set the Mailbox Size Limit
- Specify customer information, and a signature if necessary
- Enable\Disable Autoresponder
- Enable\Disable Mail forwarding
- Click Save

• This will prompt WSP to call the SmarterMail web services to create the domain, and the newly created user. I have not found a way to purely add just a domain to SmarterMail using WSP. A user must be created to prompt the domain creation

• Using the hosting space menu on the left, navigate to Advanced Web Statistics and click Add Statistics Site

• Select the website that was created in step 6c, the site ID will populate on its own once the site is created

• Specify your users, and passwords

• Click Add Site

• The statistics site will then be added into SmarterStats. You can view the site statistics by navigating to Advanced Web Statistics and click View Statistics, you will automatically be signed in as the user.

• You should now have a new customer set up that can take advantage of your hosting plan that uses SmarterMail.

Marketplace

Marketplace Overview

The Marketplace provides SmarterMail users with access to various add-ons that complement the functionality of their SmarterMail experience. These add-ons may include document collaboration tools, chat applications, AI integration, communication platforms, and more. The Marketplace categorizes the integrations by purpose. For example, File Storage will include any cloud storage providers that can be used with SmarterMail. The Marketplace offers both free and paid options, allowing users to customize their environment based on their needs using the tools, applications, and services they want.

Purpose

The primary purpose of Marketplace is to extend SmarterMail by extending the functionality by integrating a variety of popular applications and services. Our goal is to give administrators the freedom to choose the tools they prefer, rather than having SmarterTools build everything directly into SmarterMail.

SmarterMail's Marketplace will leverage existing, well-known products, such as email clients, chat and online meeting tools, AI solutions, and more. SmarterTools intends to empower administrators to work with tools they're already comfortable using. Unlike others who build these features into their platforms, we believe there's no need to reinvent the wheel. This approach not only offers greater flexibility but also transforms SmarterMail into a fully fledged communications platform.

Through the Marketplace, users can:

- Integrate various tools and services for better communication and collaboration.
- Customize SmarterMail's functionality to meet specific business needs.
- Extend the platform's utility through seamless add-on integrations.

Benefits

Marketplace streamlines management by providing tools and functionality that require minimal configuration. System Administrators and Domain Administrators can create a more efficient and tailored email and collaboration platform for their teams.

For Users

- Enhanced Productivity: Marketplace serves as a comprehensive hub for email communication, inter-office chatting, and document sharing.
- Seamless Integration: The Marketplace functionality allows for easy integration of apps with

SmarterMail, ensuring a smooth user experience and minimizing disruption in workflow.

• Extensive Add-ons: Marketplace offers a wide variety of third-party apps, enhancing productivity and enabling users to personalize their email experience based on their specific needs.

For Domain Administrators

• Greater Customization: Tailor the SmarterMail environment to align with the domain's operational needs.

• Simplified Management: Access tools and functionalities without extensive configuration.

• Improved User Experience: Offer end-users additional capabilities like document sharing, chat options, and more.

For System Administrators

• Centralized Access: Easily manage and integrate add-ons from a single interface.

• Enhanced Flexibility: Choose functionalities based on organizational requirements rather than relying solely on pre-built features.

• Scalable Infrastructure: Incorporate new tools as your communication needs grow.

Quick Links

AI Integration

• AI Integration Overview
• OpenAI

Document Collaboration

• Document Collaboration Overview
• OnlyOffice
• Collabora

Live Chat

• Live Chat Overview
• RocketChat

Online Meetings

• Online Meetings Overview
• SmarterMail Meetings

File Storage

- File Storage Overview
- Google Drive
- Dropbox
- OneDrive
- ownCloud
- Leitzcloud/vBoxx
- SmarterMail File Storage

Email Client

- Email Client Overview
- eM Client

Marketplace Help for Users

Getting Started with Marketplace

SmarterMail can connect to third-party cloud storage providers such as Dropbox, OneDrive, Google Drive, vBoxx, Leitzcloud , and OwnCloud . So users can generate links to files stored in the cloud while composing emails. This allows users to quickly share files without worrying about attachment size limits on the server or increasing their mailbox size as you simply link to the file at its original location, the file isn't actually attached to the message. note: The availability of items in the Marketplace is controlled by administrators. System administrators have overall control, while Domain Administrators can enable or disable options if they have been granted permission by a system administrator. If neither administrator enables any options for users, the Marketplace will not appear in the interface.

- Accessing the Marketplace: Log into your SmarterMail account and navigate to the More tab, then click on the Marketplace link.
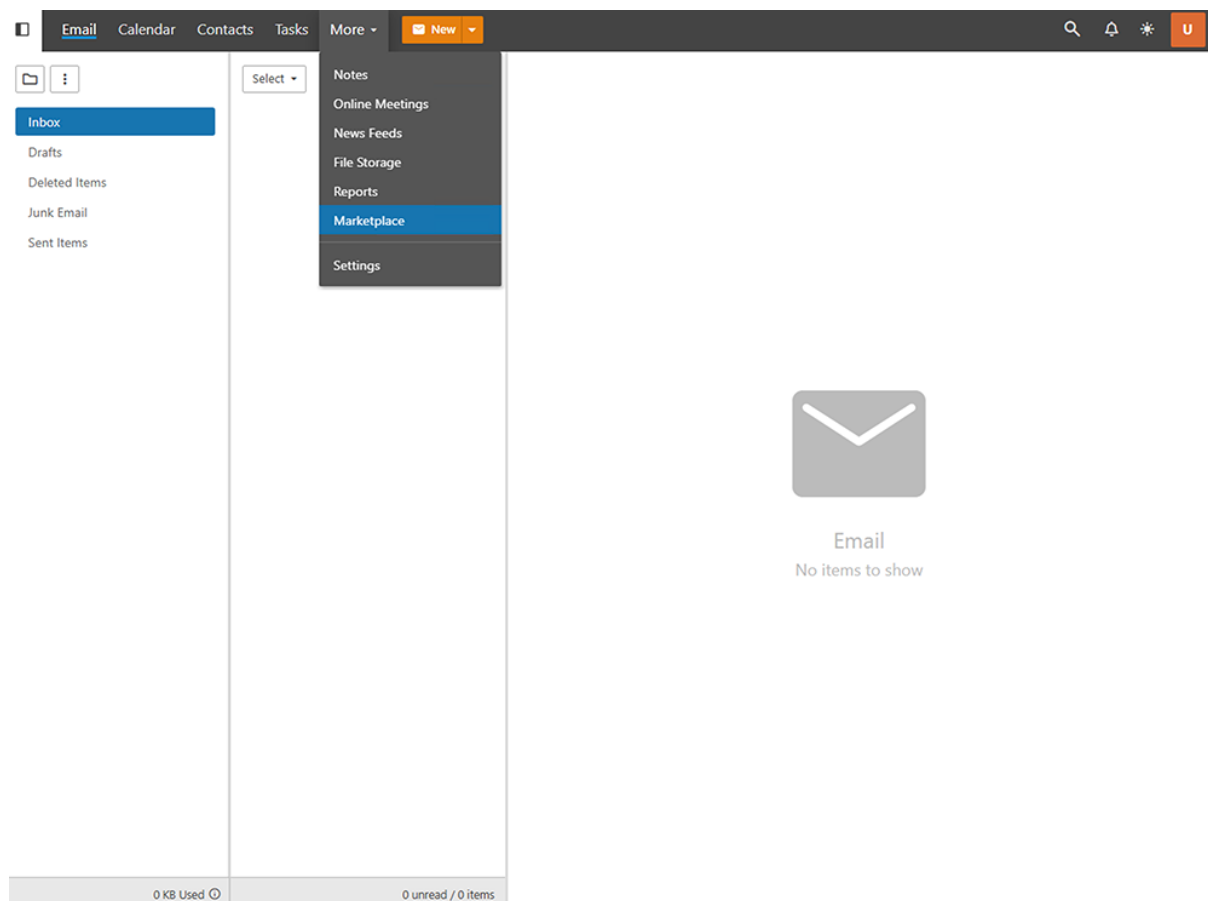
• Browse Available Add-ons: Explore the available options, filtering by functionality, such as AI Integration, Document Collaboration, Chat or File Storage .
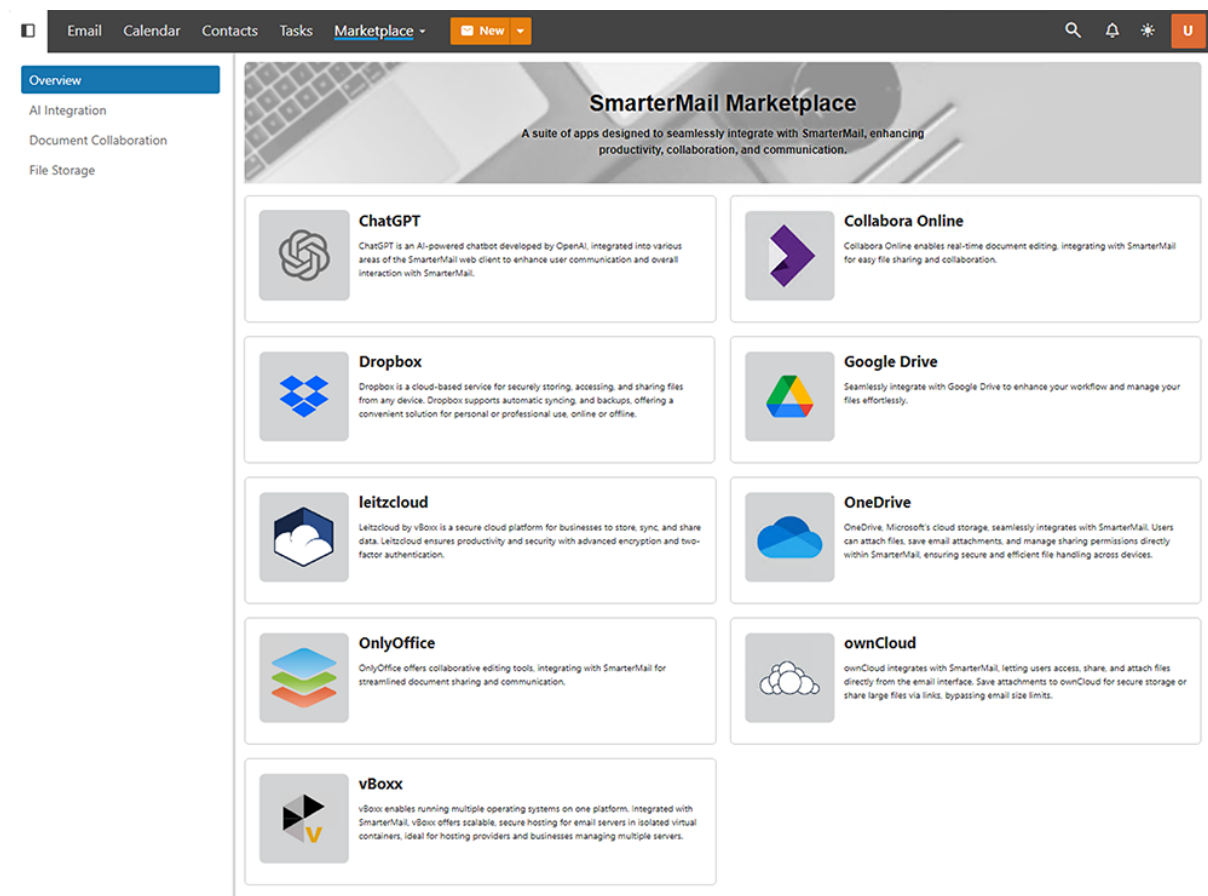
• Connecting a Cloud Service: To establish a new connection with a cloud storage provider, click More , then Marketplace . Select the service you wish to connect, then follow the on-screen prompts to complete the process.
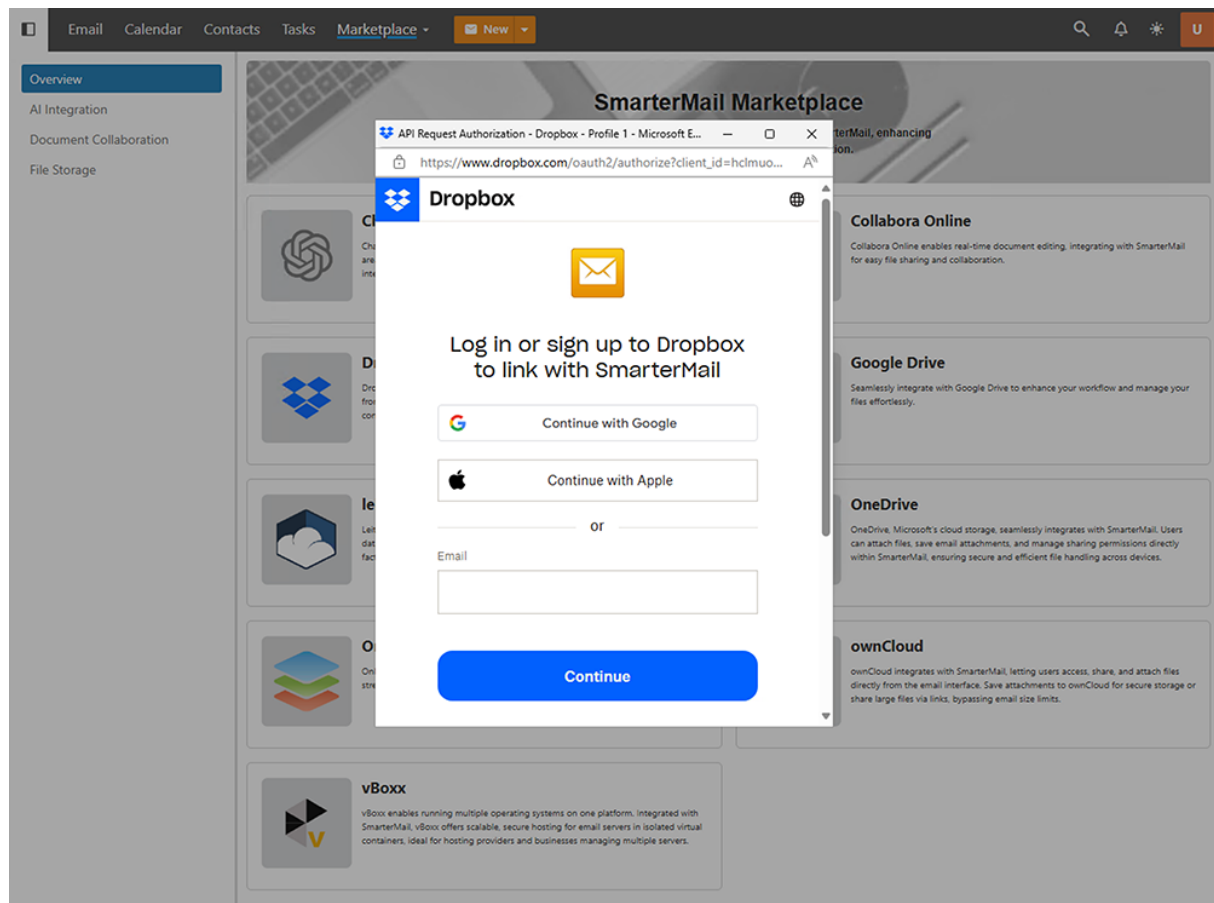
Additional Configuration

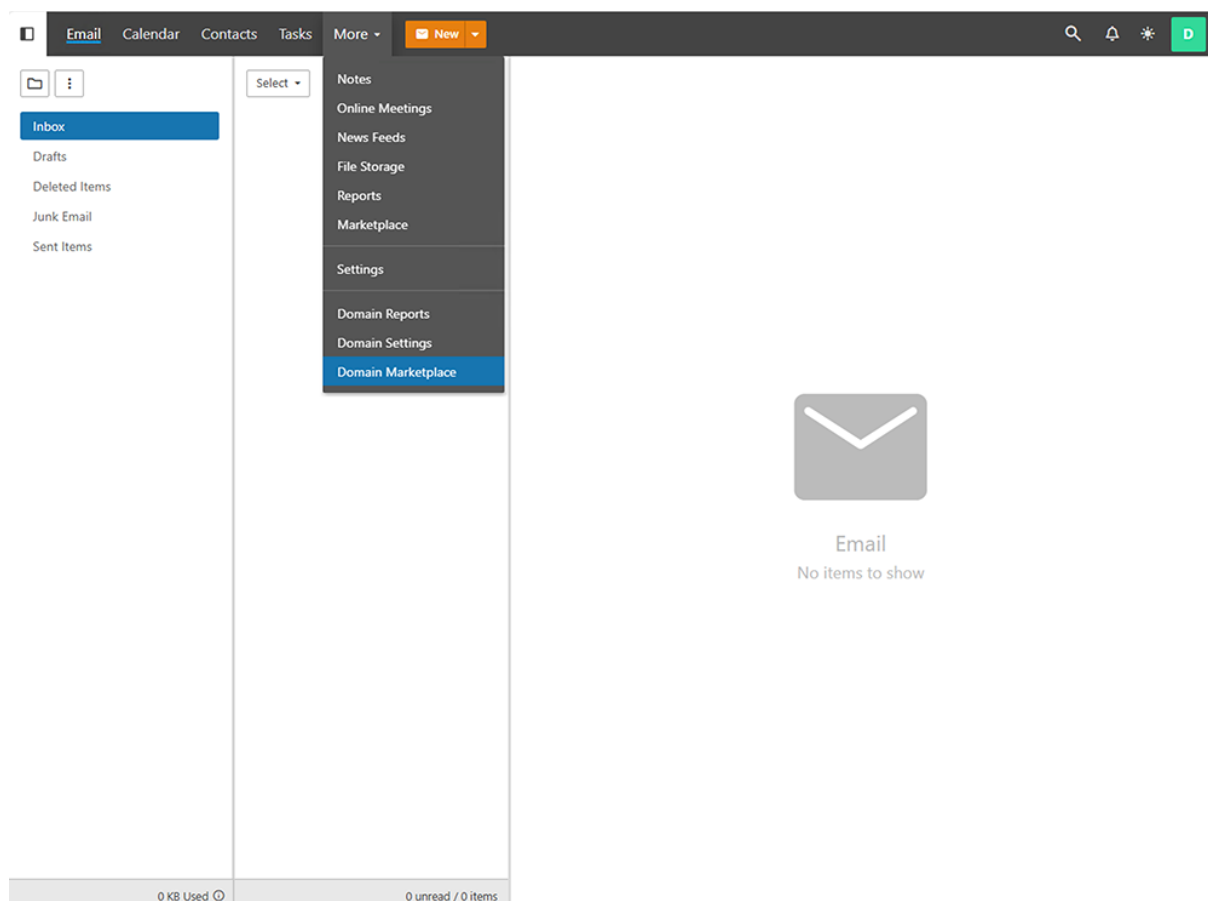For a step-by-step guide on configuring add-ons, refer to the following help topics:

- Composing an Email with AI Assistance

- Proofread an Email with AI Assistance

- Translate an Email with AI Assistance

- Modify the tone of an Email with AI Assistance

- Configuring RocketChat

- Connecting to Google Drive

- Connecting to Dropbox

- Connecting to OneDrive

- Connecting to ownCloud

- SmarterMail File Storage

- Using OnlyOffice

- Using Collabora

Marketplace Help for Domain Administrators

Getting Started with Marketplace

Domain Administrators can have limited administrative functions, if granted by the System Administrator . These functions enables Domain Administrators to manage and configure add-ons within the Marketplace. This includes tasks such as setting server addresses for cloud connectivity add-ons. The following steps outline how Domain Administrators can enable add-ons available in the Marketplace. For Domain Administrators: System Administrators have full control over enabling add-ons and can choose to retain permissions at their level. If a System Administrator does not enable any Marketplace add-ons, those add-ons will not be visible to Domain Administrators or users.

> • Accessing the Marketplace: Log into your SmarterMail account as the Domain Administrator and navigate to the More tab, then click on the Domain Marketplace link.
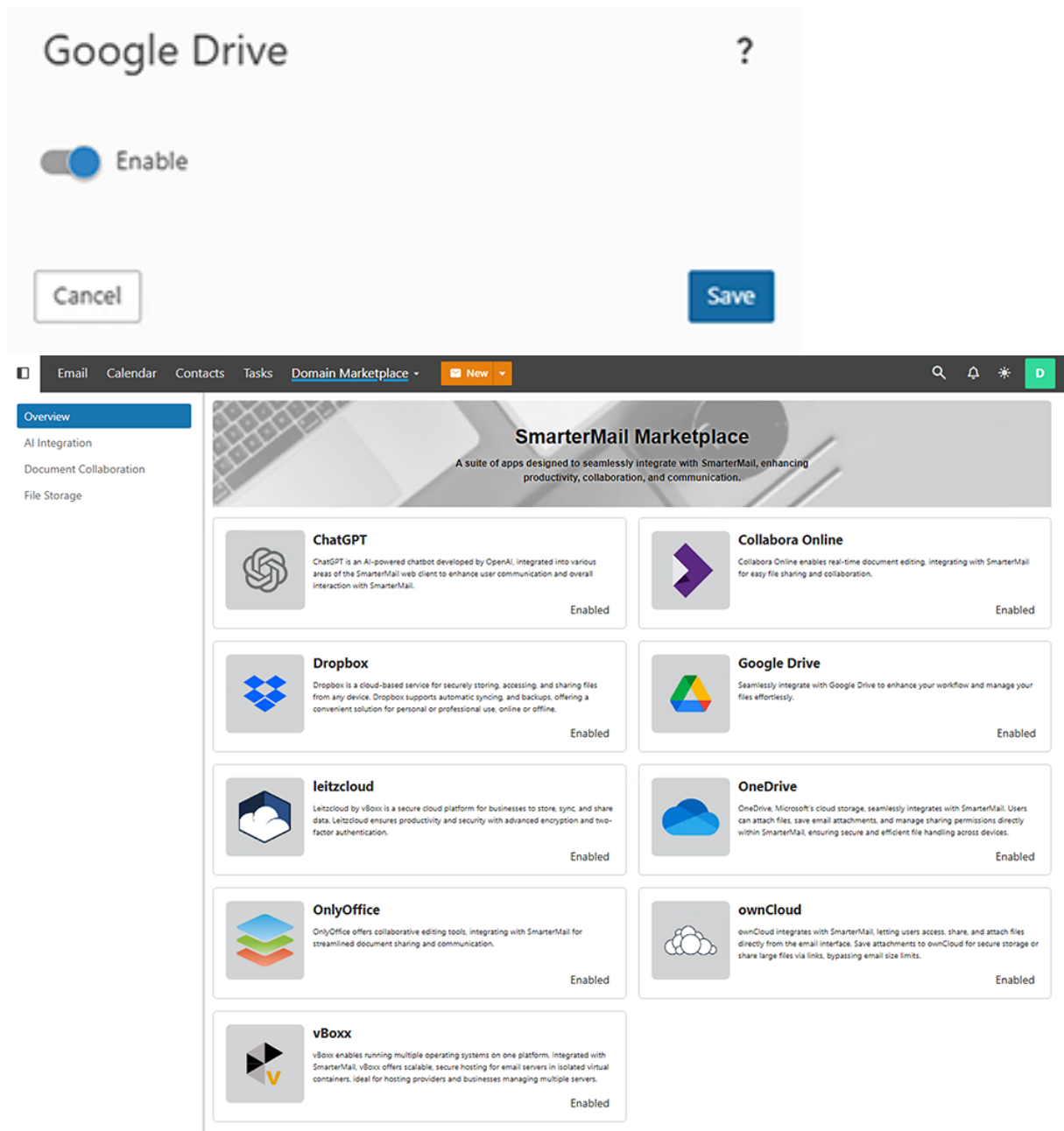

• Browse Available Add-ons: Explore the available options, filtering by functionality, such as AI Integration, Document Collaboration, Chat or File Storage ..

• Select and Enable: By default, most available add-ons are Disabled . To enable an add-on, click on its card and toggle the switch from Disabled to Enabled , then click Save . Repeat this process for any additional add-ons you wish to enable and follow the on-screen prompts. Some add-ons may require additional configuration, such as entering server addresses or logging in with system administrator credentials.• After enabling add-ons, the Marketplace will indicate which add-ons are active by displaying the status as Enabled . Enabled add-ons will display the features available at the user level, along with any personal configurations related to cloud connectivity services or add-ons.

Additional Configuration

For a step-by-step guide on configuring add-ons, refer to the following help topics:

- Configuring ChatGPT
- Configuring eM Client
- Enabling RocketChat
- Configuring RocketChat
- Connecting to Google Drive
- Connecting to Dropbox
- Connecting to OneDrive

- Connecting to ownCloud

- Connecting to Leitzcloud/vBoxx

- Configuring OnlyOffice

- Configuring Collabora

Marketplace Help for System Administrators

Getting Started with Marketplace

The System Administrator can log in to a domain and manage settings as a domain admin. However, the overall Marketplace is managed by the System Administrator within Domain Defaults, where they control the features available to domain admins. In SmarterMail, the System Administrator login is different from user and domain administrator logins. Unlike standard user accounts, System Administrators do not have mail folders, calendars, or other email-related features. Their primary role is to manage the SmarterMail installation, including adding domains, configuring anti-spam and anti-virus settings, setting up gateways, overseeing server operations, and managing the Marketplace. System Administrators also have top-tier administrative functions, allowing them to configure and manage add-ons within the SmarterMail Marketplace. This includes setting server addresses for cloud connectivity add-ons and granting system administrator permissions.

Below are the steps to enable Marketplace add-ons:

- Accessing Marketplace Dashboard: Log into your SmarterMail account as the System Administrator and and go to the specific domain you wish to manage.

- In the Options tab, scroll down to the Marketplace card. Most add-ons are disabled by default. As the system administrator, can enable any add-on you choose. Simply toggle the desired add-on and click Save at the top of the page.
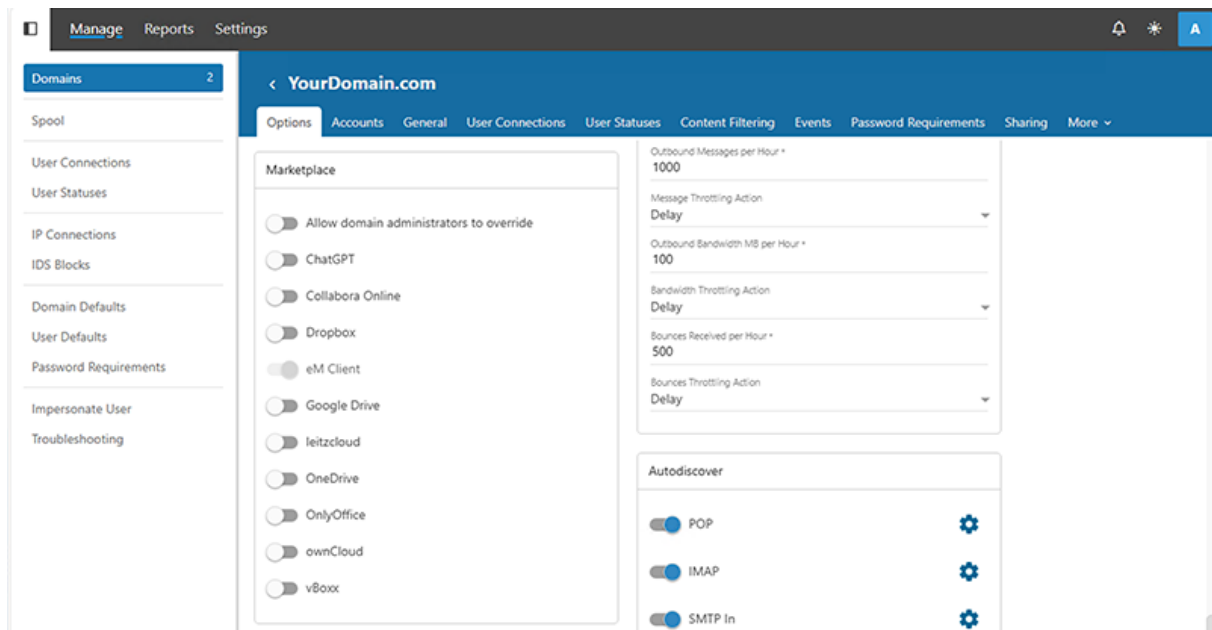
note: Enabling Allow Domain Administrators to Override grants domain administrators the ability to bypass system admin controls. This includes enabling specific add-ons and configuring technical settings such as server addresses, tokens, and APIs.

• This screen below will show that the add-ons are disabled from the user's perspective.
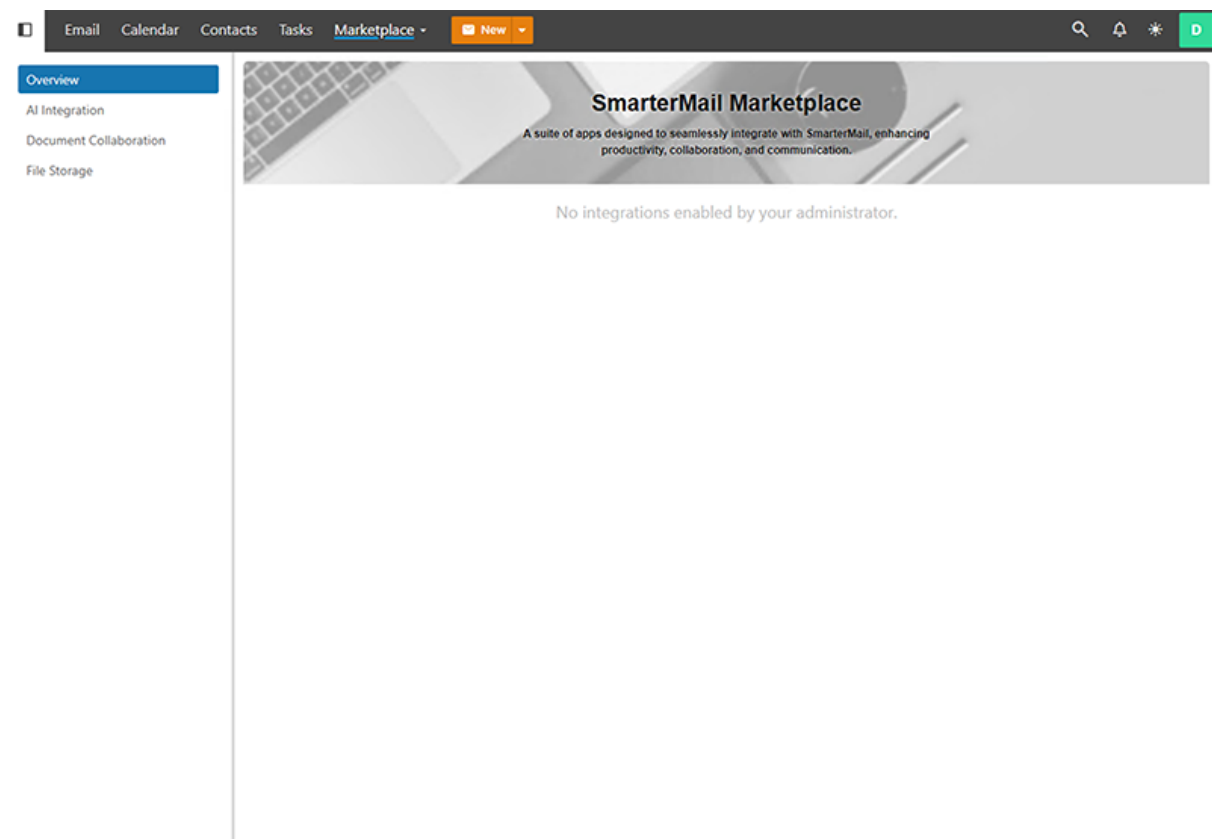
• As a System Administrator, you have full control over enabling add-ons for your organization. Simply toggle the desired add-ons to activate them and leave the others disabled. This ensures that only the necessary add-ons are in use. The screen below displays what users will see on their end.
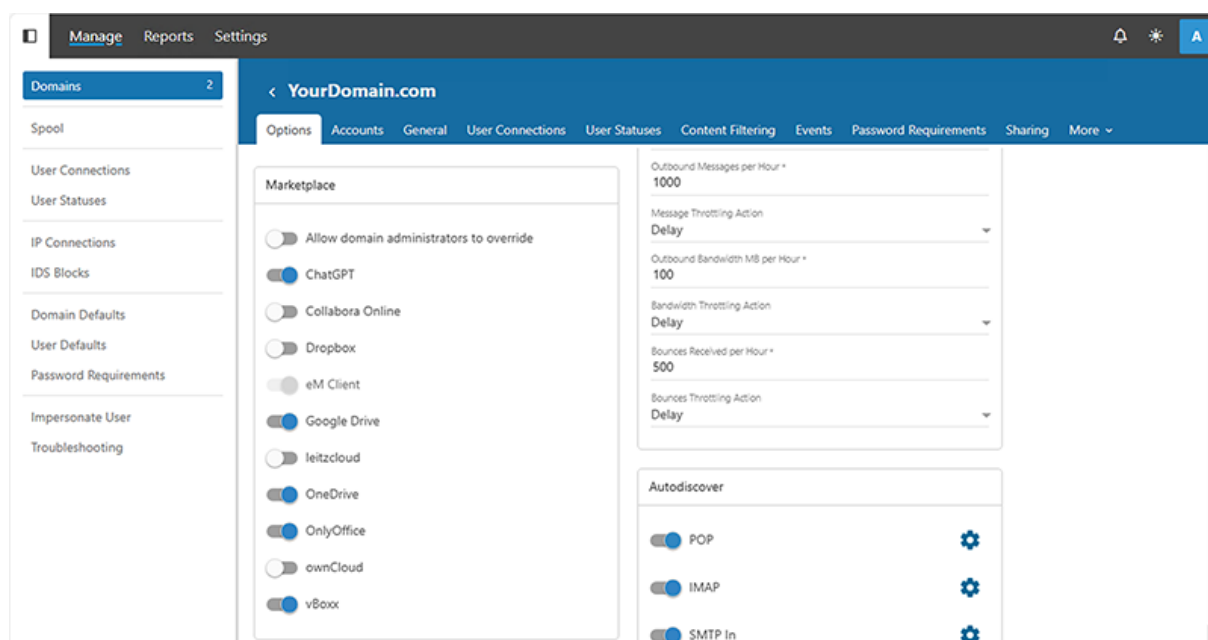
• After enabling add-ons, the Marketplace will indicate which add-ons are active by displaying the status as Enabled . Enabled add-ons will display the features available at the user level, along with any personal configurations related to cloud connectivity services or add-ons. This screen displays what users will see on their end.
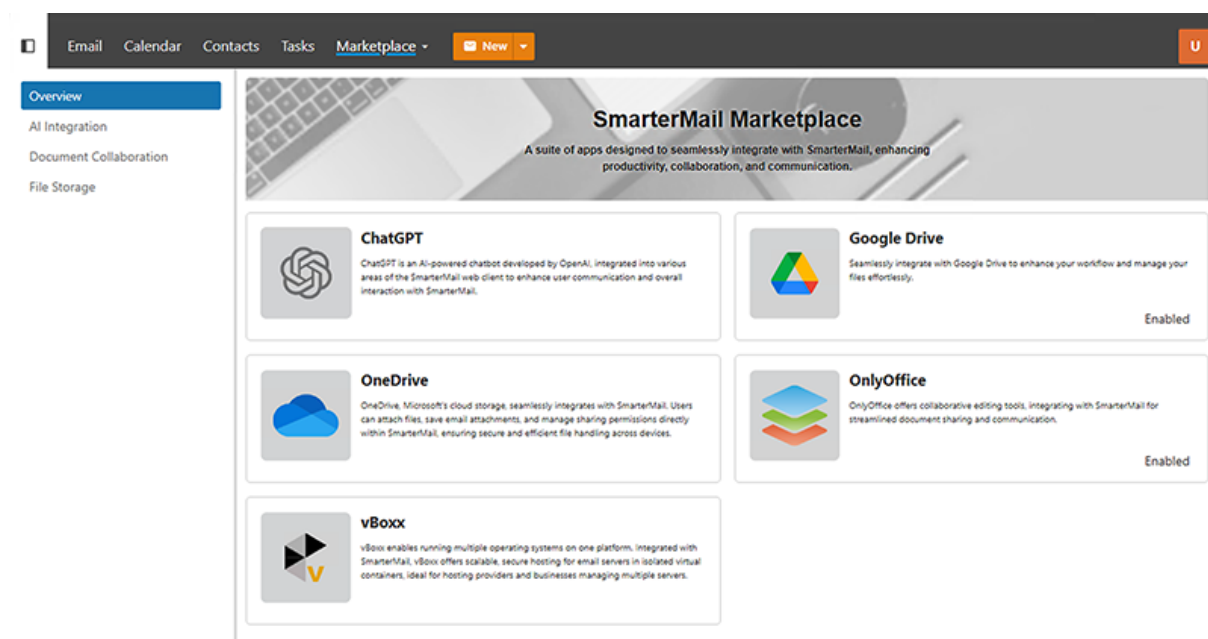
Marketplace Integrations

AI Integrations

AI Integration Overview

The integration of Artificial Intelligence (AI) into SmarterMail's Marketplace is designed to enhance the overall user experience by introducing an intelligent Assistance for email communication. By leveraging AI-driven features, SmarterMail Users, Domain Administrators, and System Administrators can streamline email management, automate routine tasks, and improve overall productivity. AI-powered tools can assist with creating emails, creating invites, newsletters, and announcements. This new feature creates a more intuitive and efficient workflow, reducing manual effort and increasing responsiveness. As AI continues to evolve, SmarterMail remains committed to providing innovative solutions that empower users to work smarter and more effectively.

Purpose

The primary goal of AI integration in SmarterMail is to optimize email workflows, making communication more seamless and efficient. By reducing the time and effort required for drafting and responding to emails, AI enhances user productivity while maintaining a professional and polished correspondence style.

Benefits

- Improved Efficiency: AI-assisted email drafting reduces the time spent on composing messages.
- Enhanced Communication: Smart suggestions help users craft clear, concise, and well-structured emails.
- Streamlined Workflow: AI-driven follow-up recommendations ensure timely responses and better task management.
- Increased Productivity: Automated Assistance minimizes repetitive tasks, allowing users to focus on more critical responsibilities.

This AI-powered enhancement within SmarterMail's Marketplace represents a significant step toward smarter, more intuitive email communication.

Available Integrations

- Configuring OpenAI

OpenAI

Marketplace effortlessly connects with OpenAI's ChatGPT to help users improve their overall communication. By using AI-powered automation, Marketplace users can tap into ChatGPT's capabilities for crafting email responses, add descriptions to calendar invitations, generating content for tasks, and more. The integration not only saves time and reduces workload but also ensures that email communications are polished and professional.

The integration of ChatGPT is generally managed by the domain administrator. They are responsible for selecting the AI model to use, setting up the OpenAI API Key, and setting the number of max requests per day for users. However, domain administrators can allow users to override the domain settings so user can generate and use their own OpenAI API keys. When is is allowed, when the user clicks on the ChatGPT card in the Marketplace, they'll see existing settings, but can add their own information, select their own AI Model, and more.

Jump To:

- Configuring ChatGPT
- ChatGPT API Key

Configuring ChatGPT

Configuring ChatGPT is a simple process. First, ensure that ChatGPT is enabled by clicking on the ChatGPT card. A modal box will appear, where you'll need to enter your OpenAI API key and set a daily request limit.

Note: If a domain administrator selects Enable for "Allow users to use their own API key" this allows any user to input and use their own API key if they have one available.

ChatGPT API Key

Don't have an API key? Follow the steps below to obtain one from OpenAI.

- Sign Up or Log In to OpenAI

- Visit the OpenAI website.

- If you already have an account, simply click Log In and enter your credentials.

• Click on Sign Up if you don't have an account and complete the registration process.

• Set Up a Billing Plan

• Once logged in, navigate to the Billing section of the OpenAI dashboard.

• Add a valid payment method. OpenAI typically provides a free trial credit for new users, but for extended usage, a paid plan is required.

• Choose a pricing plan that suits your usage.

• Generate an API Key

• Go to the API Keys page.

• Click Create new secret key .

• Assign a name to your API key (optional but helpful for identification).

• Copy and save the API key immediately after generation. Store it securely .

• Secure Your API Key

• Never share your API key publicly.

• Rotate or revoke keys if you suspect unauthorized access.

• Manage Your API Key

• You can view, revoke, or regenerate API keys from the API Keys page .

• For multiple projects, generate different keys for better management and control.

Document Collaboration

Document Collaboration Overview

Marketplace makes teamwork effortless by offering powerful collaboration features for team members, customers, and partners. With a fully integrated office suite, you can view, edit, and collaborate on documents, spreadsheets, and presentations, all in one place. Thanks to seamless integration with SmarterMail's File Storage, you can work on existing files or create new ones while keeping everything securely stored within the platform. Plus, with support for OnlyOffice and Collabora, you get a flexible, efficient workflow that makes working together easier than ever.

Purpose

Document Collaboration is all about boosting productivity by making it easy to edit and work on documents in real-time—no extra downloads or third-party file transfers needed! Since it's built right into File Storage, SmarterMail users can keep everything in one place, making teamwork smoother and more organized. Whether you're updating a report, brainstorming ideas, or reviewing files with your team, this feature keeps collaboration seamless, accessible, and hassle-free.

Benefits

- Real-Time Collaboration: Multiple users can simultaneously edit and update documents, spreadsheets, and presentations.
- Seamless Integration: Files stored in SmarterMail's File Storage can be opened, edited, and saved directly within the platform.
- Automatic File Management: Newly created or modified files are automatically saved in File Storage for easy retrieval.
- Flexible Compatibility: Works with third-party office suites like OnlyOffice and Collabora, allowing users to choose their preferred editing tools.
- Enhanced Productivity: Eliminates the need for downloading and re-uploading files, ensuring an efficient and organized workflow.

With Document Collaboration Storage, SmarterMail users can work smarter, keep files secure, and collaborate effortlessly, all within a fully integrated system.

Available Integrations

- OnlyOffice
- Collabora

OnlyOffice

OnlyOffice is a complete office suite that gives users the ability to view, edit, and collaborate on documents, spreadsheets, and presentation decks. When enabled, SmarterMail users can use their own (or their organization's) installation of OnlyOffice to edit files currently stored in File Storage, or even create new files and have them stored automatically in their File Storage area. They can also use OnlyOffice to view attachments, based on the supported file types. (E.g., .txt, .docx, .xls, etc.)

OnlyOffice

Server Address *
https://onlyoffice.smartertools.com

Max Connections (0 = Unlimited) *
20

Max Connections for Each User (0 = Unlimited) *
2

In order to set up OnlyOffice for a domain, you will need to Enable OnlyOffice Integration for the domain, then configure the following:

- OnlyOffice Server URL - This is the full URL to the OnlyOffice server. It can be a FQDN (e.g., onlyoffice.some-domain.com) or an IP address.
- Max Connections (0 = Unlimited) - This is the maximum number of connections the domain can make to the specified OnlyOffice server. Note: The number of max connections to a single OnlyOffice server can vary by license.
- Max Connections for Each User (0 = Unlimited - This is the maximum number of connections a single user can make to the specified OnlyOffice server. As such, it works in conjunction with the Max Connections setting.

OnlyOffice Tips

- If the customer has OnlyOffice running on a different domain than SmarterMail, the x-frame-src header will need to be removed on the OnlyOffice server.
- When working with OnlyOffice Community Server, be sure to include "/ds-vpath" at the end of the OnlyOffice URL. (If NOT using Community Server, this may not be necessary.)

Using OnlyOffice

OnlyOffice is a complete office suite that gives users the ability to view, edit, and collaborate on documents, spreadsheets, and presentation decks. The online version can be integrated with SmarterMail's File Storage area, so SmarterMail users can edit files currently stored in File Storage, or even create new files and have them stored automatically, using their own installation of OnlyOffice.

Note: The integration of an organization's OnlyOffice server is handled, and initiated, at the System Administrator level. If your organization has an OnlyOffice server, but you do not have the option to create or edit files using OnlyOffice, check with your SmarterMail administrator.

Creating New OnlyOffice Files

• Creating a new file using OnlyOffice is extremely simple: just use the New button and select the type of file you want to create.• Once you've made your choice, the New Document modal will open, allowing you to name your file, select (or change) the type of file you want to create, and then select where you want the new file to be stored. Once done, click the Save button and the new file is created.• A new browser tab opens so you can begin editing your new file.Note: Based on OnlyOffice's configuration it's only possible to have a maximum of 20 "sessions" open at one time per OnlyOffice document server.
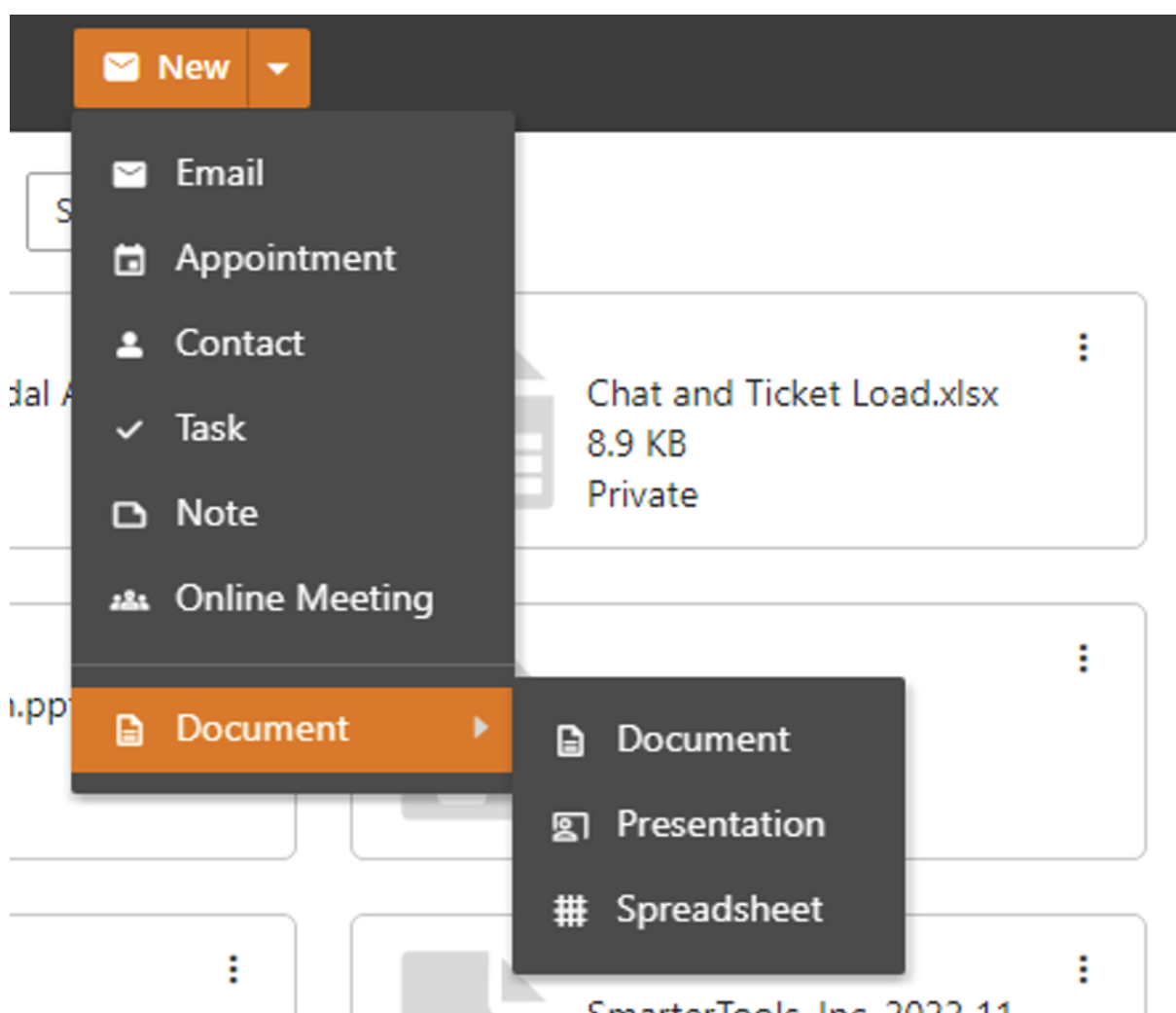
Editing Existing Files
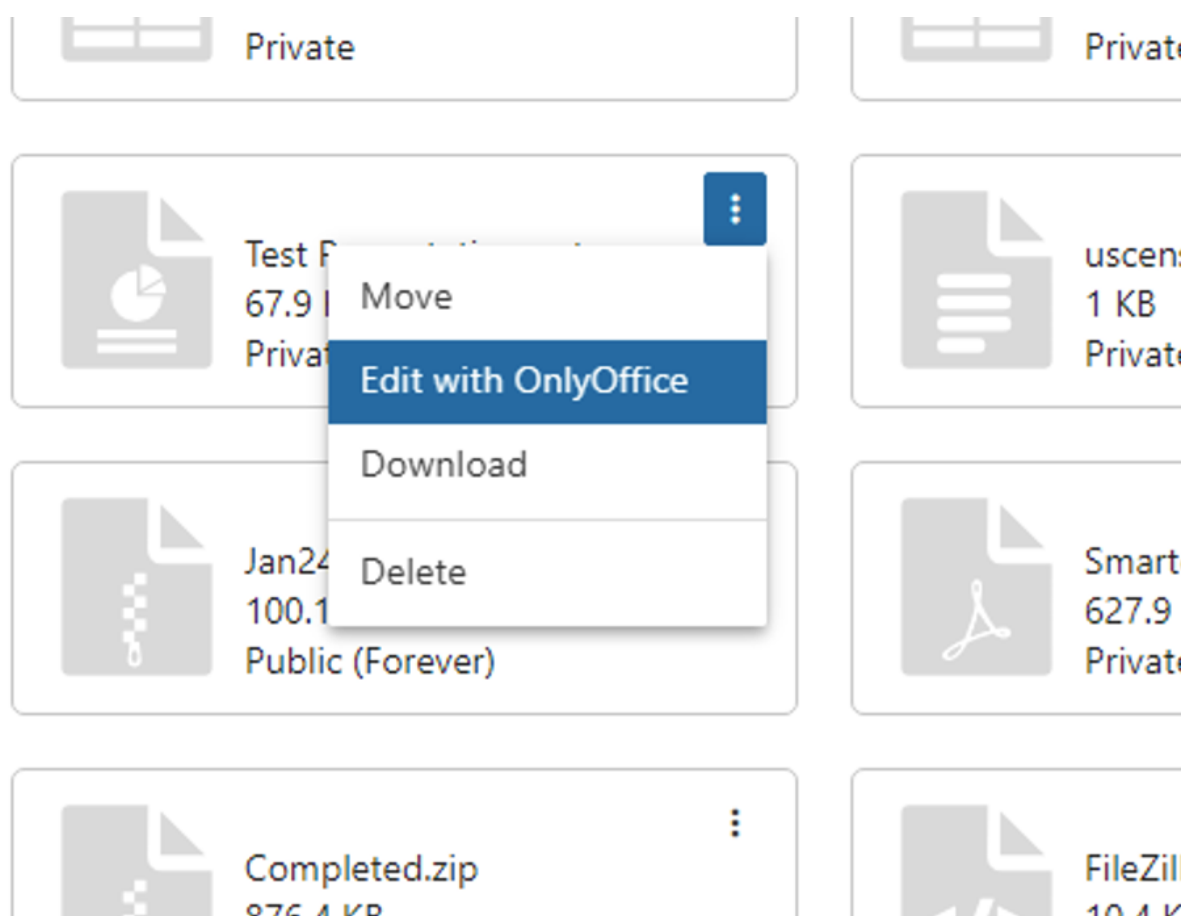
Editing an existing file is just as easy. Simply click the Actions (☐) button on any text file, document, spreadsheet, or presentation, and select Edit with OnlyOffice from the menu options. The OnlyOffice editor will open in a new browser tab, and you can edit to your heart's content.

Worth Noting

There are a few things worth noting regarding the integration of OnlyOffice:

• Depending on licensing, OnlyOffice sessions may be limited. If so, the system administrator will need to know that when setting up the integration. They also have the ability to set the maximum number of sessions any one user can have open at a time.

• OnlyOffice has an automated save and timeout feature that cannot be controlled by SmarterMail. By default, if a file is open in a tab for more than 60 minutes, without any session activity, it will automatically save and the session will time out.

• If SmarterMail goes down when a file is open, the file will appear in File Storage with a warning icon on it. When you open the file, you're presented with some recovery options. (Recover document and overwrite, rename and recover document, Download, or Delete the recovered copy.)

Collabora

Collabora is a complete office suite that allows users to view, edit, and collaborate on documents, spreadsheets, and presentations. When enabled, SmarterMail users can utilize their own or their organization's Collabora installation to edit files stored in File Storage or create new files that are automatically saved in their File Storage area. They can also use Collabora to view attachments, based on the supported file types. (E.g., .txt, .docx, .xls, etc.)

Collabora Online

Server Address *
https://collaboraonline.smartertools.com

Max Connections (0 = Unlimited) *
100

Max Connections for Each User (0 = Unlimited) *
5

In order to set up Collabora for a domain, you will need to Enable Collabora Integration for the domain, then configure the following:

> • Collabora Server URL - This is the full URL to the Collabora server. It can be a FQDN (e.g., collabora.some-domain.com) or an IP address.
> • Max Connections (0 = Unlimited) - This is the maximum number of connections the domain can make to the specified Collabora server.

Note: The number of max connections to a single Collabora server can vary by license.
• Max Connections for Each User (0 = Unlimited - This is the maximum number of connections a single user can make to the specified Collabora server. As such, it works in conjunction with the Max Connections setting.

Collabora Tips

> • If the customer has Collabora running on a different domain than SmarterMail, the x-frame-src header will need to be removed on the Collabora server.

• When working with Collabora Community Server, be sure to include "/ds-vpath" at the end of the Collabora URL. (If NOT using Community Server, this may not be necessary.)

## Using Collabora

Collabora is a complete office suite that gives users the ability to view, edit, and collaborate on documents, spreadsheets, and presentation decks. The online version can be integrated with SmarterMail's File Storage area, so SmarterMail users can edit files currently stored in File Storage, or even create new files and have them stored automatically, using their own installation of Collabora Online. Note: The integration of an organization's Collabora server is handled, and initiated, at the System Administrator level. If your organization has an Collabora server, but you do not have the option to create or edit files using Collabora Online, check with your SmarterMail administrator.

Creating New Collabora Files

Creating a new file using Collabora is extremely simple: just use the New button and select the type of file you want to create:
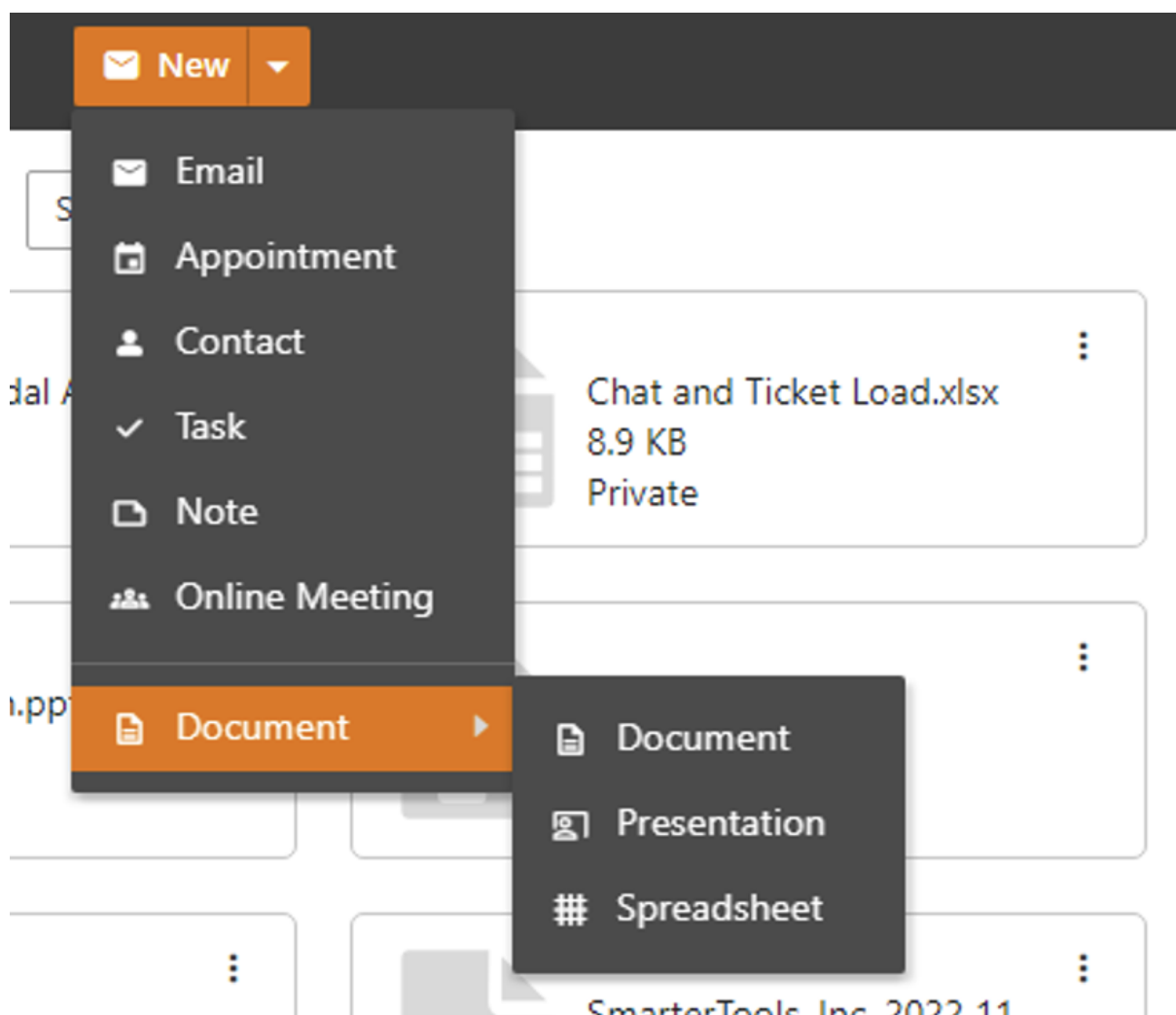
Once you've made your choice, the New Document modal will open, allowing you to name your file, select (or change) the type of file you want to create, and then select where you want the new file to be stored. Once done, click the Save button and the new file is created, and a new browser tab opens so you can begin editing your new file. Note: Based on Collabora's configuration it's only possible to have a maximum of 20 "sessions" open at one time per Collabora document server.

Editing Existing Files

Editing an existing file is just as easy. Simply click the Actions (□) button on any text file, document, spreadsheet, or presentation, and select Edit with Collabora Online from the menu options. The Collabora editor will open in a new browser tab, and you can edit to your heart's content.

Worth Noting

There are a few things worth noting regarding the integration of Collabora:

- Depending on licensing, Collabora Online sessions may be limited. If so, the system administrator will need to know that when setting up the integration. They also have the ability to set the maximum number of sessions any one user can have open at a time.
- Collabora has an automated save and timeout feature that cannot be controlled by SmarterMail. By default, if a file is open in a tab for more than 60 minutes, without any session activity, it will automatically save and the session will time out.
- If SmarterMail goes down when a file is open, the file will appear in File Storage with a warning icon on it. When you open the file, you're presented with some recovery options. (Recover document and overwrite, rename and recover document, Download, or Delete the recovered copy.)

Live Chat

Live Chat Overview

This feature is only available in SmarterMail Enterprise.

SmarterMail's live chat integrations make instant, secure communication easy for users within the same domain, right from the webmail interface. Whether on desktop or mobile, many live chat providers include support for popular clients such as Adium, IM+, and other XMPP-based apps. In addition, many have their own clients available. SmarterMail has built-in text, voice, and video chat, teams can collaborate in real-time. SmarterMail's XMPP/Jabber server ensures seamless messaging for individuals or small groups, whether through webmail or an instant messaging app. Additional features include file sharing, automatic archiving, and downloadable chat history, keeping conversations accessible and organized.

Purpose

The purpose of live chat is to offer a fast and efficient alternative to email for instant communication. While email remains a vital tool for professional correspondence, live chat enables immediate interaction, making it ideal for quick discussions, problem-solving, and collaboration.

Benefits

• Instant Communication: Users within the same domain can chat in real-time, reducing response times and improving productivity.

• Multi-Platform Support: Many work with desktop and mobile chat clients, particularly those that support XMPP.

• Seamless Presence Syncing: User statuses (Online, Offline, Away) can synchronize across third-party clients and the webmail interface.

• Enhanced Collaboration: Many offer text, voice, and video chat options, with the ability to generate shareable video chat links.

• Customizable Experience: Users can personalize their text chat experience within the webmail interface.

Available Integrations

• SmarterMail Chat
• RocketChat

RocketChat

RocketChat is a powerful team communication platform that enables real-time messaging, file sharing, and seamless integrations. By integrating with SmarterMail, users can receive email notifications, alerts, and messages directly within RocketChat channels, streamlining communication and enhancing collaboration. This integration ensures users stay informed without constantly switching between platforms.

Configuring RocketChat

This section is for users who will be using RocketChat in SmarterMail. Follow these steps to properly configure RocketChat in SmarterMail.

• Log into your RocketChat Workspace . For most domains, the URL is http://rocketchat.yourdomain.com . Use the credentials provided by your System Administrator or Domain Administrator .
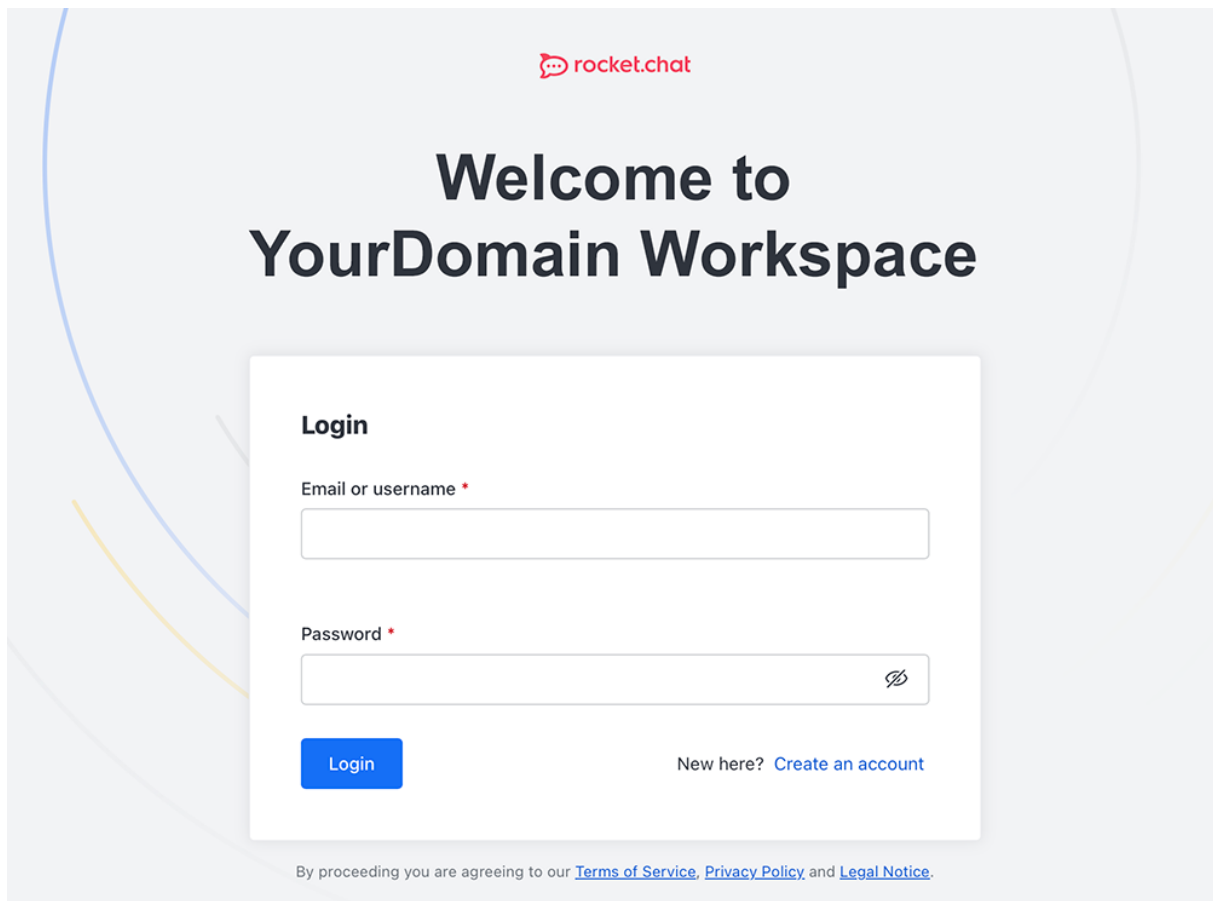
• If Two-Factor Authentication (2FA) is enabled, you will receive a 6-digit verification code via email. Enter the code and click Verify .

Here is your authentication code:

000-000

Do not provide this code to anyone.

If you didn't try to login in your account please ignore this email.

Blog | **Github** | **Facebook** | **Instagram**

© Rocket.Chat Technologies Corp.

Made with ❤️ in 🇧🇷 🇨🇦 🇩🇪 🇮🇳 🇬🇧 🇺🇸

Email two-factor authentication

Enter authentication code

✕

Enter the code we just emailed you.

000-000

Resend email

Cancel   Verify

• In your RocketChat Workspace , click on your user profile/avatar in the top-right corner, then click Preferences . Navigate to Personal Access Token in the left-hand menu.

Account ✕

👤 Profile

🎚 Preferences

🔒 Security

</> Integrations

🔑 Personal Access Tokens
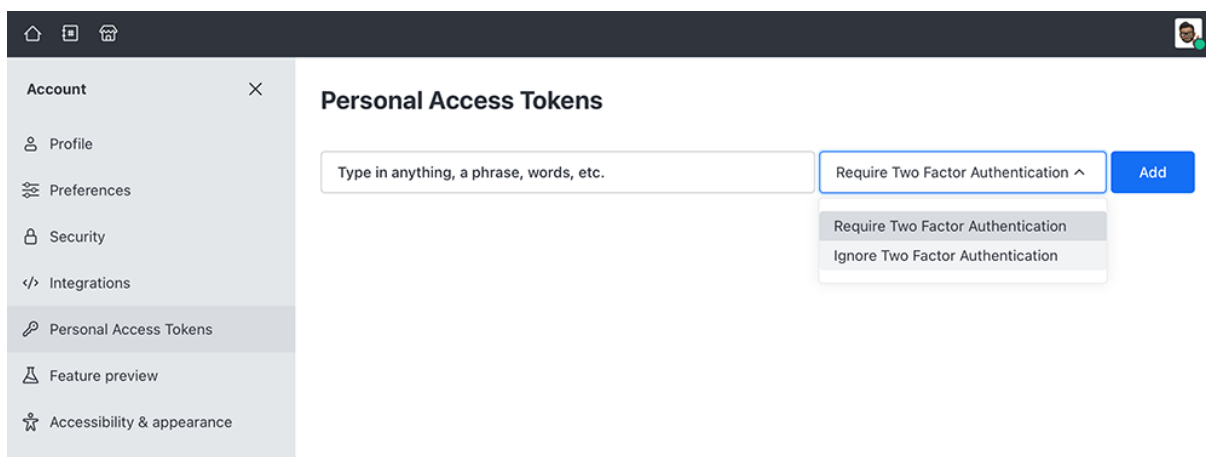
⚗ Feature preview

🧍 Accessibility & appearance
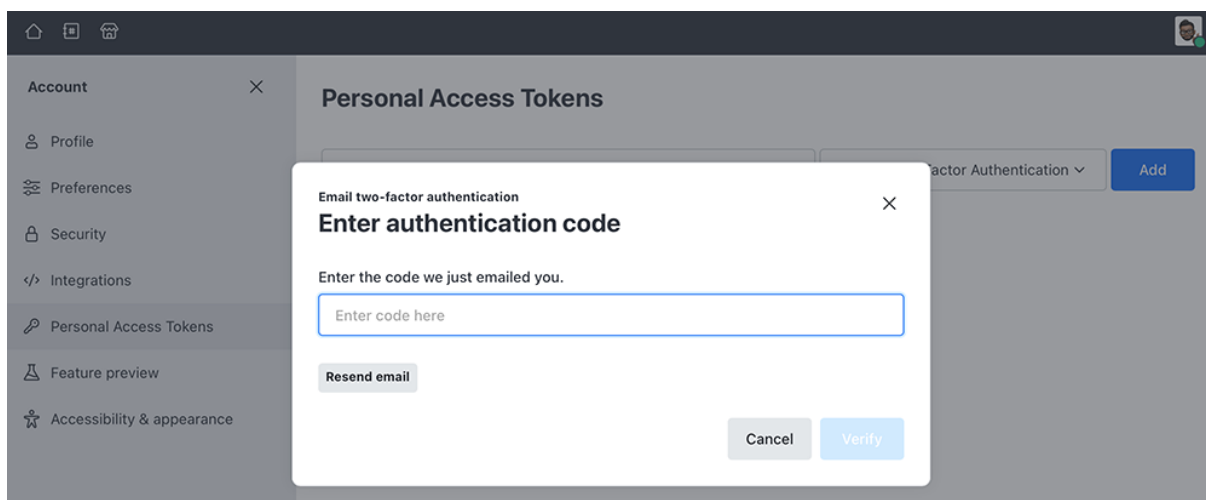
• To create or add a Personal Access Token , provide a name or phrase for it to enhance security and confirm the user's identity. Click Add , then enter your RocketChat password when prompted. (Optional: You may enable or ignore Two-Factor Authentication.)

• RocketChat will email you an authentication code. Enter that code.

• Click Verify to generate your Personal Access Token . note: Save the token details securely. Your Personal Access Token will not be shown again.
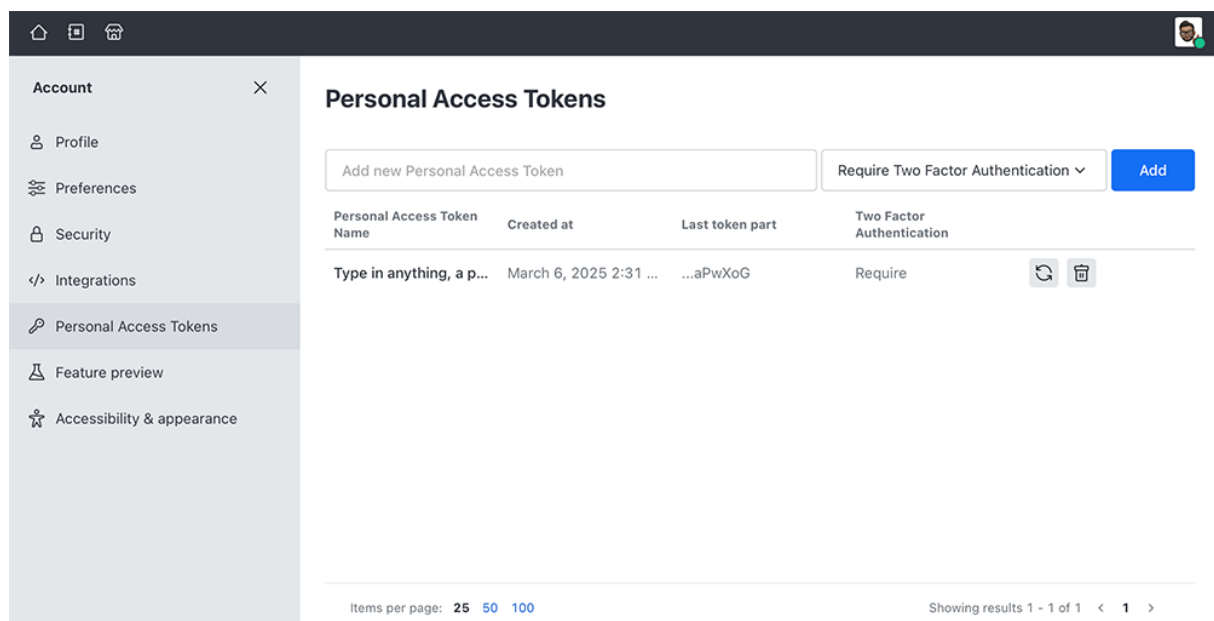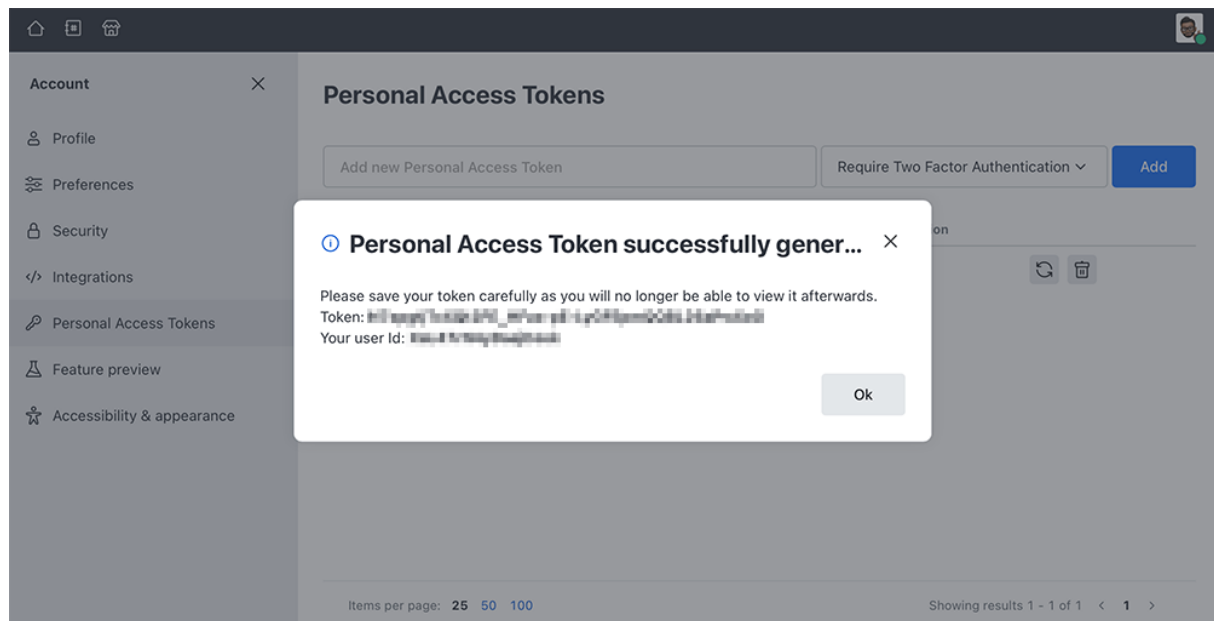
• Log into the Marketplace settings for your account.

• Find the RocketChat card in the list of available integrations.

• Toggle Enable and enter the following details: RocketChat Server URL, RocketChat User ID, Personal Access Token . Click Test Connection to verify the setup, then click Save to finalize the integration.

If you are unsure of your RocketChat Server URL, most organizations use
https://rocketchat.yourdomain.com . Contact your System Administrator or Domain Administrator if
needed.

When you receive a new chat, a red notification box will appear in the lower right corner of your
browser. Clicking on the message will open RocketChat in a new tab.

Enabling RocketChat (for Domain Administrators)

This section is for Domain Administrators only. Follow these steps to enable RocketChat in the
Marketplace and configure it for your domain.

• Log into the Marketplace settings for your domain.

• Locate the RocketChat card in the list of available integrations. Enable RocketChat by toggling it on. note: Domain Administrators can Enable RocketChat if the System Administrator has enabled the Allow Domain Administrators to Override and included RocketChat as an option. In this case, Domain Administrators can turn it on or off for their domain. However, if the override is disabled, only the System Administrator can manage RocketChat settings.
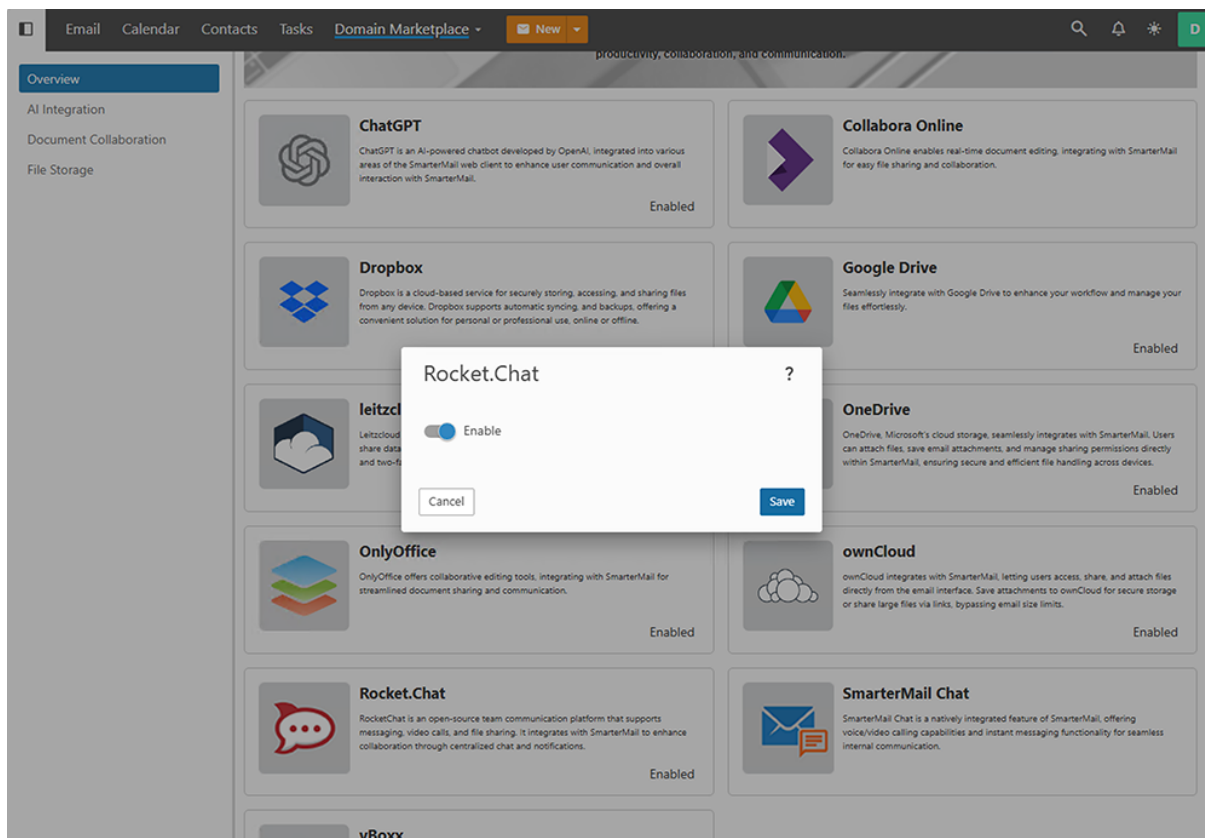
• Your Domain Administrator or System Administrator should have sent you your user credentials and key from RocketChat's servers via email.

• When you receive a new chat, a red notification box will appear in the lower right corner of your browser. Clicking on the message will open RocketChat in a new tab.

Enabling RocketChat (for System Administrators)

This section is for System Administrators only. Follow these steps to enable RocketChat in the Marketplace and configure it for your domain.

• Log into the Marketplace settings for your domain.

• Locate the RocketChat card in the list of available integrations. Enable RocketChat by toggling it on.
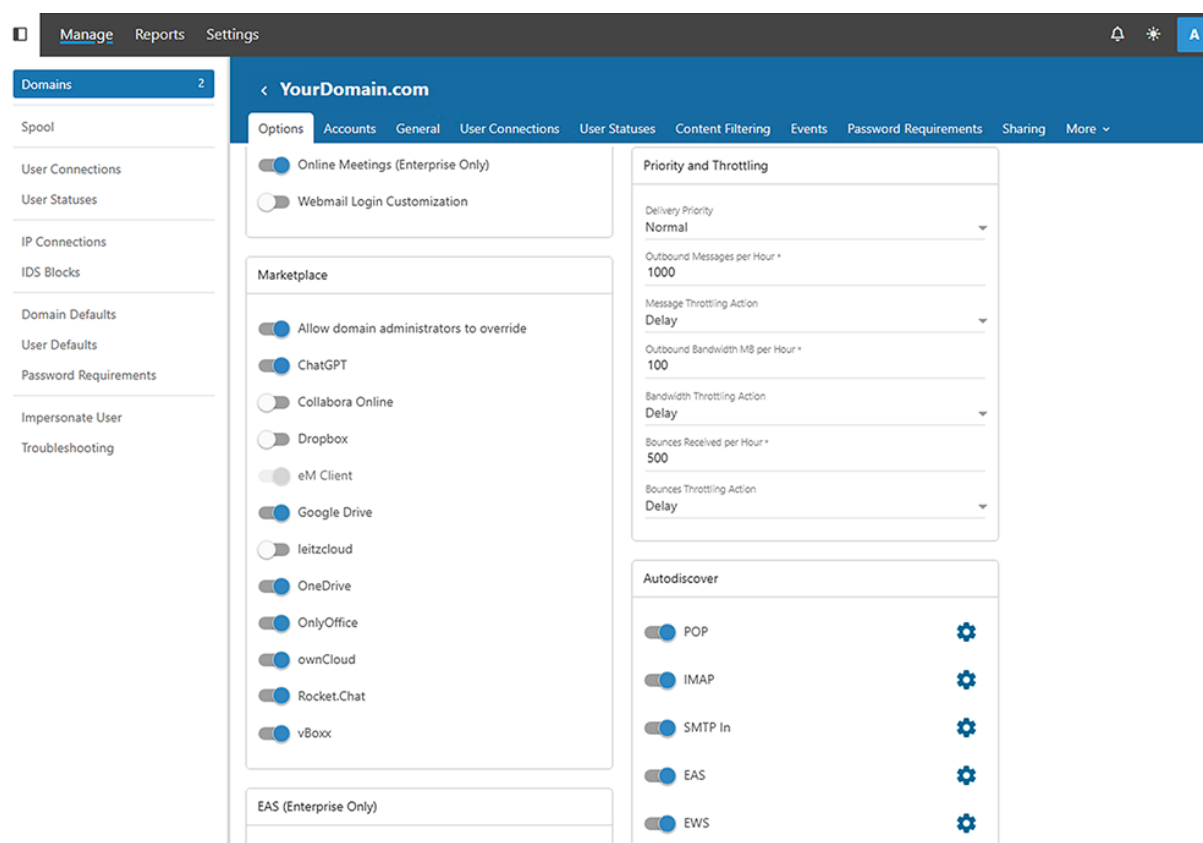
SmarterMail Chat

This feature is only available in SmarterMail Enterprise.

SmarterMail's Chat feature offers a seamless and secure way to stay connected with colleagues and teams. Powered by a strong XMPP/Jabber server, it supports voice, video, and text chat, making it an ideal solution for both individual and group conversations. Chat can be accessed directly from the webmail client or through your favorite instant messaging apps on desktop and mobile, such as Adium, IM+, and other XMPP-compatible clients.

Key Features:

- Voice, video, and text chat for real-time communication.
- Support for desktop and mobile clients for flexibility on the go.
- File sharing with previews for effortless collaboration.
- Immediate archiving to keep conversations secure and organized.
- Downloadable chat history for easy reference. Note: In order to use chat, your SmarterMail installation MUST be secured with an SSL certificate. This is because the audio, video and live chat connections require HTTPs connections in order to work properly and securely.

Jump to:

- Navigating Chat
- Starting an Audio or Video Chat
- Sharing Files and Links
- Connecting to Third-Party Chat Clients
- Searching Chat

Navigating Chat

Layout

The Chat icon is in the top, right corner of the web interface. When a new chat is received, the icon will display an unread flag.
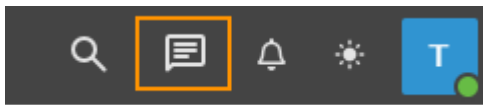
Clicking on the icon will pop out the chat window, allowing you to respond to the chat request or start your own.

The chat window is divided into two main areas:

- The Chat Users/Aliases view. This area displays the contacts on your domain. If aliases are set up so that multiple people can chat at the same time, those show at the top of the view with individual users showing below, separated by a horizontal line. A user's status is also displayed. (The status for an alias is not displayed because aliases contain multiple individuals, so tracking the status of an alias won't work since each individual in the alias can have a different status.)
- The Actual Chat Area. This is where your text chat occurs. Previous conversations are listed, in order, beginning with the most recent session you've had with that user. The 75 most recent lines are displayed OR the chats you've had with that user in the last 30 days are displayed, if the total lines don't add up to 75. Scrolling up in this area will display older threads.

Chat With... - This area allows you to type in the username of an individual. The Chat With area is especially helpful in cases where a domain has a large number of users. Typing in a username allows you to find the person you want to chat, quickly and easily, versus having to scroll through a large list of users.

Modifying Your Status

In order to set your chat status you'll need to right-click on your user avatar, then select your status from the dropdown menu.

As for the status definitions:

• Available - You are available to receive and respond to chats via the webmail interface. When a user is marked as Available, they will see other members of their domain who are also active and available.

• Away - You are logged in but are away from your computer and may not respond right away.

• Do Not Disturb - You are logged in, but busy. Therefore, you're not available at the moment and may not respond for an extended period of time.

• Offline - When this setting is checked, any user that is offline will appear in the users list, but the username and availability will be greyed out. Deselecting this will hide all offline users from the list.

Starting an Audio or Video Chat

Put simply, to start a chat with an individual, or people within an alias, simply click on the name and start typing.

SmarterMail's chat includes real-time audio and video chat for user-to-user interaction. To start either an audio or video chat with another user, use the Actions (□) button and choose the type of chat you want to start, and that call will be started with the user. The video window will overlay on top of the group chat window.

Sharing Files and Links

To share a file, you can simply drag files into the chat area or use Actions (□) button and select "Upload to Chat". Alternatively, you can use the paperclip icon under the text box to upload files.

Depending on the file type, when a file is shared a thumbnail will display for image files such as .JPG and .PNG file types and/or a link to the file is displayed. When someone clicks on the thumbnail or link, a preview of the file will be displayed in a new browser window so that the recipient can look at the file before they download it. Shared links can just be pasted in the live chat box and links open in a new window.

Interacting with Individuals or Aliases

When chatting with users or aliases, there are a few different actions that are available to you.

When chatting a user, if you click on their username in the chat window, you have the following options:

• Send Email - Selecting this action opens a new Compose window, allowing you to email that user.

• Invite to Appointment - Selecting this action opens a New Appointment window, allowing you

to create an invitation that can be sent to the user, and anyone else, for an appointment, meeting, etc.

When chatting with an alias, if you click the aliasn name, you also have a few different options:

• View Members - Selecting this opens a modal that displays the usernames and addresses of every user included in the alias. You can then click on any user and you have the ability to send an email to them.

• Send Email - Selecting this action opens a new Compose window, allowing you to email the alias directly.

Connecting to Third-Party Chat Clients

This feature is only available in SmarterMail Enterprise.

If you prefer to use a third-party client to receive and respond to chats, you will need to ensure the client you choose supports the XMPP (or Jabber) protocol. Examples of clients that support XMPP include Adium, Digsby, iChat, Pandion, Pidgin and Trillian. However, there are a number of others.

More information on integrating SmarterMail's chat with commonly used third-party clients may be found in the SmarterTools Knowledge Base . Note: In order to use chat your SmarterMail installation must be secured with an SSL certificate. This is because the audio, video and live chat connections require HTTPs connections in order to work properly and securely.

Searching Chat

This feature is only available in SmarterMail Enterprise.

On occasion, you may need to refer to a previous text conversation you had with a contact. One of the best things about SmarterMail is that it indexes all communication, so all of your chats are stored and, therefore, retrievable, so your information is never too far away.

Search Methods

There are 2 ways to search chats:

• Using downloaded transcripts, or
• Using Message Archive search.

User Downloaded Transcripts

Users are able to download a text file that is the history of all of the chats exchanged with a particular user or group. A zipped version of that file (it's compressed because that text file can be quite large) to your local machine where it can be opened in a text editor. Using the search feature of that text editor

allows you to find the search phrases you're looking for as well as the entire threads where those search phrases were discussed.

<u>**Chat Search**</u>

Domain administrators have the ability to search chats for all users. The only requirement is the User name you want to find. The display Name and Text you want to search are optional. It's worth noting, however, that if a User is deleted from SmarterMail, so is their chat history.

Online Meetings

Online Meetings Overview

Online meetings provide a seamless and secure way for users to host real-time video and audio conferences, supporting collaboration beyond the limitations of traditional live chat. Unlike live chat, which is restricted to users within the same domain, online meetings allow external participants such as contract workers, consultants, and clients to join discussions. With built-in video, audio, text chat, and document sharing capabilities, online meetings serve as a powerful communication tool for businesses and teams.

Purpose

The primary goal of integrating online meeting providers is to provide a seamless platform for teams to connect through audio, video, and text chat. These integrations allow users to initiate and manage meetings directly from the SmarterMail webmail interface. Online meetings offer a comprehensive solution that brings strong communication tools directly into your email platform, fostering a more connected and efficient work environment.

Benefits

- Audio and Video Conferencing: Host virtual meetings with participants ensuring effective communication across teams.
- Screen Sharing: Enhance presentations and collaborative efforts by sharing entire screens, specific applications, or individual browser tabs during meetings.
- File Sharing: Easily upload and share files with preview capabilities, facilitating seamless collaboration and information exchange among participants.
- Participant Chat: Engage in unlimited text chat with real-time image and link previews, enriching the interactive experience during meetings.

<u>**Available Integrations**</u>

- SmarterMail Online Meetings

SmarterMail Online Meetings

SmarterMail's Online Meetings feature offers seamless audio and video conferencing for up to 9 participants, extendable to 16 with an external STUN/TURN server, and unlimited text chat participants. Built on the WebRTC framework, it ensures efficient bandwidth usage and high-quality communication. Users can share entire screens, specific applications, or individual browser tabs, enhancing collaboration. File sharing is integrated, with uploaded files stored in SmarterMail's File Storage for easy retrieval. Meeting organizers have full control over settings, including guest access and permissions, making Online Meetings a better alternative to third-party conferencing solutions such as Zoom or Microsoft Teams.

This feature is only available in SmarterMail Enterprise.

Jump to:

- Creating an Online Meeting
- Online Meetings and Calendar Invites
- Online Meetings Video Chat
- Screen Sharing
- Online Meeting File Uploads
- Uploading and Sharing Files

Creating an Online Meeting

When creating a new online meeting you'll be presented with this:

Title your meeting and you're ready to get started as the meeting's title is all that is actually required to save the meeting. However, there are a few other settings you can add on the creation screen: you can add a password and/or you can schedule the online meeting so that it will be used on a regular basis. Once you click the Save button, you can either stop there or open the meeting and further customize your settings.

Complete Settings

After you create your meeting, you can open it and modify its settings. As an aside, you can edit these settings at any time by clicking on the Settings (gear) icon whenever you open your meeting. Below is what the settings page looks like:

Just as with other areas of SmarterMail, the settings for an online meeting include various cards for categorization. The cards, and their respective settings, include:

Details

> • Title - This will be whatever you called the online meeting when it was initially set up, but you can change it at any time.
>
> • Secure with a password - If you want to lock access to the meeting with a password, that's not a problem. Simply set the password here to whatever you want. When sending out the invitation, however, be sure to let your participants know the password or they won't be able to join.
>
> • Allow guest users - Don't want to force your attendees to log in? No problem! Just enable "Allow guest users" and anyone with the link can attend the meeting, no log in required.
>
> • Allow attendees to start the meeting - Enabled by default, this means attendees can start the meeting without the Organizer to be present.

Security

> • Waiting Room - Waiting rooms allow organizers to specify which attendees should wait to be admitted into an Online Meeting. No one, Guests, or Everyone can be subject to waiting. When a new attendee "joins", a modal appears announcing they're waiting to be admitted into the meeting.

> • File upload permissions - Each meeting has the ability to allow users to upload files. However, the meeting organizer can set file upload permissions so that only the organizer has upload permissions, people who are authenticated users can upload files, or anyone can upload. Note: It IS possible to restrict the file extensions that are able to be uploaded to an online meeting. However, the File Storage Extension Blacklist is set by the system administrator.

> • Mute Others - Organizers can pick which type of attendee has the ability to mute other Online Meeting participants. While users may be allowed to mute other participants, they do not have the ability to un-mute participants. They must un-mute themselves.

Date and Time

> • Scheduled Meeting - Toggle Scheduled Meeting if you want to continue using the same online meeting on a regular basis. This is similar to creating recurring Calendar appointments where you set the state date and time as well as the ending date and time. Note: When an Online Meeting is created as part of a standard SmarterMail Calendar appointment, these will be set to mirror the date(s) and time(s) associated with the Appointment.

> • End Behavior - At the end of the scheduled recurrence, you have options to Archive Meeting, which ends the schedule but keeps the meeting in your list, Delete Meeting, or Keep Active.

Video Settings Note: Some browsers, such as Safari on macOS, default some audio/video settings. As a result, attendees may not have the ability to edit these settings.

> • Webcam - This is the stream quality for your online meeting. Video can take up a lot of bandwidth, so keeping this set to Low is a "best practice" if at all possible.

> • Microphone - This allows you to set the default microphone you use during the meeting. This will generally default to whichever default input device is set for your computer, but you can change it to headphones, an attached USB mic or any other input device you have set up.

> • Speakers - Just as with the microphone setting, this is the audio output for the meeting. Again, this will generally default to whichever default output device is set up for your computer, but you can change it to whatever.

Several advanced audio controls are also available:

> • Automatic volume controls - Enabling this allows SmarterMail to automatically handle increasing or decreasing the volume of the meeting.

> • Echo cancellation - Enabling this allows SmarterMail to automatically handle echo

management.

• Reduce background noise - Enabling this allows SmarterMail to automatically handle reducing any background noise that may be picked up by the microphone selected.

Meeting Link

• Meeting Link - This is the link to the meeting that can be shared with whoever you want to attend. You can select the text and copy it, or use the copy icon.

File Storage

This section will initially be empty. However, as you use the meeting, it will keep track of the number of files shared in the meeting and the space taken up by those files.

Chat

While chat is a great feature of online meetings, it may be necessary to delete the chat. For example, if the same meeting is used on a weekly or monthly basis for a meeting, you may want to delete the live chats after whatever information in the chat was transcribed to a separate document, once tasks have been created from action items, etc. This area allows you to delete all of the live chats that have occurred during the meeting.

Once you have all your settings in place, be sure to save them. As an aside, if you need to change a setting, like allowing guests to upload images, you can change that during the meeting and the setting takes effect immediately.

Online Meetings and Calendar Invites

When creating a meeting invitation in your calendar, you have the option to "Create Online Meeting". This setting allows organizers to have a new online meeting created, automatically, to be used for the appointment that's being set up. The meeting will use the appointment's Subject as its name and will appear in the Online Meetings area. In addition, a link to the meeting is sent with the meeting invitation to all attendees. By default, meetings are initially created to allow for guest users, do not have passwords assigned, and are set so that only the Organizer can upload files. Therefore, if any of these settings need to be changed, they'll need to be changed prior to the meeting date/time, and any changes manually sent to the attendees. note: If an appointment that has an online meeting associated to it is cancelled or otherwise deleted, the online meeting is not deleted immediately. Instead, SmarterMail runs a nightly routine that will remove online meetings associated with deleted/cancelled appointments.

Access Previous Meetings

Any meeting room you create are saved as a separate cards. That means you can access, and re-access,

any past meetings. While the video isn't saved, any live chats and shared documents ARE saved, allowing you to refer back to those at a later date whenever needed.

Participated Meetings

Not only are the meetings that YOU create listed, so are meetings that you've been invited to. To access these, simply click on the Participated Meetings option from the left navigation pane. Here, meetings that you've participated in are listed as separate cards. While you won't be able to edit any information on these cards, you do have the ability to revisit the meetings, see chats, re-login to the video chat and more.

Sharing Online Meeting URLs

The URL for an online meeting can be accessed in two locations:

> • Using the Actions (□) menu on a meeting's card — simply click on the menu and select Copy Link from the dropdown. Online meeting can be deleted from this location as well.• By opening the actual meeting and copying the URL from its settings.

The first method is, by far, faster and more convenient. It allows you to quickly grab a URL and share it in a live chat, in an email or when creating a single or recurring appointment.

Online Meetings

This feature is only available in SmarterMail Enterprise.

With Online Meetings, you can have real-time audio and/or video chat with up to 9 participants at the same time. In addition, each participant has complete control over their interaction — that is, they can manage the microphone and speakers that are used. Participants can also mute others, so if someone is in a noisy environment and they forget to mute their microphone, each participant can mute that person themselves. Note: In order to use online meetings your SmarterMail installation MUST be secured with an SSL certificate. This is because the audio, video and live chat connections require HTTPs connections in order to work properly and securely.

Starting an Online Meeting

When accessing an online meeting, you're initially presented with a live feed of your webcam, as well as the options to change the camera and/or the microphone used for the audio portion of the meeting.

You can use this page to modify those settings and, if necessary, troubleshoot any issues. (e.g., ensuring your browser window has the proper permissions for accessing your camera.)

Once you're ready, simply click the Join Meeting button.
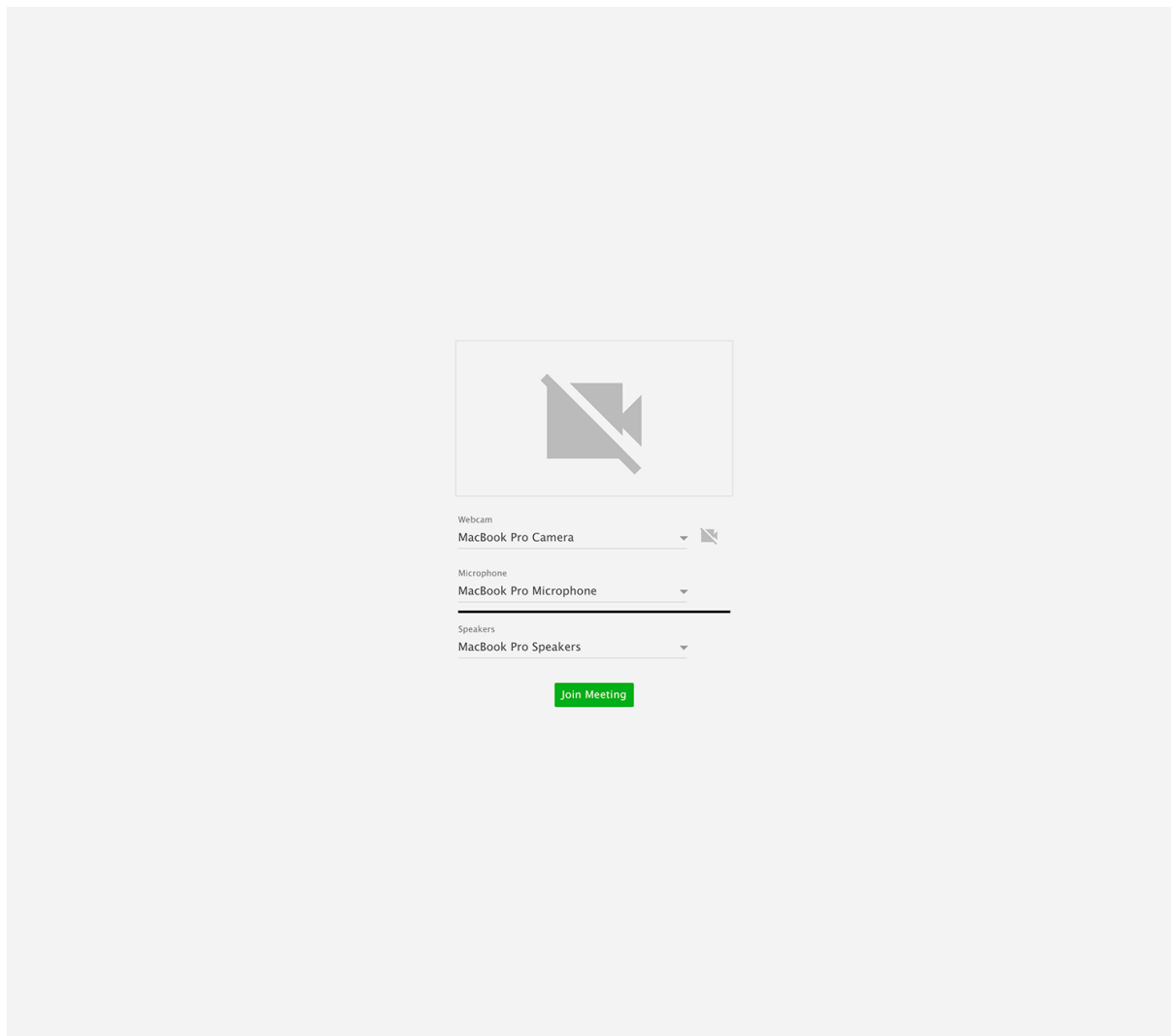
Once you enter the room, you'll see your own audio/video feed as well as the video feed of other participants. As more people join their feeds will also display. If someone turns off their camera, you'll see a blank box with a monogram in the middle of the box, so you know who that's supposed to be.

Screen Sharing

From training sessions to document collaboration, screen sharing makes online meetings even more helpful and productive, enhancing the ability for people to communicate and work together. With screen sharing, users are able to share the following:

• Your Entire Screen - Users can opt to share their entire screen, regardless of how many applications are open. This allows them to switch between applications during a meeting. When they have multiple monitors, they can even select which monitor they want to share.
• Application Windows - If multiple applications are open, rather than share an entire screen, specific applications can be shared. This makes it easy to collaborate on office documents, troubleshoot code, review marketing material and more.
• Specific Browser Tabs - Just as with applications, it's also possible to share a specific browser tab. So, you're online meeting can be running in one tab while a separate one that is open to a website, online application, calendar or more can be shared and worked on as a group.

To start sharing your screen during a meeting:

• In the toolbar at the top of the video chat, click on the Sharing icon• Select the item/screen you want to share: an entire screen, an application or a browser tab.

• Generally, you will be taken to the screen you're sharing so you can interact with it during the meeting. It will have a light blue outline demonstrating what you're sharing. You can, however, go back to the meeting and your shared screen will take the "focused" area of the meeting. (I.e, be the largest screen displayed at the top of the meeting.)

• When done, simply de-select the Sharing button. (Or, you may also receive a notification that you're sharing an item and can stop the share from within that notification.)

Video Settings

Participants have some control over the audio and video settings that are used. To modify those settings, simply click on the Settings icon. On the Video Settings card you'll be able to set:

• Webcam - You can set your video quality from High to Very Low. In cases where a participant is on a poor internet connection, or even using a cellular connection, the Low or Very Low settings may be preferred to help reduce bandwidth.

• Microphone - The meeting will select a default microphone for you. However, if you want to change it to a headset mic or something else, you can do that here.

• Speakers - The default speaker set should be used by default, but if an external source is desired, it can be selected from the dropdown.

• Automatic volume controls - Enabling this allows SmarterMail to automatically handle increasing or decreasing the volume of the meeting.

• Echo cancellation - Enabling this allows SmarterMail to automatically handle echo managment.

• Reduce background noise - Enabling this allows SmarterMail to automatically handle reducing any background noise that may be picked up by the microphone selected.

Troubleshooting and Status Indicators

From time to time, issues may arise when connecting to an online meeting. Common issues seen are an attendee seeing having a black video screen and below are a few troubleshooting steps for attendees who are experiencing issues:

• First, and arguably the simplest, is to make sure the attendee has turned on their microphone and camera once they join. By default, both are turned off for attendees.

• It's possible that the attendee's browser is blocking their microphone and/or their video

camera. Have the attendees double-check their browser settings to ensure the browser is allowing the use of the camera and/or microphone.

• Pop up blockers and/or ad blockers can interfere with browser-based audio and video chat. Have the attendee add an exception to their ad blockers for your email domain, or at least temporarily allow the connection.

• If they're using any security software, such as Eset or Malwarebytes, these may need to be checked so that access to the camera and microphone aren't being blocked.

• If they have "turned on" both their mic and camera, but you still see a black screen for them, have them leave the meeting, then rejoin. (Simply turning the video off, then back on may work as well.) The majority of the time this will re-negotiate the connection to the meeting and clear up the issue.

• If possible, have the attendee clear their browser cache. This is useful if they've attended previous online meetings and a recent update was applied to the SmarterMail server.

• Of course, network issues — either on the organizer's end or the attendee's end — will cause problems. Most times, having the attendee turn off their video and simply use voice communication can stabilize a connection.

• Finally, online meetings DO require the use of SSL. If your mail domain isn't secured with an SSL certificate, this will cause problems.

Sometimes, you might run into issues when joining an online meeting, like seeing a red, green or orange connection icon next to an attendee's video.

• Red: This indicates "High RTT" or round-trip time. Think of this in terms of "ping" time: the higher the number, the longer it takes for a response to a request to get back to you. This can be seen by experiencing lag in voice or video displays and is generally a consistent issue.

• Green: This indicates high "jitter". Jitter essentially means that the signal is inconsistent: the signal is strong some times, weak at others. So it's a bit different than high RTT as it's not consistent.

• Orange: This indicates issues with frame rate. This can be seen by a degradation in video quality. However, even if you see this icon, you may not notice any issues as the variance my not be discernible.

Online Meeting File Uploads

This feature is only available in SmarterMail Enterprise.

Part of having a collaborative meeting is the ability to upload and share files. The online meeting organizer has the ability to set the file upload permissions for the meetings they set up. They can allow anyone to upload files, only allow authorized users (people who log in) to upload, or limit file uploads to just themselves. However, anyone who participates in the meeting can download any files that are

shared. Note: Management for files uploaded during an online meeting belongs solely to the meeting organizer, regardless of who has the ability TO upload files. This is to ensure that all files are preserved as part of the meeting, at the organizer's discretion. Therefore, the disk space used for uploads also counts towards the total disk space of the organizer.

Setting File Upload Permissions

The meeting organizer has the ability to set permissions for the types of attendees that can upload shared files. This is done in the meeting's Settings area on the Details card. There is a File upload permissions dropdown that includes the following permissions:

- Organizer Only - The only person who can upload files to an online meeting is the user who set up the meeting in the first place.
- Authenticated Users - Attendees who log into the online meeting are able to upload files; guests can not upload.
- Everyone - All attendees are able to upload files as needed.

Uploading and Sharing Files

Once permissions are set, it's time to upload and share some files. A few quick things to note:

- Just as with the File Storage area, whenever possible a thumbnail of the file will be displayed. If a thumbnail can't be displayed, then an icon representing the file type will be displayed.
- Shared files will show the file name and the file size on their respective cards.
- Clicking on the Actions (□) icon allows for the download and/or deletion of individual file.

As for actually uploading files, there are a few ways to do this:

- Drag and Drop - You can drag and drop files directly into the list and they will be uploaded and displayed in the Files area. Files uploaded to chat will display a download link in the chat, just as they do in a regular Live Chat , but they'll show up in the Files area as well.
- Upload Button - You can also use the Upload button in the Files area or the paperclip icon in the Chat area to upload files. Regardless of which option you use, your File Explorer (or similar) opens, allowing you to choose a file to upload.

Downloading or Deleting Shared Files

Each file that's shared in an online meeting has its own card. Each card, in turn, has an Actions (□) option in the upper, right corner. Clicking on that gives a participant the ability to download that particular file. In addition, a participant can delete the file, should they choose to.

File Storage

File Storage Overview

SmarterMail's file storage integrations provide a secure and efficient alternative to traditional email attachments. By allowing users to upload and share files via links instead of embedding large attachments directly in emails, this feature enhances mail server performance, improves security, and eliminates common attachment size restrictions. File storage systems enable users to store files on the mail server or on cloud storage providers and then distribute them through shareable links. This reduces the strain on the mail server's email spool, preventing large attachments from slowing down email performance. Additionally, file storage solutions generally provide flexibility in sharing, allowing users to manage file access levels, set expiration dates for links, and apply password protection for added security.

Purpose

The primary goal of secondary file storage options is to optimize email communication by addressing the limitations of traditional attachments. By keeping large files out of the email spool, this feature ensures that mail servers remain reliable and efficient. It also enables users to share larger files without being restricted by domain or system administrator policies, enhancing collaboration and accessibility.

Benefits

• Improved Mail Server Performance: Reduces the load on email servers by keeping large files separate from the email spool.

• Bypass Attachment Restrictions: Allows users to send large files without being limited by domain or hosting provider rules.

• Enhanced Security: Protects recipient mail servers from potentially unsafe attachments while avoiding file type restrictions.

• Flexible File Sharing: Users can set files as public or private, apply password protection, and establish expiration dates for links.

• Persistent File Access: Files shared in live chats and online meetings remain available for future use.

• Shorter, More Secure Links: Upgraded file-sharing links are now more secure and easier to distribute. note: SmarterMail's File Storage stores files on the mail server that count toward the user's disk space allocation, so it is recommended that users regularly delete unused files to free up space. Additionally, users upgrading from SmarterMail 15.x or earlier must re-send any previously shared file links, as older links will no longer function with the new security enhancements.

<u>**Available Integrations**</u>

- Dropbox
- Google Drive
- Leitzcloud/vBoxx
- OneDrive
- ownCloud
- SmarterMail File Storage

Connecting to Dropbox

Dropbox is a user-friendly cloud storage and collaboration platform that enables you to store, share, and access files from any device. Integrating Dropbox with SmarterMail can improve your file management experience. You can easily attach large files to emails by linking them from your Dropbox account, which helps reduce email storage and ensures that recipients always receive the most up-to-date version of the file. These links navigates around mail server attachment size limits, making it easier to share large files. Plus, you can set permissions (view/edit) and expiration dates for Dropbox links in SmarterMail, ensuring secure sharing.

To integrate Dropbox with SmarterMail:

- Within Marketplace , navigate towards the Dropbox card, make sure your System or Domain Administrator has Dropbox enabled.
- Click on the Dropbox card, a pop-up window will display log-in credentials.

• Log into your Dropbox account through a secure OAuth connection, granting SmarterMail access to your Dropbox account with necessary permissions.
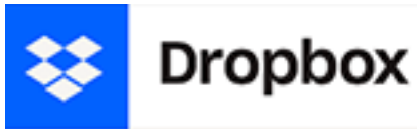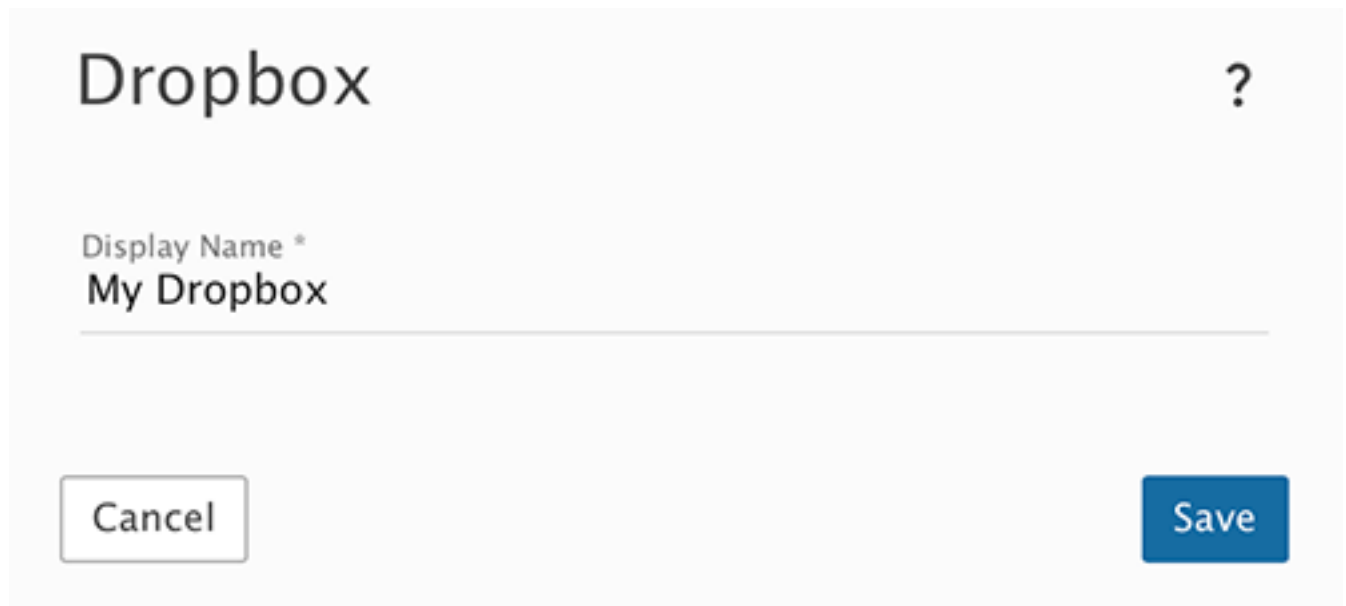
• You can name your cloud service in the Display Name field (This is mandatory). The default name is "My Dropbox" . Click Save to apply your changes and confirm the name of your cloud connection.

Dropbox ?

Display Name *
My Dropbox

Cancel   Save

Attaching Linked Files from Dropbox

> • Once connected, users can easily browse their Dropbox files and insert shareable links directly into email messages.
>
> • Simply click the Actions (□) button, select Link File , and a pop-up window will appear, allowing you to choose your preferred cloud service, select Dropbox .
>
> • Navigate to the desired file and click on it.
>
> • Dropbox will automatically generate a hyperlink for the file. You'll also have the option to set permissions, add a password, or establish an expiration date for the link, ensuring secure and controlled access.

Connecting to Google Drive

Google Drive is a user-friendly cloud storage and collaboration platform that allows you to store, share, and access files from any device. Integrating Google Drive with SmarterMail enhances your file management experience by making it easy to attach large files to emails through shareable Google Drive links. This not only reduces email storage but also ensures recipients always have access to the latest version of the file. These links bypass mail server attachment size limits, simplifying the process of sharing large files. Additionally, you can set permissions (view/edit) and expiration dates for links within SmarterMail, ensuring secure and controlled file sharing.

To integrate Google Drive with SmarterMail:

> • Within Marketplace , navigate towards the Google Drive card, make sure your System or Domain Administrator has Google Drive enabled.
>
> • Click on the Google Drive card, a pop-up window will display log-in credentials.

G Sign in with Google
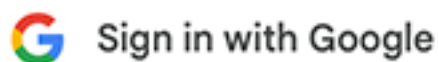
Sign in

to continue to **SmarterMail**

Email or phone

Forgot email?

Before using this app, you can review SmarterMail's **privacy policy** and terms of service.

Next

English (United States) ▼   Help   Privacy   Terms

• Log into your Google Drive account through a secure OAuth connection, granting SmarterMail access to your Google Drive account with necessary permissions.

G **Sign in with Google**
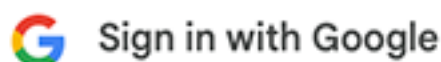
smartertools.com wants access to your Google Account

Select what **smartertools.com** can access

See, edit, create, and delete only the specific Google Drive files you use with this app. **Learn more** ☑

Because you're using Sign in with Google, smartertools.com will be able to

Associate you with your personal info on Google ☑

See your primary Google Account email address ☑
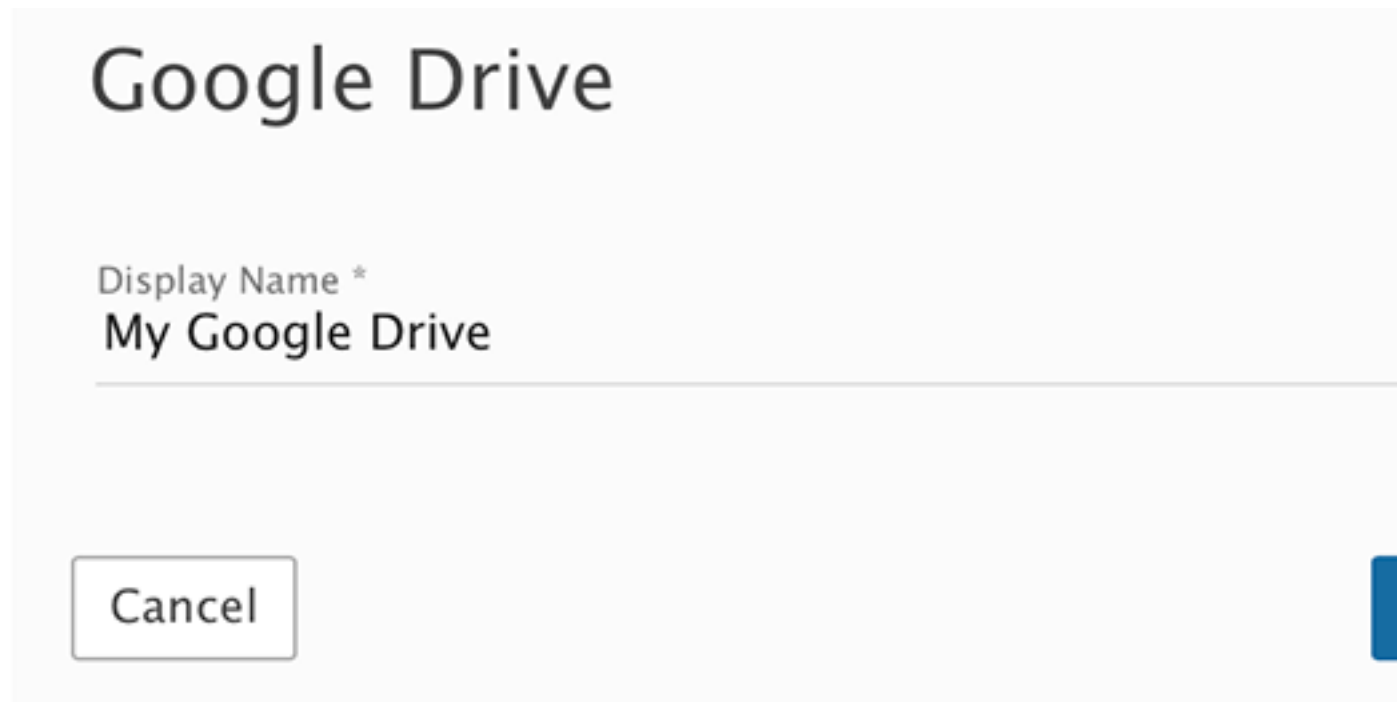
Make sure you trust smartertools.com

ⓘ **Learn why you're not seeing links to smartertools.com's Privacy Policy or Terms of Service**

• You can name your cloud service in the Display Name field (This is mandatory). The default name is "My Google Drive" . Click Save to apply your changes and confirm the name of your cloud connection.

Attaching Linked Files from Google Drive

> • Once connected, users can easily browse their Google Drive files and insert shareable links directly into email messages.
> • Simply click the Actions (□) button, select Link File , and a pop-up window will appear, allowing you to choose your preferred cloud service, select Google Drive .
> • Navigate to the desired file and click on it.
> • Google Drive will automatically generate a hyperlink for the file. You'll also have the option to set permissions, add a password, or establish an expiration date for the link, ensuring secure and controlled access.

Connecting to Leitzcloud/vBoxx

Leitzcloud is a secure and user-friendly cloud storage and collaboration platform that enables businesses to store, sync, and share data while ensuring productivity and security through advanced encryption and two-factor authentication. By integrating Leitzcloud with SmarterMail, users can easily attach large files to emails using shareable links, reducing email storage and guaranteeing access to the latest version of the files. This integration bypasses mail server attachment size limits, making it

simpler to share large files. Additionally, users can set permissions (view/edit) and expiration dates for links within SmarterMail, ensuring secure and controlled file sharing.

To integrate Leitzcloud with SmarterMail:

> • Within Marketplace , navigate towards the Leitzcloud card, make sure your System or Domain Administrator has Leitzcloud enabled.
> • Click on the Leitzcloud card, a pop-up window will display log-in credentials.
> • Log into your Leitzcloud account through a secure OAuth connection, granting SmarterMail access to your Leitzcloud account with necessary permissions.
> • You can name your cloud service in the Display Name field (This is mandatory). The default name is "My Leitzcloud" . Click Save to apply your changes and confirm the name of your cloud connection.

Attaching Linked Files from Leitzcloud

> • Once connected, users can easily browse their Leitzcloud files and insert shareable links directly into email messages.
> • Simply click the Actions (□) button, select Link File , and a pop-up window will appear, allowing you to choose your preferred cloud service, select Leitzcloud .
> • Navigate to the desired file and click on it.
> • Leitzcloud will automatically generate a hyperlink for the file. You'll also have the option to set permissions, add a password, or establish an expiration date for the link, ensuring secure and controlled access.

Connecting to OneDrive

OneDrive is a user-friendly cloud storage and collaboration platform that allows you to store, share, and access files from any device. Integrating OneDrive with SmarterMail enhances your file management experience by making it easy to attach large files to emails through shareable OneDrive links. This not only reduces email storage but also ensures recipients always have access to the latest version of the file. These links bypass mail server attachment size limits, simplifying the process of sharing large files. Additionally, you can set permissions (view/edit) and expiration dates for links within SmarterMail, ensuring secure and controlled file sharing.

To integrate OneDrive with SmarterMail:

> • Within Marketplace , navigate towards the OneDrive card, make sure your System or Domain Administrator has OneDrive enabled.
> • Click on the OneDrive card, a pop-up window will display log-in credentials.

Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

🔑 Sign-in options

Terms of use   Privacy & cookies   • • •

• Log into your OneDrive account through a secure OAuth connection, granting SmarterMail access to your OneDrive account with necessary permissions.

Microsoft

Let this app access your info? (1 of 1 apps)

SmarterMail needs your permission to:

Maintain access to data you have given SmarterMail access to

Allows SmarterMail to see and update the data you gave it access to, even when you are not currently using the app. This does not give SmarterMail any additional permissions.

Read your profile

SmarterMail will be able to read your profile.

Access OneDrive files

SmarterMail will be able to open and edit OneDrive files, including files shared with you.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://microsoft.com/consent. Show details

• You can name your cloud service in the Display Name field (This is mandatory). The default name is "My OneDrive" . Click Save to apply your changes and confirm the name of your cloud connection.

<u>Attaching Linked Files from OneDrive</u>

- Once connected, users can easily browse their OneDrive files and insert shareable links directly into email messages.
- Simply click the Actions (▢) button, select Link File , and a pop-up window will appear, allowing you to choose your preferred cloud service, select OneDrive .
- Navigate to the desired file and click on it.
- OneDrive will automatically generate a hyperlink for the file. You'll also have the option to set permissions, add a password, or establish an expiration date for the link, ensuring secure and controlled access.

Connecting to ownCloud

ownCloud is a free, open-source platform for storing, sharing, and collaborating on files online. It's ideal for individuals and small teams, offering secure cloud storage, easy file sharing, and real-time collaboration. With ownCloud, files stay synced across devices, ensuring seamless access and updates. When integrated with SmarterMail, ownCloud enhances email workflows by allowing users to attach, store, and share files directly from their cloud storage. This integration streamlines collaboration while maintaining security and control over data, making file management more efficient for businesses and teams.

To integrate ownCloud with SmarterMail:

- Within Marketplace , navigate towards the ownCloud card, make sure your System or Domain Administrator has ownCloud enabled.
- Enter your ownCloud credentials and server address. In the Display Name field (required), assign a name to your cloud service, the default is My ownCloud .

• Click Save to apply your changes and confirm your ownCloud connection.

• Once ownCloud is connected to SmarterMail, your ownCloud files will be accessible in File Storage under the More link.
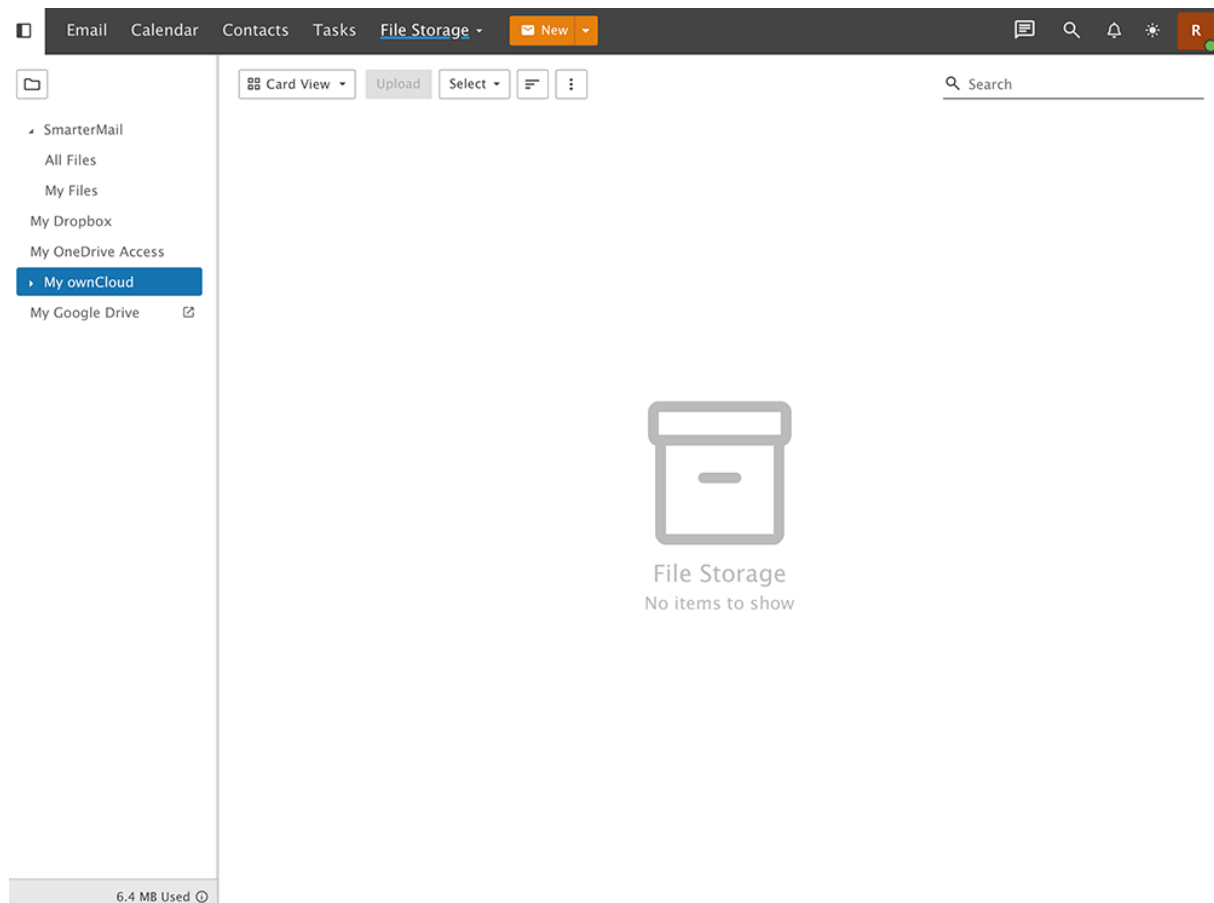
Attaching Linked Files from ownCloud

• Once connected, users can easily browse their ownCloud files and insert shareable links directly into email messages.

• Simply click the Actions (☐) button, select Link File , and a pop-up window will appear, allowing you to choose your preferred cloud service, select ownCloud .

• Navigate to the desired file and click on it.

• ownCloud will automatically generate a hyperlink for the file. You'll also have the option to set permissions, add a password, or establish an expiration date for the link, ensuring secure and controlled access.

SmarterMail File Storage

SmarterMail's file storage feature allows users to upload files to the server and share them via public links. One benefit of using file storage is that it reduces the stress on the server by keeping large files out of the spool. SmarterMail's file storage feature bypasses some limitations of sending standard email attachments plus it can help keep a mail server secure and running reliably.

• Max File Size (KB) - The maximum size a file can be in order to be uploaded to the File Storage area. This has a relationship to the file size limits for attachments, and any files uploaded to Online Meetings and/or Chats as all of those items are stored in a user's File Storage area.

• Root Webmail URL - The base URL of any file stored and shared in file storage. By default, the base URL corresponds to the domain the mail server is set up on (i.e., http://mail.example.com). If SmarterMail is configured on an external IP that allows a network address translation (NAT) to an external IP, the system administrator may need to modify the root URL.

One key benefit is that it allows users to send larger files without worrying about hitting any attachment size restrictions enforced by a domain administrator, system administrator or hosting company. Sending links instead of actual files also helps recipient mail servers as it keeps potentially insecure files from hitting the mail server, not to mention it bypasses any file type restrictions a recipient's mail server may have set up. For example, if an email administrator blocks Powerpoint files, sending the link to that presentation versus the presentation itself ensures the recipient receives the file. Note: Files uploaded to the server are counted toward the user's disk space allocation, so users are encouraged to delete files that are no longer used from the server whenever possible.

With file storage, users can upload files to the mail server and then share them by sending out links to those files. Recipients can then download the files to their local desktop or mobile device. Files can be public or private, links can be secured with a pre-shared password, they can last forever or have expiration dates, and much more. Note Regarding Upgrades: One of the many security changes made to recent Builds of SmarterMail was to re-format the links used when sharing files. Therefore, any customer who upgrades from SmarterMail 15.x or earlier to a current Build will need to re-send any existing publicly-shared links as older links will no longer work. The new links are not only much more secure, they're much shorter, making them easier to send and use.
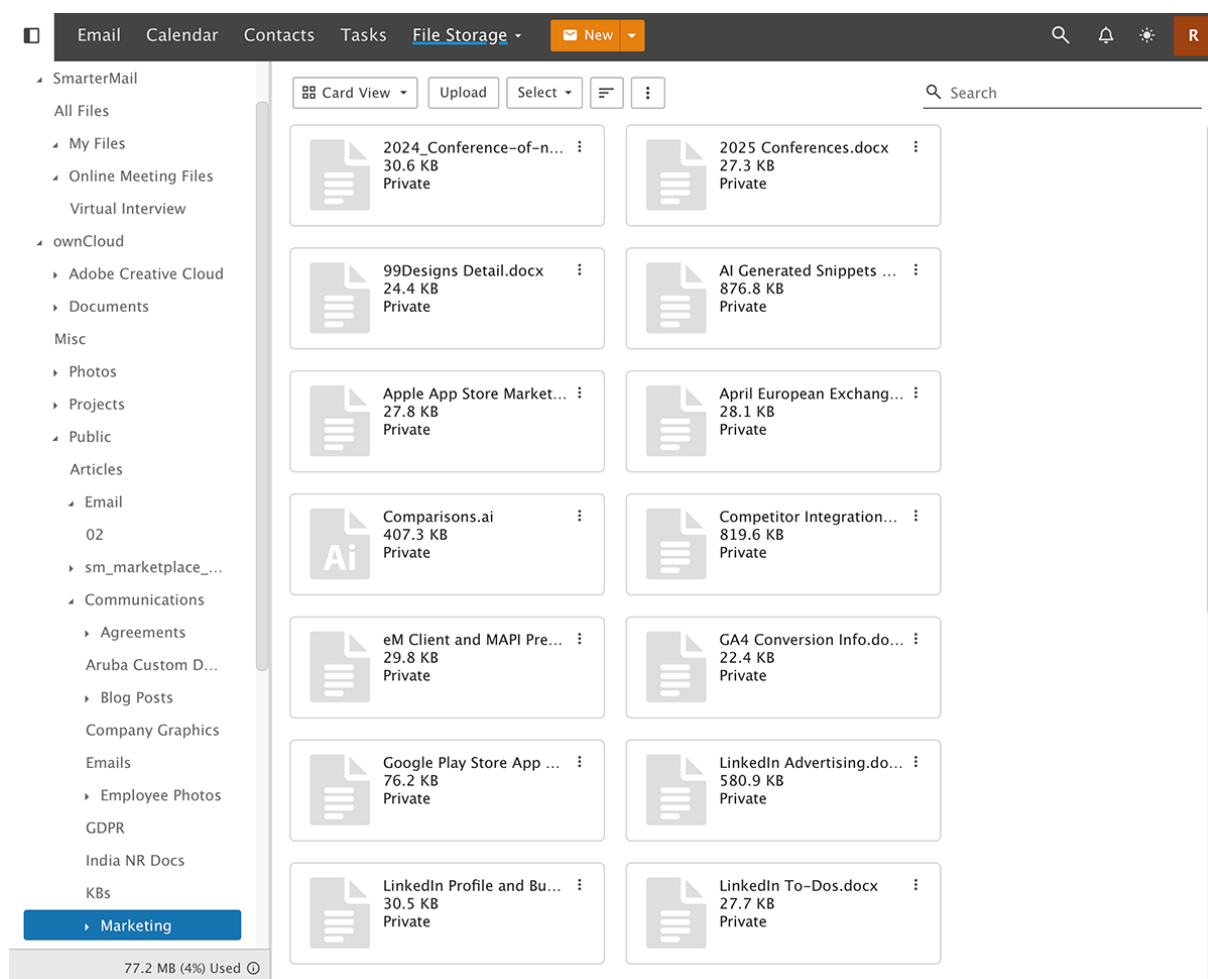
Navigating File Storage

File Storage Layout

When you view file storage, each file you've uploaded will be listed on a separate card. Each card lists the following information, which is described in detail further down this page:

> • File Type Icon - An icon that represents the type of file uploaded (e.g., page with a zipper for a .ZIP file). For image files, SmarterMail attempts to generate a thumbnail of the file rather than use a generic icon, though not all image file types are supported.
>
> • Filename - The actual file name plus its extension.
>
> • Size - The size of the file.
>
> • Status - Whether the file is available to the public or if it's private. If it's a public file, the expiration date and time for the link is displayed, if one has been set.

In general, the following options are available when viewing all of your files:

> • Upload - Clicking this button allows you to upload a file to File Storage.
>
> • Select - Allows you to select more than 1 file at a time. To select multiple files, click Select and then click on one or more cards. To exit Select mode, click the Select button again. To de-

select a file, simply click on it again. Alternatively, click the down arrow and you're presented with the following options:

• Select All - Selects all files in the list you are viewing.

• Deselect All - Deselects all the selected files.

• Enter Select Mode - Allows individual files to be selected from the list, one at a time.

• Sort - Clicking the Sort menu brings up the following options:

• Filename - The file's name. (E.g., Sales_Analysis.xlsx)

• Size - The size of the file. (E.g., 40KB)

• Date Uploaded - The date the file was uploaded to File Storage.

• Public - Whether the file is able to be downloaded by anyone (i.e., Public) or not. Files available to the public are listed first.

• Reverse Order - Changes the sort from ascending to descending, and vice versa.

• Actions (□)

• Move - Move the file(s) to another folder or location.

• Download - Download the file(s) to your local machine.

• Delete - Deletes the selected files. NOTE: You can also use the Delete key on your keyboard.

Uploading Files

Uploading a file to SmarterMail's file storage works just like any other upload: Using the Upload button, your file system opens and you can navigate to where the file you want to upload is located. Simply select the file and click "Open" and the file begins its upload. The time it takes to upload the file depends on a number of things, such as the file's size and the type of internet connection you have.

You can also simply drag-and-drop a file, or group of files, into the folder you've selected and are viewing. Dragging and dropping works just like using the Upload button.

By default, files uploaded are set to "Private", so they can't be shared. For more information on sharing files, see Sharing Uploaded Files .

Uploading Folders

There are two ways to upload entire folders to file storage:

• Drag and Drop - Simply open File Explorer on your desktop and drag the folder into the Files area of File Storage. The folder itself and the contents will be uploaded, and the folder will be automatically added to navigation pane under the folder you've uploaded to (e.g., My Files). Simply click on the folder name to view the files.

• From the Folders Menu - At the top of the folders list is the Folder button. One of options

when you click on it is Upload Folder . Selecting that opens up File Explorer. Simply navigate to the folder you want to upload, select it and click the Upload button in File Explorer.

Deleting, Downloading and Moving Files

Once a file has been uploaded, you may want to remove it or re-download it to your local machine. Clicking on the Actions (☐) button in the top, right corner of a file's card presents you with:

- Copy Link - When a file is made Public, this is the link that can be used to share that file with others. This is simply a quick way to copy the link to use.
- Move - Allows you to move the file to a new folder.
- Download - Allows you to save the file locally.
- Edit with OnlyOffice - This allows you to edit the supported file type using an existing installation of OnlyOffice, right from a browser. For more information, see OnlyOffice Online .
- Delete - Allows you to delete the individual file.

Regarding folders, simply right-click on a folder name to open its context menu.

File Storage Folders

Adding folders for storing file uploads is the perfect way to keep those files organized.

Option 1: Using Right-Click within the directory.

- Navigate to the location where you want to create the folder.
- Right-click in the empty space.
- From the menu, select New Folder . Additional options include: Move Folder , Edit Folder , and Delete Folder .

Option 2: Using the New Folder Icon

- Look at the top of the left sidebar.
- Click on the New Folder icon.
- Choose to either: add a New Folder , or Upload a Folder.

Online Meetings and Attachments Folders

An added benefit of file storage in SmarterMail is that files uploaded to an online meeting, or files that are attached to items (e.g., tasks or calendar appointments) are also stored. When files are uploaded or attached in these areas, Online Meetings Files and/or Attached Files will appear. Under these headers, folders with names that match online meeting titles and/or folders that match a particular area (e.g., Tasks, Appointments, etc.) appear. Within these folders, the files that were uploaded and/or attached are displayed for storage and later use.

Cloud Storage Folders

Along with any custom folders you create, if you've added any Cloud Storage Connections, those will appear in File Storage as well. It's worth noting that you are not able to upload any new files to these storage providers — you need to use their native apps — but you can view the contents of each as well as download files as needed.

File Storage Extension Blacklist

By default, SmarterMail allows system administrators to keep a list of file extensions that are excluded from file storage. These files generally can cause issues for people who download them, much less the SmarterMail server itself. These file types can include, but are not limited to: Windows executable files, Java files, Batch files and more.

Sharing Uploaded Files

As mentioned, the primary purposes of File Storage in SmarterMail are to both bypass any potential attachment limits imposed by domain administrators and alleviate any potential stress or performance impact on the mail server. SmarterMail keeps files uploaded in a different location than email attachments, but, just like with email attachments, files uploaded count against any total disk space allocations for your entire mailbox. That said, SmarterMail does show users how much disk space they're using, and even separates file storage disk space from overall email space.

Sharing files is easy, but it does require a couple of simple steps. These include:

- Enabling public access to the file, and
- Sharing the link to the file in an email or group chat.

Enabling Public Access

Once the file is uploaded to the file storage area, it will be listed alphabetically by file name and displayed along with all of your other files. To set the sharing options for the file, you simply need to edit the file's settings by selecting its card from the list. Once you've clicked on the file's card, the following options will be available:

- Filename - The name of the file. This defaults to the file name of the uploaded file plus its extension. However, you can change this to whatever you like.
- Enable Public Access - Toggling this option allows you to make the file available for sharing via a public link. Keeping the toggle off makes the file private, and, therefore, unable to be shared.
- Expiration Date / Time - The date and time that the public link to download the file expires. Leave this set to "None" and the link will never expire. Several default timeframes are available,

from 1 hour up to 1 year. You can change the timeframe as needed. If you want to remove the expiration date/time, simply move the slider back to the off position.

• Password - The password used to download the file. Leave this blank if you don't want to password protect the link.

• Public Download Link - This is the direct link to the file. This can be shared to anyone by copying the link and inserting it into an email message or live chat.

Sharing a Link

Once you've added public access to a file, the next thing you need to do is share it with someone.

To share a file directly from the webmail interface, simply type up your message, and when you want to insert the link, select the Actions (□) button and when the menu drops down, select Link File . A modal window opens and you'll be able to select a file from anywhere within File Storage. Click the Link button, the file's name is inserted into your message, and that file name also acts as the clickable link for the user. They simply click the file name and they can download and save the file anywhere.

If you're using a separate email client, or even live chat, you can use the Public Download Link. Just add that entire link to any message created in an email client, when using live chat, when exchanging text messages or any other communication method and whomever you're talking to can download your file.

Email Client

Email Client Overview

SmarterMail seamlessly integrates with various email clients, mirroring Microsoft Exchange in how it handles languages and folder synchronization. Whether using Outlook, Thunderbird, Windows Mail, eM Client, or Mac Mail, SmarterMail ensures that emails, special folders, and language settings sync efficiently across platforms. In some cases, SmarterMail even surpasses Exchange in its ability to manage language changes and prevent duplicate folder issues.

Purpose

The purpose of SmarterMail's email client integration is to provide users with a smooth and flexible email experience, regardless of their preferred client. By supporting multiple sync protocols, SmarterMail ensures that emails, special folders (such as Sent Items and Drafts), and language settings remain consistent across devices. This allows users to work efficiently, whether accessing email through a web browser or a third-party client.

Benefits

- Seamless Syncing Across Clients: SmarterMail ensures correct folder mapping on initial sync and updates folder names when the language is changed in webmail.
- Better Language Handling Than Exchange: Unlike Exchange, SmarterMail minimizes duplicate folder creation when switching between languages, reducing clutter.
- Multi-Client Compatibility: Works with Outlook (Windows & Mac), Thunderbird, Windows Mail, eM Client, and Mac Mail, ensuring flexibility for users.
- Automatic Folder Updates: Special folders update their names automatically when the language in SmarterMail is changed, maintaining consistency across platforms.
- Improved Performance and Stability: SmarterMail prevents unnecessary syncing issues and ensures special folders do not unnecessarily duplicate across email clients.
- Flexible Protocol Support: While IMAP connections are commonly used, SmarterMail optimizes language and folder synchronization when connecting through other supported protocols. Important Note: When changing a user's language setting in SmarterMail, it is recommended to remove and re-add the email account in the client to ensure proper synchronization and avoid potential duplicate folder issues.

SmarterMail's strong email client integration ensures a smooth and consistent experience, making it an ideal choice for businesses and individuals who rely on multiple platforms for email communication.

Quick Links

- eM Client

eM Client

This settings page is only available to domain administrators.

SmarterTools' groundbreaking partnership with eM Client gives SmarterMail users access to one of the most powerful and fully customizable email clients around. eM client offers an ideal replacement for Microsoft Outlook and is available for both Windows and MacOS. It gives users the features they need, and the functionality they expect, including calendars, contacts, tasks, notes, instant messaging integration, sharing and collaboration, delegation, automated account configuration, and more!

Thanks to our partnership, domain administrators can receive a complimentary eM Client Business Pro license that comes with 3 device activations. In addition, if more device activations are needed, they can be purchased directly from eM Client at a 25% discount! Activations can be handed out to any users of the qualifying domain and are tracked and managed right from within SmarterMail.

The way eM Client's licensing works is each organization receives one license key, but a single key can have multiple devices activated. For example, one key can have 10 devices attached to it.

Activations can be added at any time, and each activation acquired receives the 25% discount from eM Client.

Prerequisites

There are a few things that need to be set up properly in order to take advantage of this partnership. These include:

- You need to have a licensed version of SmarterMail installed. (Free Editions and trials are not eligible.)
- Your installation should be able to access our activation servers.
- Port 443 should be open to the public. (A requirement for the above.)
- Domains must be active and able to send and receive email.
- Only top-level domains are eligible due to eM Client's licensing.

This page will walk through acquiring the eM Client license, then how to manage activations once they've been handed out to users. note: eM Client licenses are only available for top-level domains. Third-level (mail.example.com) or subdomains are not eligible.

- Domain Verification
- License Ownership
- Getting a License Key
- Managing Activations
- Purchasing Additional Device Activations

Domain Verification

In order to receive an eM Client license, the domain first needs to be verified by SmarterTools. To verify the domain, do the following:

- Login as a domain admnistrator and go to Domain Settings
- Select eM Client from the tree menu.
- In the content pane, click the Request Code button on the Verify Domain card.

In the background, SmarterTools will generate a verification code that's sent to the email address of the domain administrator walking through the eM Client licensing process. This ensures that the domain is set up properly and is able to receive email from an external sender, which is a requirement because the license key is sent directly from eM Client.

- Go to the domain administrator's inbox and look for the verification email. It will come from "noreply@@smartertools.com".
- Copy the verification code.

Note: Codes can only be used once . They expire in 4 hours.

• Return to the eM Client Licenses page and paste/type in the code.

• Click the Verify Code button.

Domain verification is complete when the page refreshes and you see a new page with a short form to fill out.

License Ownership

Once the domain is verified, some basic information about the organization requesting the license is required in order to get the license key from eM Client. It's important to note that the eM Client license should be associated to a business rather than an individual. While the domain administrator can be the one to request the license, a shared organizational email address (e.g., vendors@@your-domain.com) or a management address should probably be used for the account that's created in eM Client's License Manager. This ensures that any issues with the license can be handled by any domain administrator rather than a single individual. The information requested includes:

> • Organization Name* - The name of the company, business, or individual who will own the license key.
>
> • Full Name - The full name of the organizational contact.
>
> • Owner email address* - The email address for the organization that will be associated with the key.
>
> • Confirm owner email address*
>
> • Country - The local of the organization.
>
> • Privacy policy links and confirmation - We take great care in selecting our partners. However, it is still a good idea to read and understand the privacy, cookie, and data protection policies of any company you do business with.

Only "Organization Name" and "Owner email address" are required. Once the information is filled out, click the Submit button.

Getting a License Key

Clicking "Submit" sends the information to eM Client and then the eM Client license key is returned. The page will reload and information about the key is displayed on the page for the domain administrator. This information includes:

> • The Activation Key itself and the number of device activations in use versus available devices. The key can be passed out to the users you want to activate eM Client. There is a handy "copy to clipboard" icon as well. Initially, you will see (0 of 3 Devices), but that will increment as people start using the key you pass out, and as you add device activations.

• The "Support" date shows when eM Client's complimentary "VIP support" will expire. eM Client Pro users are provided with 12 months of "VIP Support" directly from eM Client. At the end of the 12 months, VIP Support can be renewed as needed.

• "Version" information gives you the major version that's associated to the key. All minor updates to eM Client Pro users are available for free. Once a new major version is released, the license owner can purchase the upgrade to that major version, if they're so inclined.

In addition, a new email is sent to the domain administrator walking through the eM Client process AND to the address input for the "Owner email address". This email details how to access eM Client's License Manager.

Managing Activations

Once the domain administrator receives the license key, it can be distributed to users of the domain. Users will need to download eM Client for their particular platform, either Windows or MacOS . (Currently, eM Client is BETA testing mobile versions for Android and iOS.)

Once the first license is activated, it will appear on this page. Information about the activation is also displayed. The information includes:

• Account - The email address of the user who activated the license. This will be the account that's listed first in eM Client. Therefore, if multiple accounts are set up, this would be the one that appears at the top of the list of accounts in eM Client's Settings. Note: if N/A is displayed, this means the license was activated in an eM Client installation, but an account was set up WITHOUT email. For example, a user set up their account to only use chat (XMPP) or set it up using EWS or WebDAV and only set up calendars, contacts, or a both. In order for an email account to be listed it must be set up for email.

• Activated - The date and time the account was activated in eM Client.

• Last IP - The IP address used to activate the account.

• Last Version - The version of eM Client being used by that account.

• Activation State - Whether the account is Active or Inactive, meaning whether the account is using an eM Client activation or not.

Domain administrators also have the ability to activate or deactivate Accounts from this page. Simply select an account and use the Actions menu to perform the necessary action. It's also possible to use the right-click context menu on an account. (Deactivating licenses can take up to 24 hours based on how eM Client's licensing system processes license requests.)

eM Client License Manager

If more information is needed beyond what is provided on the eM Client Licenses page, an account is created in eM Client's License Manager for the organization. Using eM Client's License Manager it's possible to view additional information about each device activation, see deactivated users, see transactions associated to the license key, and much more. Accounts are created using a default password, so in order to gain access to License Manager, a password reset will be required. To do this, do the following:

- Go to eM Client's License Manager .
- Click on the Reset Password link.
- Enter the Organizational email.
- Submit the password reset request.

An email will be sent from eM Client to that address. It will contain a link that will allow you to reset your License Manager password.

eM Client License Manager Login

The password reset email that is sent also includes the User Group and User Name you will need when logging in to eM Client's License Manager and for requesting support from eM Client. It is strongly recommended that the information provided is kept somewhere that's accessible to those individuals who need it. *@

Purchasing Additional Device Activations

As mentioned, additional device activations can be purchased directly from eM Client at a 25% discount. To purchase additional activations simply click the Purchase button at the top of the eM Client Licenses page. Clicking that will take a domain administrator to a landing page on eM Client's website where additional device activations can be purchases. The activations are automatically discounted and added to the license key assigned to the domain. (As an added benefit, eM Client already discounts additional device activations, and the 25% discount available to SmarterMail users is ADDED to that discount!)

Once a purchase is complete, confirmations are sent to the Organizational email. Simply refreshing the page will display a new (X of Y Activations) line, showing the increase in available device activations, next to the Activation Key on the eM Client Licenses page.

Interface Diagrams

SmarterMail User Interface

To better understand the different areas of the user interface, please refer to the diagrams below.

Navigation

The navigation bar is where you navigate through the various pages of the webmail client. From left to right, they are:
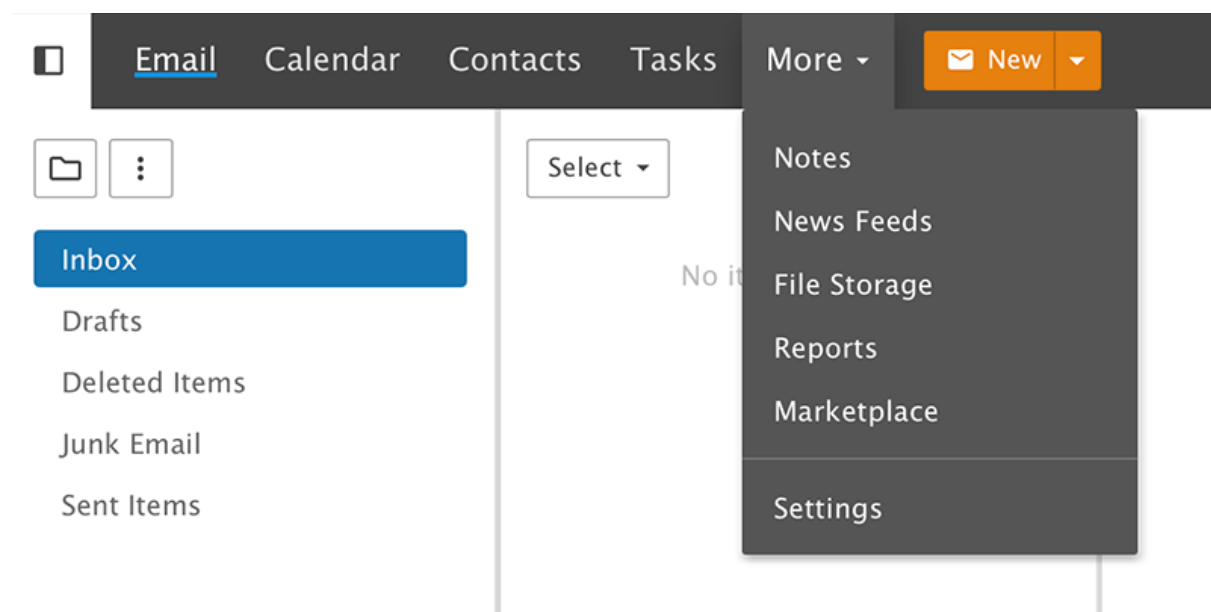
• Email

• Calendars

• Contacts

• Tasks

• More

• Notes

• Online Meetings

• News Feeds

• File Storage

• Reports

• Settings

• Marketplace

• Domain Reports (Domain Administrators only)

• Domain Settings (Domain Administrators only)

To the far right (not shown), the following is available:

• Advanced Search

• Live Chat

• Notifications

• Switch Theme

• User Icon/Dropdown

The New button is slightly unique: it enables webmail client users the ability to quickly create new messages, new appointments, new contacts, etc.
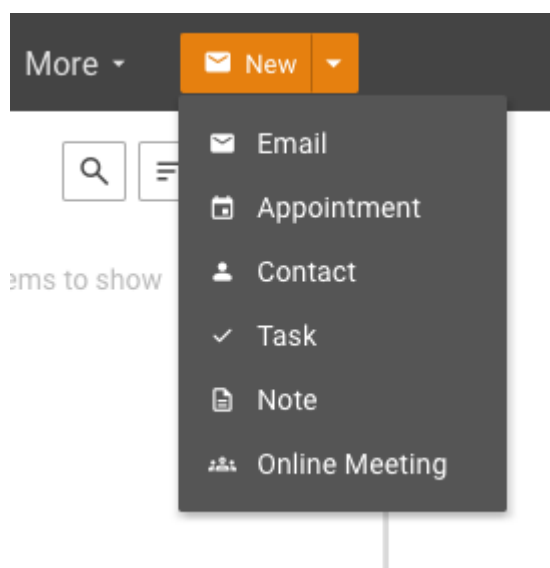
Folders List

The Folders list is used throughout SmarterMail and lists the various folders containing information pertaining to the section you're in. For example, when in Email, it lists all your default, custom and shared folders. In Calendars, it lists your default calendar as well as any secondary calendars that were created as well as shared calendars.

Image has no valid type.

Content Pane

The Content Pane is also used throughout SmarterMail and is where messages, contacts, reports, pages, etc. are presented to users.

Message List

When viewing your Inbox or any other folder in the Email section of SmarterMail, this is where all of the messages residing within the folder you're viewing are displayed.
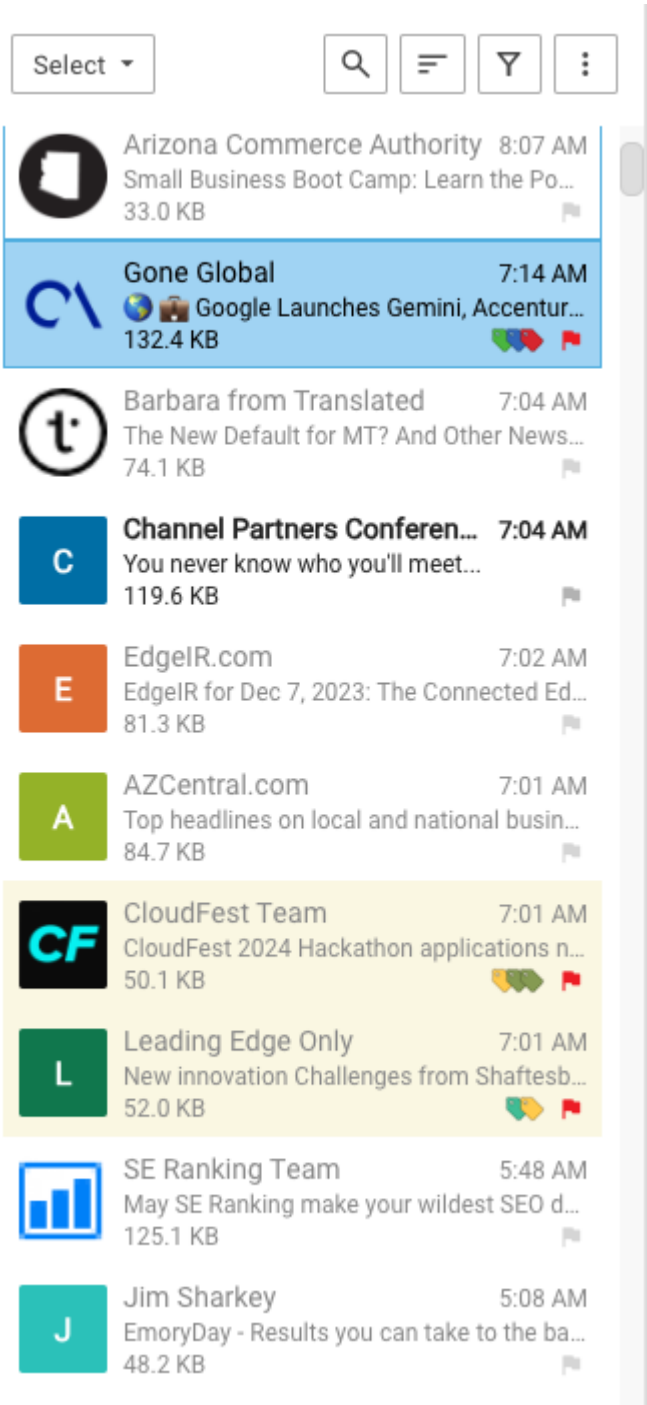
Interaction Buttons

Each section of SmarterMail has a number of buttons that can be used to interact with items within that section. Reply, Delete, Move to Junk, Mark, Actions (☐), Next Message, Previous Message and Pop-Out (This opens the message in a new window). are available The buttons available are based on the section you're viewing.

Concepts

Roles of SmarterMail

SmarterMail is a feature-rich Windows mail server that brings the power of enterprise-level functionality and collaboration to businesses and hosting environments. SmarterMail is powerful enough to be used as a complete mail system that performs all of the following roles from a single server. SmarterMail installations can also be used to perform specific functions on mail networks to enhance an existing infrastructure or to gain performance — whether you are running SmarterMail as your primary mail server or to support another mail server that is having difficulty performing under the current load.

As you will discover, SmarterMail can be used to fulfill a variety of roles that can be deployed for little to no cost. Adding SmarterMail in one — or several — of these roles will increase the stability and longevity of your email system.

Your Primary Mail Server

Use SmarterMail as your primary mail server and provide customers with an unmatched email service that includes industry standard connection methods like POP3, SMTP, and IMAP, as well as support for EAS and EWS/MAPI at the server level, offers multi-language support, and provides all of the features and functionality you expect from enterprise-level mail servers like Microsoft Exchange.

SmarterMail does this via a completely browser-based design, delivering all of the coordination, communication, and world-class collaboration functionality that you expect through an intuitive and modern web interface. Whether a standard user, a domain administrator, or a system administrator, you have every feature in SmarterMail right at your fingertips, using any mobile or desktop browser, and available from anywhere, at any time.

As an Inbound Gateway

Configure SmarterMail as your inbound gateway server and reduce the load on your primary server. In this role, SmarterMail can manage all inbound SMTP sessions and detect abuse and intrusion attempts. In addition, SmarterMail can also host third-party antivirus and antispam software, such as Declude or Trend Micro, and pre-scan messages prior to delivery to the primary mail server. Best of all, these functions can be integrated at no cost by downloading and installing SmarterMail Free Edition to operate as your inbound gateway server.

As an Outbound Gateway

In high-volume scenarios, SmarterMail can reduce primary server load by functioning as your outbound gateway server to spool outbound messages. One benefit of configuring SmarterMail in this role is that it functions as an effective method to combat blacklisting and can help ensure a quick system recovery. For example, if one of your IP addresses is blacklisted by an external email provider, you can resolve the issue by changing the IP address of the gateway server or turning off the gateway server until the IP address is removed from the blacklist (providing there are multiple gateway servers set up). In addition, this configuration of SmarterMail can run spam checks on outbound messages to prevent spam messages from being sent to remote servers, thereby reducing the likelihood of a blacklisted IP address. These functions can also be integrated at no cost by downloading and installing SmarterMail Free Edition to operate as your outgoing gateway device.

As a Backup MX Server

In the case that your primary mail server goes down, ensure that your users will continue to receive incoming email by setting up a backup MX server. When the primary mail server cannot be contacted, email servers on the Web will attempt delivery to the backup MX server. When the primary server comes back online, the backup MX server will deliver all held email.

As All of the Above

SmarterMail was built for a large-scale, multi-tenant environment: a shared web hosting company. Anyone familiar with multi-tenant environments knows they are taxing, from an employee perspective as well as a system resource perspective. Users demand performance, and administrators need tools to ensure the users get what they want. Knowing this, SmarterMail was built for efficiency, performance, security, and reliability — all the while knowing that it needed to be easy to use, and easier to manage and maintain.

As a result, SmarterMail can handle an immense amount of email, and can act as an inbound gateway, an outbound gateway, and provide enterprise-level communications services for users — all from a SINGLE installation.

As SmarterMail has grown, so has our commitment to what got us here: efficiency, performance, security, and reliability. Those goals PLUS building one of the most functional, and cost-effective, email and communications platforms available, one that rivals Microsoft Exchange — and BEATS it most cases.

SmarterMail and Microsoft Exchange An Administrative Comparison

Who Should Use This Document

This document provides a comparison of SmarterMail Enterprise mail server software and Microsoft's Exchange Enterprise mail server. It is designed specifically for server and system administrators and provides information on the hardware, software and licensing requirements of both products, with an overall cost breakdown in each category.

It is equally important to review the end user experience for both products as well. Therefore, please review the white paper SmarterMail and Microsoft Exchange: An End User Comparison for a more complete feature-by-feature comparison of both products from the end user's point of view.

For the purpose of the comparison in this document the following criteria were used:

> • Based on a small to medium business (SMB) utilizing multiple domains, potentially for multiple brands.
> • Up to 250 mailboxes populating the mail server. This is simply a user limit for the sake of comparison and in no way infers a maximum user limitation, either within Exchange or SmarterMail.
> • Accommodations for organizations wanting both webmail access as well as organizations wanting a mixture of webmail and standard desktop email clients.
> • Mobility using multiple mobile devices (e.g., Apple iPads and phones, Android tablets and phones).
> • Complete synchronization across a variety of mobile and desktop environments.

Overview

At first glance, comparing a mail solution against the historical significance of Microsoft's Exchange Server may seem like a rather daunting task. After all, a study in 2008 estimated that a full 65% of workers worldwide were using Microsoft's email server. However, at that time there was a lack of competitive products that offered comparable functionality. That is no longer the case, and once you start peeling layer upon layer of complexity away from the Exchange infrastructure, vulnerabilities begin to appear. This is especially true when you look at Exchange from an administrative standpoint.

With that in mind, there are several areas where SmarterMail Enterprise far surpasses Exchange Server — areas that are of vital importance to small businesses and server administrators alike:

> • Licensing — All of the software required comes with a cost, from the base operating system being used to the cost of the actual product and product licensing. As a result, cost can be high

on the list of priorities when planning out a new system or even a migration/change of an existing system.

• SmarterMail has a much smaller footprint and lower cost of entry and, as you'll see, a lower long-term cost as well. Beginning with the base operatins system, SmarterMail can run on any existing Windows Server license, just like Exchange. However, SmarterMail also runs on Linux, which removes the cost of Windows licensing. This is beneficial for customers looking to move, say, from Microsoft 365 to an on-premises solution.

• Requirements and planning — There are hardware and software considerations when planning to build out an email and messaging platform. Exchange is well known for its complexity and difficult planning and installation requirements.

• SmarterMail offers a simple set of requirements as far as hardware is concerned, and can easily support the criteria explained using one server for all domains and users, antispam and antivirus functionality, and more. With regards to administration, nothing more than basic server administration and implementation skills are necessary as SmarterMail has a single installation file and does not require any additional software, such as a Microsoft SQL or MySQL database. In addition, SmarterMail can be run in a Docker container. See the SmarterTools Docker Hub for more information.

• Management and Maintenance — Once the mail server is installed, someone needs to be able to monitor the day-to-day activity and health of the server, users need to be added or removed to domains, antispam or security settings need adjusted, and more. Being able to perform these tasks quickly, easily and from anywhere is extremely important.

• SmarterMail provides a simple and understandable set of management and maintenance tools built into an "access anywhere, at any time" web-based interface. In addition, SmarterMail offers a "Top-Down" administrations structure where system administrators can offload simple tasks, such as user creation and user settings management, to individual domain administrators.

• Backups/Restores — Storage and recovery capabilities of online communications is hugely important. What options are there and what are the costs?

• SmarterMail can be backed up and restored using standard backup and recovery technology, and the files and folders required for backup are easily identifiable and accessible, whether using something like Robocopy or any backup agent. No further investment in specialized hardware or software is needed.

Comparison of Licensing

From a licensing perspective, a clear and concise licensing structure makes it much easier to plan out both an initial installation as well as any migration. Taking this into account, is it better to require an

all-in-one licensing model or one that requires virtually each individual piece to have its own licensing requirement?

Price Comparison (Windows Only)	Exchange	SmarterMail
Windows	✗	✓
Linux	✗	✓
Docker	✗	✓
250 User License	$741.00	$900.00
CALs	$23,037.50	Not Applicable
Anti-Spam	Included	$375.00*
Anti-Virus	Included	$375.00*
Live Chat	Included	Included
MAPI	Included	$325.00
EWS	Included	Included
EAS (250)	Included	$1,425.00
Total Cost	$23,778.50	$3,400.00

Microsoft Exchange 2019 license with 250 Client Access licenses

250-User Enterprise License featuring Cyren Anti-Spam* and Cyren Zero-Hour Anti-Virus Protection*.

Server Licensing

First, let's look at simple server licensing costs. This is licensing solely for the mail server software that is installed. Remember, for the purposes of this comparison we are going to look at a business that requires up to 250 mailboxes.

> • Exchange — Exchange is $741.00 for the license alone. However, Exchange also requires Client Access Licenses (CALs) so individuals can connect to it. For 250 users, that's another $23,037.50. Then there's the cost of Windows licensing, which can be either a one-time cost or a monthly cost if the company is on Microsoft's Server Provider Licensing (SPLA).
> • SmarterMail — Enterprise licensing for 250 mailboxes is $900.00. However, additional add-ons are required to gain Exchange-like functionality: Microsoft Exchange ActiveSync for mobile synchronization, and Microsoft MAPI for true Outlook compatibility. Even with these add-ons, the overall cost of SmarterMail is a mere fraction of Exchange. Then factor in that SmarterMail can run on Linux. That eliminates any additional OS licensing!

Client Access Licensing

A CAL is simply what the name implies: it's a license required for a client — whether that is a user or a device — to access a server.

• Exchange — Requires user or device CALs, depending on how or what is connecting to the Exchange server.

• A user CAL is generally defined as a license for the person connecting, regardless of whether they connect via Microsoft Outlook, webmail or mobile device.

• A device CAL is defined as a license for each device that is connecting (e.g., desktop, mobile device, etc.).

• SmarterMail — Does not require individual licensing for each person or device that accesses a mailbox. In fact, you can buy a license that will accommodate the number of mailboxes you need — plus give you some room for growth. Whether you need 250 mailboxes, 500 mailboxes, 1,000 mailboxes or even an unlimited number, there is a licensing model to fit your need. SmarterTools even offers a fully-functional Enterprise license for 10 mailboxes that can be used indefinitely — either as a free trial or as a fully functioning mail server for a business.

Employee Expense

Employee expenses are somewhat subjective. With Exchange, you have a very complex infrastructure, requiring multiple server roles, high-end hardware and software, and extensive project planning and management. On the other hand, SmarterMail offers a much simpler installation requirement and footprint. On these merits alone, the employee expense incurred with just the installation of Exchange — not to mention the day-to-day management and maintenance of it — logically dictates that a very experienced and well-trained individual or group is required. This, in turn, equates to a higher cost.

With SmarterMail, an existing employee with a good grasp of server technologies and management skills is all that is required. That's how SmarterMail was built: with ease of use and ease of management in mind.

Comparison of Requirements and Planning

Rather than looking at the overall feature set of both products, let's take a close look at the requirements of both Exchange and SmarterMail.

Hardware

• Exchange — Generally requires separate servers for each server role in the Exchange setup. This is because Exchange requires several server roles, managing various parts of the platform. This could mean the need for multiple servers.

• SmarterMail — Has a very acceptable minimal set of hardware requirements. As there are no server roles to configure, a single server may be all that is required. In fact, SmarterMail can run on an existing server in a dual-use role. That is, SmarterMail can run on a web server or file server and doesn't require its own hardware to run. That's not to say that additional servers can't

be used: incoming and/or outgoing gateways, for example. However, a single server with a single install can be used for most small to medium-sized businesses.

Software

• Exchange — There is, of course, mail server licensing (either Standard or Enterprise) to consider. Additionally, Exchange requires Client Access Licenses (CALs) for each mailbox/user and in order to get security and antivirus, Enterprise CALs are required - at a substantially higher cost. And all needs to run within an Active Directory tree because Exchange requires the use of Microsoft's Active Directory for user management.

• SmarterMail — A simple purchase of the mail server is all that is required. Antivirus and antispam are included with SmarterMail Enterprise, but there are options to increase coverage with Message Sniffer and other products. In addition, SmarterMail does NOT require any additional roles or the use of Active Directory, though it CAN integrate with Active Directory if needed.

Planning the Architecture

• Exchange — As mentioned, Exchange has multiple different server roles (edge transport, hub transport, mailbox, client, etc.) running within an Active Directory tree. As noted earlier, each role may require separate servers. That means extensive planning is required, from Active Directory on up to actual Exchange server installation.

• SmarterMail — Considering hardware and software requirements, one server can act as the mail server and also run any necessary antispam and antivirus add-ons. Furthermore, SmarterMail also does not require Active Directory, although it can integrate into an Active Directory tree so single-authentication can be used throughout an existing infrastructure. It should be noted, however, that the lack of an Active Directory requirement may reduce the time needed to plan out an implementation and installation strategy.

Management and Maintenance

With any software implementation, system and server administrators are challenged with keeping tabs on the mail server(s) hardware and software. Furthermore, there are day-to-day tasks, things like user management, domain management, management of blacklists and content filters, and much more.

Management and Maintenance

• Exchange — As Exchange runs on a server OS, the majority of management and maintenance of the server has to be performed on the server. That means administrators generally have to remote or console into the server. In addition, management occurs via an Exchange tool that plugs into the Microsoft Management Console (MMC). If an administrator is offsite, these connections must occur through secured VPN. All of this can decrease the connection speed and

therefore increase the time it takes to complete even routine maintenance tasks. Besides, it's a somewhat convoluted and complex setup.

• SmarterMail — SmarterMail offers a powerful and extremely accessible web-based administrative front end. With the ability to set up different roles, and assign permissions based on those roles, the day-to-day management of users and domains can be distributed, leaving system administrators free to perform system duties, and domain and user management up to domain administrators. It's also possible to set up multiple, different system administrator accounts, so no one has to share logins, resulting in better tracking and change management. SmarterMail administration is fast, is easy, and it can be accomplished on-site or remotely using any standard browser. SSL connections are available, and you can even limit access to the admin area by specific IP, further enhancing security. And unlike the Exchange plug-in for the MMC, SmarterMail's administrators have access to numerous reports, from inbound/outbound spam to server health, disk space usage to abuse detection.

Learning Curve

• Exchange — When looking at everything that goes into planning an Exchange installation, there's no doubt the people planning and carrying out the installation are professionals. This, in turn, means they significantly factor into the costs associated with that installation. In addition, there are possibly increased employee costs for the level of individual necessary to manage and maintain an Exchange infrastructure. Most system and server administrators for Exchange have years of experience and untold hours of training and product-specific education under their belts. Therefore, they won't come cheap.

• SmarterMail — SmarterMail runs in a very simple, very easy to manage and maintain environment that is not unlike any base server installation. Therefore, a company can get by with existing staff and existing system and server administrators. The learning curve is much easier to manage with SmarterMail as standard server administration knowledge is about all that is required.

Backups and Restores

Your data is only as good as its most recent available backup. And even then, a backup isn't of any use unless it is recoverable and restorable. However, backups and restores of data do not have to be complex and expensive initiatives.

• Exchange — Exchange can be backed up with most existing backup technologies. However, its one big exemption is that Exchange requires a separate and specialized backup agent in order to be able to back up mail files. Anyone who has priced these agents out knows this can be a substantial expense.

• SmarterMail — SmarterMail can be backed up with any existing backup technology and does

NOT require the use of a separate, specialized agent. This reduces the costs of backup and restoration and also is one less thing for administrators to manage and maintain on the mail server. In addition, SmarterMail was built with ease of administration and management for the hosting industry. That means it was built to reduce the burden on backup systems.

Summary

When you look at all of the differences between Exchange and SmarterMail a few things really stand out:

• The planning necessary for an implementation of Exchange is far more detailed and involved than what is necessary for an installation of SmarterMail. With Exchange, you don't simply set up a web server and a database. Things like Active Directory trees need to be considered, plus the necessity of various server roles and how to configure each role. Then there is figuring out what can you combine into a single server, planning how to configure the server connections and interactions, etc. Complexity is Exchange's strong point; simplicity and ease-of-use are SmarterMail's.

• Licensing is generally a sore spot with most software implementations. However, SmarterMail gives system administrators a high-level of flexibility and power, but with substantially less cost than Exchange. Looking at the comparison tables alone demonstrates a 5X to 11X savings with SmarterMail over Exchange.

• Requirements, both from a hardware and software standpoint, again point to SmarterMail being a much wiser investment than Exchange. Minimal server OS concerns, no Active Directory (unless you need it), and much more flexible hardware options all place SmarterMail above Exchange.

• When looking at maintenance and management, plus the learning curve required, SmarterMail again gets the nod. Without the need for lengthy training or education, and simple server administration experience all that is required, SmarterMail is easily administrated by existing employees, again saving time and money.

Trust and Availability

There's no doubt Microsoft has the name. They've been around a long time and have a long history of building quality software and being on the leading edge of technology, especially when it comes to providing a robust and feature-rich email solution. However, becoming one of the largest, if not THE largest, software and services company doesn't come without some sacrifice. These sacrifices tend towards offering reliable, accessible access to support and customer service, at least affordable access to these critical needs.

That's where SmarterTools comes in.

Over the years SmarterTools has grown to over 15 million users but still sees each user as important. They have grown through investment in products and development versus in advertising and marketing, building SmarterMail into one of the most popular and respected mail servers on the market. They realize how safe, secure and reliable communication is vital to each and every user of their product. That's why SmarterTools offers services that cater directly to their customer base:

- • Access to LIVE tech support, 24/7/365
- • Upgrade and installation services
- • A popular, free public community to interact with support, developers, and fellow users
- • Responsiveness to customers that often leads to product enhancements

While it may be true SmarterTools doesn't have the name recognition as Microsoft, what is certainly not up for debate is SmarterTools' commitment to their customers, to their products, and to their desire to create the most reliable and secure mail server solution on the market.

Taking all of this into consideration, it may not be a question of "why move to SmarterMail from Exchange," or "why choose SmarterMail over Exchange," but more a question of a "why not ?"

SmarterMail and Microsoft Exchange An End User Comparison

Who Should Use This Document

This document provides a comparison of SmarterMail Enterprise mail server software and Microsoft's Exchange Enterprise mail server. The comparison is from the end user's point of view.

It is equally important to review the system and server administration experience for both products as well. Therefore, please review the white paper SmarterMail and Microsoft Exchange: An Administrative Comparison for a more complete comparison of both products from the administrative point of view.

For the purpose of any comparisons in this document the following criteria were used:

- • Based on a small to medium business (SMB) utilizing multiple domains, potentially for multiple brands.
- • Up to 250 mailboxes populating the mail server.
- • Accommodations for organizations wanting a mix of email clients: webmail, desktop, and mobile clients.
- • Complete synchronization for multiple mobile devices across various brands/operating systems. (I.e., iOS and Android.)
- • Complete synchronization across a variety of desktop environments. (E.g., a mixture of Windows and macOS desktops.)

Overview

Email is the cornerstone of modern communication. In fact, even after (or in spite of) the growth of social media like X (Formally known as Twitter) and Facebook, email is still considered the "Killer App." The is because email is ubiquitous, and in order to open a social media account you need an email address. As such, it is of vital importance that email communication is as secure, stable, powerful and versatile as possible. With SmarterMail, you get tools to not only make your email experience more enjoyable, but safer and more secure as well.

In addition to protecting users, SmarterMail offers a flexible and versatile set of tools for users to access email. These tools include an advanced webmail interface that can be used with any web browser, synchronization protocols such as CalDAV, CardDAV, and Microsoft EAS, EWS and native integration of MAPI, the protocol that powers Outlook and Exchange. All of this means users can synchronize any email client on their mobile devices, like the Samsung Galaxy line and Apple's iPhone and iPad, plus integrate their desktop clients such as Microsoft Outlook, Microsoft Outlook for Mac, Apple Mail and eM Client.

Of course, Microsoft's Exchange offers all of this as well. However, once you start comparing the two products it is evident that SmarterMail Enterprise far surpasses Exchange Server in many areas:

• Collaboration — This means the ability to share things like your daily calendar, your contacts, and even your tasks. From a calendar standpoint, equally important is the ability to set up meetings and check the availability of your friends and colleagues.

• SmarterMail contains virtually identical collaboration tools as Microsoft Exchange and adds a few extra, such as file storage and file sharing.

• Security and Antivirus — Computer/infrastructure security from online threats is a big concern, so this section discusses included options as well as third-party integration.

• SmarterMail offers powerful antivirus measures without the need to purchase third-party add-ons. However, powerful options are available, and SmarterMail can easily integrate with any third-party service or device.

• Antispam — According to Symantec's MessageLabs, spam is responsible for over 88% of all email. Options to combat these numbers, both included as well as third-party integration, are discussed in this section.

• SmarterMail offers industry-standard antispam measures upon install without the need to purchase third-party add-ons (although you can integrate third-party solutions, if desired), with over 97% of spam blocked with a default installation.

• Synchronization and Mobility — The ability to access your email, contacts, calendars, tasks, and notes, wherever you and and on whatever device you're using, is critical. This is especially

true now as more and more people are working from home or working away from the office. Being able to read and reply to emails from a phone, laptop, tablet, and desktop ensures that you have the ability to communicate, and collaborate, at any time.

• SmarterMail supports all major protocols for syncing mobile devices and desktops/laptops and actually beats Exchange in some cases by supporting multiple synchronization options.
• Access to Information and Email Migration — Having access to information is crucial in today's fast-paced environment. You need to know what's going on in the world, you need to keep track of contacts and your interaction with them, and you need to know your own status within your organization: your usage stats, your available space, both for your email as well as for your files, and much more.

• SmarterMail offers a number of "push" type technologies that give you the ability to subscribe and manage RSS feeds, reporting options of virtually all of your email usage, detailed contact information, and a quick and easy way to migrate your files, contacts, calendars and emails into SmarterMail—all within the robust webmail interface, giving you access to this information anytime, anywhere.

Collaboration

Collaboration is simply the ability to share information with friends and co-workers, from your calendar to your contacts. Additional features include the ability to schedule appointments with people, check their free-busy availability, reserve conference rooms, modify shared tasks, share contacts and "virtual cards" (vCards) and more.

Shared Calendars, Contacts, Tasks and Notes

• Exchange — One of the more notable and powerful features Microsoft introduced with Exchange is the ability to share calendars, contacts, notes and tasks with other people in an organization.
• SmarterMail — SmarterMail also offers sharing of calendars, contacts, tasks and notes. However, SmarterMail offers a way to store documents and other files and link to those in emails and tasks so others can access them as well. As an aside, while you can share links to the files, you don't have to, making SmarterMail's file storage feature even more versatile.

Security and Antivirus

Everyone wants their email to be secure—secure from virus infection, free from phishing attempts, and free from malware and dangerous attachments. Additionally, no one wants their mail servers used for spamming or for attacking others as that can lead to untold hours of downtime once unwanted activity is detected and dealt with—both internally and by those affected.

Antivirus

• Exchange — Does NOT contain any antivirus protection out of the box. That means that it must be added after the fact and can end up costing more money. At the very least, the Enterprise Client Access Licenses (CALs) are needed in order to use Microsoft's Forefront Security Suite.

• SmarterMail — Each installation of SmarterMail contains industry standard antivirus protection through Clam AV, and integrates with Windows Defender, which is generally already installed and in use on a Windows Server. This is all included at NO EXTRA COST to users, and generally runs in the background without users every knowing it. SmarterMail also offers the ability to add in a number of other antivirus applications and services.

Other Security Features

• Exchange — Exchange offers the ability to send/receive email using Secure Socket Layers (SSL), offers Active Directory authentication (actually, Active Directory is required for Exchange), and SMTP authentication by domain. This latter option means that a user must provide an authenticated username and password in order to send email from the server.

• SmarterMail — SmarterMail includes all of the features listed above, but also takes things further by offering email administrators a large number of whitelisting/blacklisting features, brute force detection, automatic denial of service (DoS) prevention, automatic harvest attack prevention and more. This is an added layer of security that protects users from unwanted events hampering communication.

Antispam

Spam is, without a doubt, the scourge of the internet. In 2012, researchers at Microsoft and Google estimated that spam costs society up to $20 billion, a figure comparable to the GDP of Bolivia 4 . Factor in the time and money spent by people during their off hours, and that number can grow significantly.

Available Antispam

• Exchange — Just as with antivirus, Exchange does not offer any antispam protection out of the box for a user's inbox. It requires a third-party solution or Enterprise CAL. That's not to say Exchange doesn't offer antispam measures for the server and for sending email. It does offer measures such as domain keys and DKIM, trusted senders, SPF records, etc.

• SmarterMail — Similar to its antivirus protection, SmarterMail offers industry-standard spam measures on a variety of fronts. For example, SmarterMail supports more than 24 separate industry black lists as well as SPF and DKIM. In addition, SmarterMail offers further protection through a proprietary pattern matching engine built upon the SpamAssassin technology and

support for remote SpamAssassin servers at no additional cost to end users. SmarterMail also supports Message Sniffer which can be included for a minimal yearly license fee.

Mobility and Synchronization

With more and more of today's workforce occupying home offices or finding themselves on the go, having an email system that can not only accommodate mobile devices—beyond simply smartphones and including iPads and Android tablets—is essential. In addition, people no longer just text or email each other, they share photos and documents as well.

Mobility and Synchronization

• Exchange — Exchange ActiveSync (EAS) is a Microsoft technology that is built into Exchange, giving users on the domain the ability to share contacts, calendars, notes and tasks and synchronize it all with their mobile device, or with desktop email clients that utilize EAS, such as Windows Mail, People, Calendar, etc.

• SmarterMail — SmarterMail also supports Exchange ActiveSync and Exchange Web Services as an optional add-ons. However, SmarterMail also supports a variety of open source synchronization technologies and specific contact and calendar protocols like CardDAV and CalDAV. Therefore, while SmarterMail supports EAS and EWS as a best-in-breed paid add-ons, they may not be required in some situations. In addition, SmarterMail's webmail client is extremely robust and offers a fully functional email interface for mobile and remote users that is accessible from anywhere there is an internet connection.

Access to Information and Email Migration

In addition to email, users expect a single interface for a variety of other communications mechanisms. In addition, transitioning from one mail system to another and the movement of email and contacts can be difficult at best. Both the gathering of information—whether in the form of news feeds or contact information—and the migration of your email communication should be as seamless and pain-free as possible.

• Exchange — The use of Outlook with Exchange means you have a single source for your RSS reader (for reading subscriptions to blogs and news outlets). The feeds you subscribe to from within Outlook translate to your Web App access as well. However, you can't subscribe to RSS feeds from Outlook Web App—those feeds can only be managed from with the Outlook client. In addition, using Outlook gives you the ability to see a variety of information about your contacts. Again, however, that information is only available from within the Outlook client. Also, what if you wanted to know about your email usage patterns? What about the amount of disk space you used compared to the amount you have available? These reports are not available, either from Outlook Web or from the Outlook client. And what if you wanted to be

notified if a particular contact sent you an email? What if you wanted to know when your mailbox reached a certain disk limit? None of that information is available from Exchange. Yes, you can create rules in Exchange and Outlook, but those are for email management, not email notification. Finally, while Exchange itself offers the ability to migrate email accounts from one system to another, this isn't possible for end users and must be accomplished by an administrator.

• SmarterMail — SmarterMail brings power to the webmail interface with the ability to subscribe and manage your RSS feeds right from a browser window. In addition, if you want to know your usage stats, that information is at your fingertips plus information on your traffic stats, POP/IMAP usage, any errors you've received—all of this across any date range that you can manage and set. As for contact info, SmarterMail gives you access to a number of related items when you do an advanced search for a contact's email address: recent emails sent to and from that contact, plus messages that included you AND the contact, any appointments, and a list of tasks and/or notes that include the contact. As for events, SmarterMail has them: you can set up events on collaboration features, email or even your disk usage. Events let you know when something occurs, so you have the information you want when you need it. Finally, there are the migration tools. Once your user is set up in SmarterMail, you have the ability to manage the migration of email to that mailbox, regardless of whether it is from Gmail, Hotmail or any other POP/IMAP account. The tools are yours to use at your convenience. And don't forget: all of this is available from an access anywhere, at any time browser-based interface. You're not restricted to a single email client that resides on a computer you may, or may not, have access to.

Summary

When you look at all of the differences between Exchange and SmarterMail a few things really stand out:

• The collaboration features match on practically a one-to-one basis. Therefore, it amounts to the branding issue—just like people buy Nike shoes over Adidas. The sneakers are practically identical, but people just recognize the Nike brand since it's associated with so many sports figures.

• SmarterMail offers antispam and antivirus at no additional cost upon installation. While you can use add-on services and applications (like the wonderful products from Message Sniffer and other companies), there's no need.

• Mobility and synchronization are the future, and SmarterMail is there.

• The information is right there, at your fingertips—from anywhere, at any time. Whether it's information on who has sent you what, or if you need to find that spreadsheet that the CMO

sent; whether you want to know when you reach 75% of your disk space capacity or need access to your RSS feeds, SmarterMail offers it all right from your Web browser.

Trust and Availability

There's no doubt Microsoft has the name. They've been around a long time, and have a long history of building quality software and being on the leading edge of technology, especially when it comes to providing a robust and feature-rich email solution. However, becoming one of the largest, if not the largest, software and services company doesn't come without some sacrifice. These sacrifices tend towards giving users access to support and customer service — at least affordable access to these critical needs.

That's where SmarterTools comes in.

Over the last eight years, SmarterTools has grown to over 15 million users, but still sees each user as important. They have grown through investment in products and development versus in advertising and marketing, building SmarterMail into one of the most popular and respected mail servers on the market. They realize how safe, secure and reliable communication is vital to each and every user of their product. That's why SmarterTools offers services that cater directly to their customer base:

- Access to LIVE tech support, 24/7/365
- Upgrade and installation services
- A popular, free public community to interact with support, developers, and fellow users
- Responsiveness to customers that often leads to product enhancements

While it may be true SmarterTools doesn't have the name recognition as Microsoft, what is certainly not up for debate is SmarterTools' commitment to their customers, to their products, and to their desire to create the most reliable and secure mail server solution on the market.

Taking all of this into consideration, it may not be a question of "why move to SmarterMail from Exchange," or "why choose SmarterMail over Exchange," but more a question of "why not ?"

1 https://www.pewresearch.org/internet/fact-sheet/mobile/

2 http://www.messagelabs.com/intelligence.aspx

3 http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx

4 The Economics of Spam, Justin M. Rao and David H. Reiley

Help for Users & Domain Administrators

Logging in to Webmail

SmarterMail users can access SmarterMail using any mobile or desktop web browser in addition to connecting their mailbox to an email client such as Microsoft Outlook for Windows or Mac, Apple Mail or even using the email clients that come standard on most mobile devices. The major advantage of using the webmail interface, however, is that users can log in to their SmarterMail mailbox from any computer or mobile device with internet access, from anywhere in the world.

To log in to the SmarterMail web interface, users will need to obtain the appropriate link and login information (Username and password) from their domain administrator or system administrator. Generally, the link will take the form of a standard email URL such as https://mail.example.com, though it may vary based on how your hosting company, ISP or administrator has it set up.
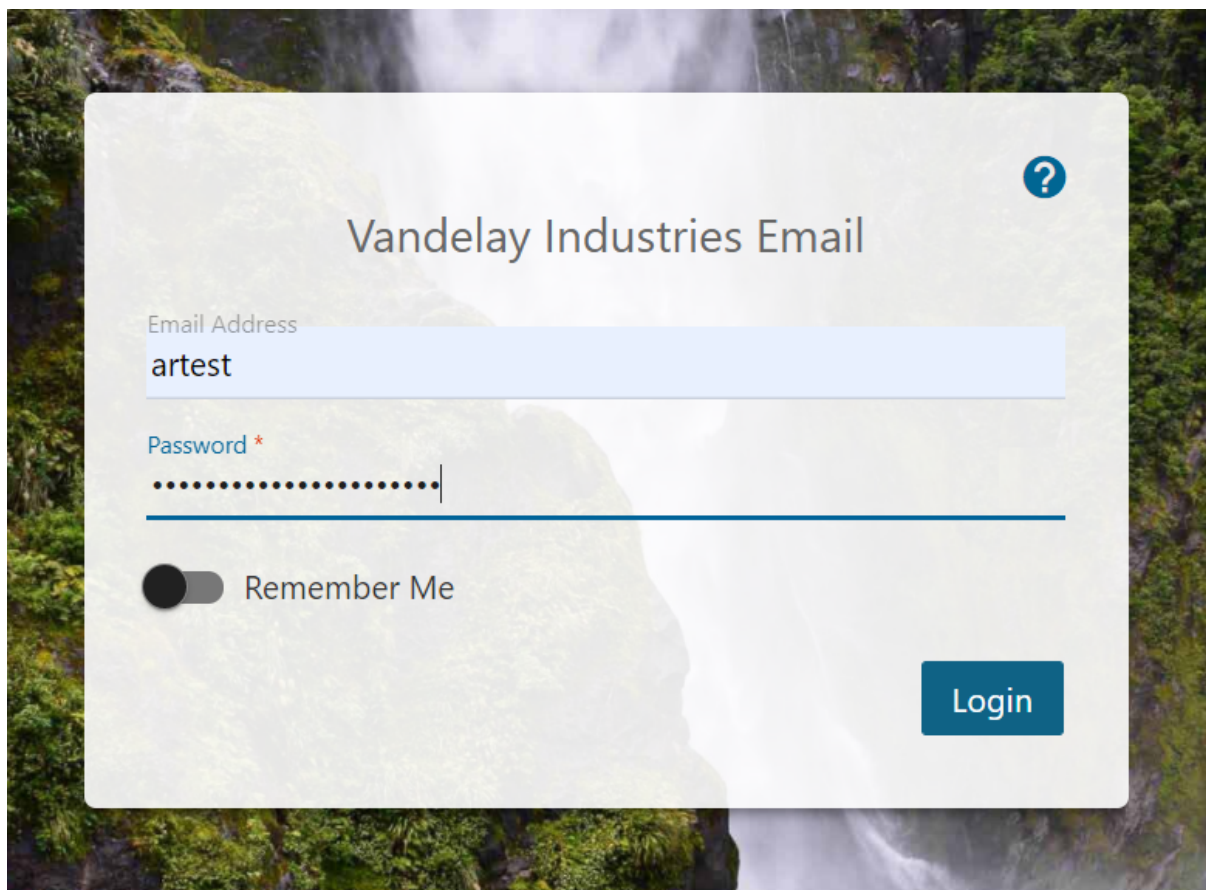
On your initial log in, you're presented with the Getting Started page. Here, you'll adjust some basic settings for your webmail account. These include:

- Theme - Whether you want your webmail to be displayed in a Light or Dark Theme.
- Time Zone - This is generally set by the domain administrator for your account, but it can be changed as needed on your initial login, as well as at any time by adjusting your Preferences.

• Country - The country you're in. This will, more than likely, follow your Time Zone setting.

• Recovery Email Address - This is a backup email address that can be used for password resets as well as for Two-Step Authentication, should that ever be enabled for your account.

At the final step of logging in, SmarterMail informs you about the importance of browser notifications. Enabling browser notifications will display calendar reminders, toast notifications for new emails, group chat notifications and more.

Once all this is complete, you will be logged into your SmarterMail mailbox and your Inbox will be displayed. If you have trouble logging in or experience issues with your email account, contact your email provider for troubleshooting help. The email provider is usually the owner of the domain or the person who set up your email for you, like your company's IT person, website administrator or hosting company.

Staying Logged In

To stay logged in to SmarterMail even after closing the browser, be sure to enable Remember Me . This will allow SmarterMail to encrypt the email address and password and will automatically log you in the next time you visit your webmail URL. Note: Browser cookies must be enabled for this feature to work. In addition, SmarterTools does not recommend selecting this option if you use a public or shared computer or device.

Synchronizing with SmarterMail

Overview

SmarterMail is a powerful collaboration mail server that supports the synchronization of calendars, tasks, notes, and contacts on desktop applications like Microsoft Outlook and over-the-air synchronization for most popular mobile devices.

It should be noted that synchronization capabilities may vary depending on the edition of SmarterMail that you are using:

• For full synchronization capabilities, SmarterTools recommends upgrading to SmarterMail Enterprise. SmarterMail Enterprise users have the ability to synchronize their mailboxes using any of the protocols discussed in this document.

• SmarterMail Professional users can download their email using IMAP or POP3 retrieval, and sync calendars and contacts using free protocols like CalDAV and CardDAV. However, they cannot sync calendars, contacts, tasks or notes using either EAS or MAPI/EWS and so miss out on a more complete user experience.

• SmarterMail Free users have the ability to synchronize their mailboxes using any of the

protocols discussed in this document except EAS and MAPI/EWS, which are only available as add-ons to SmarterMail Enterprise.

For information on how to sync a specific device or client to SmarterMail please go to the Desktop and Mobile Synchronization section of the SmarterTools knowledge base . That section of the knowledge base contains a number of articles that offer step-by-step instructions that cover things such as connecting Outlook 2019 to a MAPI mailbox, using Autodiscover on Android devices, setting up Adium with XMPP and much more.

This document covers the synchronization methods and processes for the following applications and devices:

- macOS

- Contacts
- Calendar (iCal)
- Apple Mail
- Microsoft Windows 11

- Windows Mail
- People
- Calendar
- Cross Platform Options

- Microsoft Outlook
- eM Client
- Mozilla Thunderbird
- Mobile Devices

- Apple iOS
- Google Android Note: This is not an exhaustive list of all compatible applications and mobile devices. SmarterTools recommends contacting the manufacturer for details regarding the available synchronization protocols for applications and/or mobile devices not listed in this document.

Who Should Use This Document

This document is intended to be used in conjunction with the SmarterMail Online Help, Knowledge Base articles (KBs), and other SmarterTools reference sources as part of an overall solution. It should be used by:

• Hosting companies, Internet Service Providers (ISPs) and IT professionals as part of a complete SmarterMail communications solution for their customers
• Individual users of SmarterMail seeking to maximize the functionality and features of the SmarterMail account

Synchronization Protocols

SmarterMail uses multiple synchronization technologies to sync mailbox items with email clients and mobile devices:

• EAS is an optional add-on that syncs SmarterMail mailboxes, calendars, contacts — including contact pictures — with mobile devices as well as the default clients installed with Windows 10/11, such as Windows Mail, Calendars, and People.
• MAPI/EWS are optional add-ons that sync SmarterMail messages, contacts, calendars and tasks to third-party email clients that support the protocol, including Microsoft Outlook 2016 and above for Windows, Outlook for Mac, Apple Mail and eM Client. SmarterMail is the ONLY mail server on the market, other than Microsoft Exchange, that fully supports the MAPI protocol. As a result, Microsoft Outlook users can get the same level of features and functionality they do with Microsoft Exchange when using SmarterMail and MAPI/EWS.
• CalDAV is an extension of the WebDAV protocol that syncs SmarterMail calendars natively with Macs, iPads, iPhones, Thunderbird, and other devices/applications that use the technology. Note that some Android devices require the use of third-party apps that support CalDAV. More information on CalDAV implementations can be found by reviewing Implementations of CalDAV and CardDAV .
• CardDAV is an extension of the WebDAV protocol that syncs SmarterMail contacts — including contact pictures — natively with Macs, iPads, iPhones, and other devices/applications that use the technology. Note that some Android devices require the use of third-party apps that support CardDAV. More information on CardDAV implementations can be found by reviewing Implementations of CalDAV and CardDAV .
• Add to Outlook is a synchronization method based on Microsoft's Sharepoint platform. However, Microsoft no longer supports the synchronization features within SharePoint that are used by the Add to Outlook connector. Therefore, Add to Outlook is becoming less and less secure, and less and less reliable as there is no more assistance from Microsoft for it. As a result, Add to Outlook is offered "As Is". For a more feature-rich experience, EAS (for mobile devices and Windows Mail) or MAPI/EWS (for Outlook for Mac or Windows, and Apple Mail) should be used.

Synchronized Devices

SmarterMail makes it easy to view the devices and protocols used to synchronize your mailbox to desktop and mobile clients. The Connectivity page, available in a user's Settings area, shows users a variety of information about the devices that are synced to their accounts, including the last successful synchronization. Users also have the ability to reset the synchronization state of devices on the Synchronized Devices card.

Desktop Applications

SmarterMail supports synchronization with many desktop applications and email clients, including:

- Apple Contacts
- Apple Calendar
- Apple Mail
- Windows Mail
- Windows Calendar
- Windows People
- Microsoft Outlook
- eM Client
- Mozilla Thunderbird

macOS

macOS is the primary operating system for the MacBook, Mac mini, iMac and Mac Pro lines of desktops and laptops.

Apple Contacts

Apple Contacts is the default application for macOS users built for managing contact data. It is intended to be used in conjunction with Apple's Mail and Calendar programs to provide Mac users with full email, calendar, and contact management.

MAPI/EWS

The MAPI/EWS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can use EWS to sync contact data with Apple Contacts on computers running Mac OS 10.6 and above.

CardDAV

Users can synchronize their SmarterMail contacts — including contact pictures — with Address Book using EWS or the CardDAV protocol. Support for CardDAV is built into both products, so there is no need to download and install additional applications to sync contact data.

For more information, refer to our Knowledge Base.

Apple Calendar

Apple Calendar is the default application for macOS users built for managing calendar data. It is intended to be used in conjunction with Apple's Mail and Address Book programs to provide Mac users with full email, calendar, and contact management.

MAPI/EWS

The MAPI/EWS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can use EWS to sync calendar data with Apple Calendar on computers running Mac OS 10.6 and above.

CalDAV

Users can synchronize their SmarterMail calendars with iCal using the CalDAV protocol. Support for CalDAV is built into both products, so there is no need to download and install additional applications to sync calendar data. For more information, refer to our Knowledge Base.

Apple Mail

Apple Mail is the default email client for macOS users. It is intended to be used in conjunction with Apple's Address Book and iCal programs to provide Mac users with full email, calendar, and contact management.

MAPI/EWS

The MAPI/EWS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can use EWS to sync messages with Apple Mail on computers running Mac OS 10.6 or later.

Once the MAPI/EWS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the domain. For more information, see the Licensing and Activation page of our help documentation.

Once the add-on is activated for the domain, users can sync to Apple Mail using the protocol. For more information, refer to the KB article How To Synchronize SmarterMail with Apple Mail Using MAPI/EWS .

Message Retrieval

For SmarterMail users with MAPI/EWS, messages will automatically be synchronized with Apple Mail. SmarterMail users without the MAPI/EWS option should set up an account within Apple Mail using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP IDLE is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail. That is, unless you have the option to leave the messages on the server.

Microsoft Windows Mail, People, Calendar

Windows 10/11 is the latest operating system offered by Microsoft that is available for a variety of desktops, laptops and the Microsoft Surface tablet. Windows includes an email client (Mail) as well as both calendar (Calendar) and contacts (People) applications as part of its default installation, similar to those same features offered by Apple's operating system.

Windows Mail

Windows Mail is an email client that comes pre-installed with Windows. It allows users to set up accounts using a variety of methods.

EAS

The EAS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, EAS uses direct push technology to sync email, calendars, and contacts in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Windows Mail.

With the release of Windows, Microsoft integrated EAS with the Windows Mail application that comes as part of the Windows installation. Therefore, administrators and end users can Windows Mail using the EAS add-on as well as via IMAP or POP. note: EAS is not supported for use with any version of Outlook.

Once the EAS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article How To Activate EAS .

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding EAS to specific mailboxes. For more information, refer to the KB article How To Configure IIS for EAS .

Message Retrieval

For SmarterMail users with EAS, messages will automatically be synchronized with Windows Mail. SmarterMail users without the EAS option should set up an account within Windows Mail using either IMAP or POP3, where possible.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP IDLE is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail. note: If you have enabled Outlook to keep messages on the server, you will be able to access your messages and folders from any computer via the SmarterMail Web interface or your mobile device.

Windows People

Windows People is a contacts system that comes pre-installed with Windows. It allows users to set up contacts within Windows that can be used for a variety of purposes (e.g., emailing).

EAS

The EAS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, EAS uses direct push technology to sync email, calendars, and contacts — including contact pictures — in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Windows Mail.

With the release of Windows 10, Microsoft integrated EAS with the Windows Mail, People and Calendar applications that come as part of the Windows installation. Therefore, administrators and end users can set up Windows Mail using the EAS add-on as well as via IMAP or POP.

Once the EAS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article How To Activate EAS .

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding EAS to specific mailboxes. For more information, refer to the KB article How To Configure IIS for EAS .

Windows Calendar

Windows Calendar is a calendar application that comes pre-installed with Windows. It allows users to set up calendars within Windows that can be used for a variety of purposes (e.g., keeping track of appointments).

EAS

The EAS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, EAS uses direct push technology to sync email, calendars, and contacts in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Windows Mail.

Once the EAS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article How to Activate EAS .

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding EAS to specific mailboxes. For more information, refer to the KB article How To Configure IIS for EAS .

Cross Platform Options

Microsoft Outlook

Microsoft Outlook is an email client developed by Microsoft, Inc. for managing messages, contacts, notes, tasks, and appointments and is commonly distributed as part of the Microsoft Office suite. Outlook is offered on both the Windows and macOS platforms. SmarterMail supports synchronization of email, contacts, calendars, tasks and notes both on Windows and macOS.

MAPI/EWS

The MAPI/EWS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can currently use MAPI/EWS to sync messages, contacts, calendars and tasks with Outlook from Microsoft 365 and Outlook 2016 and above for both

Windows and Mac, and Apple Mail. note: The MAPI/EWS bundle is comprised of 2 different protocols: Outlook for Windows connects using MAPI while Outlook for Mac connects using EWS.

Once the MAPI/EWS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the domain.

Add to Outlook

The Add to Outlook (Sharepoint Sync) feature allows for two-way synchronization of calendars, contacts (but not contact pictures) and tasks with Outlook 2007 or higher, including a user's shared resources. Calendars and contacts shared at the domain level are not supported. For more information, refer to the KB article How To Synchronize SmarterMail with Outlook Using the Add to Outlook Feature . However, Sharepoint Sync does not support notification features, so items like SmarterMail calendar reminders will not be available within Outlook. For full integration, EAS (for mobile devices and Outlook 13 and above for Windows) or EWS (for Outlook for Mac and Apple Mail) should be used.

Message Retrieval

For SmarterMail users with MAPI/EWS, messages will automatically be synchronized with Outlook. SmarterMail users without the MAPI/EWS option should set up an account within Outlook using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP IDLE is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail. note: If you have enabled Outlook to keep messages on the server, you will be able to access your messages and folders from any computer via the SmarterMail Web interface or your mobile device.)

eM Client

eM Client is a cross-platform client for managing messages, contacts, notes, tasks, and appointments, and includes an integrated XMPP chat client. eM Client is offered on both the Windows and macOS platforms. SmarterMail supports synchronization of email, contacts, calendars, tasks and notes, as well as live chat, on both on Windows and OS X.

MAPI/EWS

The MAPI/EWS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can currently use MAPI/EWS to sync messages, contacts, calendars and tasks with eM Client for both Windows and Mac. The chat client that comes with eM Client uses the XMPP protocol.

Once the MAPI/EWS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the domain.

Message Retrieval

For SmarterMail users with MAPI/EWS, messages will automatically be synchronized with eM Client. SmarterMail users without the MAPI/EWS option should set up an account within eM Client using either IMAP or POP3.

Mozilla Thunderbird

Mozilla Thunderbird is a free, open source email client developed by the Mozilla Foundation. SmarterMail supports synchronization of email, contacts and calendars with Thunderbird.

CalDAV

Users can also synchronize their SmarterMail calendars with Thunderbird using the CalDAV protocol and the Lightning add-on.

Message Retrieval

For messages, users should set up an account within Thunderbird using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP IDLE is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail.

Mobile Devices

SmarterMail supports synchronization with most mobile devices on the market, including:

- Apple iOS
- Google Android

Apple iOS

Apple iOS devices include the iPod Touch, iPhone and the iPad. SmarterMail supports synchronization of email, contacts, and calendars with iOS devices.

EAS

The EAS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, EAS uses direct push technology to sync email, calendars, and contacts — including contact pictures — in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and the mobile device.

Once the EAS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article How To Activate EAS .

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding EAS to specific mailboxes. For more information, refer to the KB article How To Configure IIS for EAS .

For synchronization instructions for a specific mobile device, refer to the manufacturer's website. Additional information may be available in the SmarterTools Knowledge Base.

CardDAV and CalDAV

SmarterMail users that choose not to purchase the EAS add-on can synchronize their SmarterMail contacts — including contact pictures — and calendars with iOS devices using the CardDAV and CalDAV protocols. Support for CardDAV and CalDAV is built into these products, so there is no need to download and install additional applications to sync contact and calendar data.

Google Android

Android is an operating system designed for use in a variety of smartphones and mobile devices. Examples of devices that run on Google Android include the Google Pixel line, the Samsung Galaxy line, and devices from other manufacturers. In addition, the Kindle Fire runs on a modified version of the Android operating system. SmarterMail supports synchronization of email, contacts, and calendars with Android devices.

EAS

The EAS add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, EAS uses direct push technology to sync email, calendars, and contacts — including contact pictures — in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and the mobile device. Note: Only Android devices running version 2.0 or later support synchronization via EAS. Support for EAS may also vary by device. For example, EAS does not support Corporate Calendar or email applications for the Motorola Droid, Droid 2 or Droid X because they are custom applications that do not comply with EAS specifications.

Once the EAS add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article How To Activate EAS .

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding EAS to specific mailboxes. For more information, refer to the KB article How To Configure IIS for EAS .

For synchronization instructions for a specific mobile device, refer to the manufacturer's website. Additional information may be available in the SmarterTools Knowledge Base.

CardDAV and CalDAV

SmarterMail users that choose not to purchase the EAS add-on can synchronize their SmarterMail contacts and calendars with Android devices using the CardDAV and CalDAV protocols. While the default calendar and contacts apps may NOT support either protocol, there are some Android apps that do support both. IN addition, there are CalDAV and CardDAV specific apps that can facilitate synchronization, though these may be paid apps. More information and implementations of CalDAV and CardDAV can be found by reviewing Implementations of CalDAV and CardDAV .

Message Retrieval

For SmarterMail users with EAS mailboxes, messages will automatically be pushed to their mobile

devices as they are received. SmarterMail users without the EAS option should set up an account within the mail application provided on the mobile device using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP IDLE is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail.

Languages, Protocols and Clients

The language a user selects/sets for use in SmarterMail — also known as localization or internationalization — is EXTREMELY important. That's because it's much more than simply what is seen in the webmail client. SmarterMail's language selection is the basis for everything: the things you see in the webmail interface as well as what's returned to an email client when you connect using Outlook, eM Client, iOS Mail and more. That includes things like settings labels, folder names, calendars and calendar appointment, contact groups, email message content, log files and essentially everything within SmarterMail. Therefore, it is extremely critical that whatever language is set in SmarterMail is the language you actually want to use.

For example, BEFORE importing a PST from Microsoft Outlook, it is essential that the language selection in SmarterMail matches the language of the PST file. If this isn't done, you will have 2 versions of all the folders that are imported: those already in webmail that are in the language set for the user (e.g., Inbox, Sent Items, Deleted Items, default calendars, pre-existing contacts, etc.) PLUS those that are imported from the PST, which could be in a completely different language. You will then have to go through and move items around, delete incorrect folders, fix calendar appointments, etc. This can be a time-consuming process and may even lead to missing messages, missing contacts or incorrect calendar appointments.

As for how SmarterMail handles things like PST imports, mailbox migrations, etc., SmarterMail mirrors Microsoft Exchange.

Mailbox Migrations

Out of the box, SmarterMail supports 111 different languages for mailbox migrations. While the webmail interface supports 16 languages at this time, we support a larger number of languages for migrations in order to facilitate the transition to SmarterMail and to languages we do support.

In terms of the migration itself, if the source server is not in the same language SmarterMail is set to, we will make every effort to transition the "inbox" on the source server into the destination's current inbox folder.

There are also situations where the language set in webmail may not translate to an email client. For example, if you're using an English version of iOS or macOS Outlook will only show the folders in English, even if your webmail interface is set to a different language. This is not a SmarterMail issue, and SmarterMail has no way of converting the language in the client or on the OS to its language.

SmarterMail Language Selection and Protocols

When communicating with a client using IMAP, SmarterMail will default to the language selection of the user and of the client. Because this protocol handles things like default folder names differently than other protocols, it's easiest just to let the client handle the translations.

When using EWS, EAS or MAPI, SmarterMail utilizes server-side (as opposed to client-side for IMAP) translations that send the default folder names to the client using the language that the user has saved on the server. Unfortunately, many clients will use their own internally defined folder names for many default folders. Therefore, the folder names in SmarterMail may not match exactly to what's used in the client.

Email Clients and SmarterMail Language Settings

For the most part, SmarterMail mirrors Microsoft Exchange in how it handles languages and language changes, and an email client's interpretation of the information sent to it on an initial sync, as well as subsequent syncs, with regard to language selection. In some respects, SmarterMail is actually more language-friendly than Exchange and can understand changes in language, keeping the potential for duplicate folders at a minimum when compared to Exchange.

To understand this, take the following scenarios, noting that the languages used are arbitrary:

- Your email client is using English, but your language in webmail is set to French;
- You finish your sync to the client, then change your webmail language to English.

Using those scenarios, below is a list of email clients and how they interpret language settings during an initial sync with SmarterMail, and then what happens if the language set in webmail is changed.

(I.e., change from French to English.) Realize, these scenarios generally only govern when connecting using a protocol other than IMAP.

This is mainly how default/special folders (e.g., Sent Items) are handled as custom folders will always remain in their original language. Important Note: Language choice, and changing that language choice, is a complex process. Therefore, after a language change is made for a user in SmarterMail, it's best to remove and re-add the account in any client that is synced to that user.

Outlook for Windows

Using SmarterMail, special folders may be duplicated in Outlook, having both a French and an English version. However, these do not sync back to the SmarterMail server, so they do not appear in webmail. Microsoft Exchange acts similarly, except that it does sync a Drafts folder back to the server. (SmarterMail does not.)

When changing the language in SmarterMail, Outlook automatically updates the special folder names, but the duplicates remain and the duplicates sync back to the mail server, so they will appear in webmail. Exchange acts the same way — not initially, but after Outlook is closed and re-opened, the duplicates are synced back to the server.

Outlook for Mac

Using SmarterMail, all folders are correctly mapped in Outlook on an initial sync as well as when the language is changed in SmarterMail. Exchange acts the same way.

However, we have noticed that duplicate folders can appear after Outlook has been in use for a period of time and after an undetermined number of syncs. If this happens, duplicate folders can be cleaned up in Outlook by going to Account Settings > Advanced > Folders and resetting mappings. After the mappings have been reset, the duplicate folders can be deleted.

Windows Mail

Using SmarterMail, special folders may be duplicated in Outlook, having both a French and an English version. However, these do not sync back to the SmarterMail server. Microsoft Exchange acts the same way.

When changing languages, folder names are updated automatically in both SmarterMail and Exchange.

Thunderbird

Using SmarterMail, all folders are correctly mapped in Outlook on an initial sync. When the language is changed in SmarterMail, folder names are automatically updated in the Subscribe dialog, though a restart of Thunderbird is required for the changes to take effect.

Using Exchange, there is some folder duplication on the initial sync, though Inbox, Drafts and Sent Items are properly translated. When the language is changed, it's necessary to unsubscribe from "phantom copies" of the special French folders.

eM Client

Using SmarterMail, special folders are correctly mapped, though folders such as "Sync Issues" will still show in French. Exchange acts the same way.

When changing languages, folder names are updated automatically in both SmarterMail and Exchange.

Mac Mail

Using SmarterMail, all folders are correctly mapped in Outlook on an initial sync as well as when the language is changed in SmarterMail. Exchange acts the same way.

Conclusion

The takeaway from this is that email clients act differently on an initial sync and on subsequent language changes. Ideally, all clients would act like Outlook for Mac and Apple Mail: map folders correctly on an initial sync as well as on any language changes in webmail.

Browser Notifications

SmarterMail utilizes browser notifications in order to alert users of various activities within their account. For example, users get a pop-up notification when a message is delivered to their inbox, a calendar reminder is triggered, or an instant message is received. Simply clicking the browser notification opens that new message, that new calendar event, or that new instant message. Note: If you're using a new browser or haven't previously set the notification permissions, you will be prompted to allow this functionality when a new message is delivered to your inbox, a calendar reminder is triggered or a chat message is received. Keep in mind that clearing your browser cookies will make SmarterMail request this permission again as well.

Users can even manage which areas will trigger browser notifications from their Account settings: Calendar reminders, Chat messages, and/or New emails. Notifications that are received when the SmarterMail web interface is not open will be displayed on the Notification icon in the upper right corner of the webmail interface.

Unblocking Notifications

If "Browser notifications have been disabled in this browser." is displayed on the Notifications card you must first unblock browser notifications for the SmarterMail site in order to enable/disable

specific alerts. Please review your browser documentation for the exact steps in unblocking site notifications or refer to the Knowledge Base article, Unblock / Allow Browser Notifications .

Dismissing the Notification

If you want to eliminate the "Browser notifications have been disabled" toast notification altogether, simply click the Dismiss button. This will eliminate it from being displayed until you clear your browser cache or delete cookies in your browser.

Sharing Overview

SmarterMail gives users the ability to share several things with other people within their organization. This includes primary resources as well as secondary resources. For example, SmarterMail creates default calendars, contact lists (address books), task areas and more. These can be shared, but any new "folder" you create — a new calendar, a new tasks area, etc. — can also be shared, all on its own. For email folders, parent folders can be shared along with any sub-folders created within the parent, or individual child folders can even be shared individually. This all makes collaborating with co-workers within your organization extremely simple, as well as extremely flexible.

SmarterMail also gives domain administrators the ability to create Public Folders . These are domain-level folders that can be shared with users and user groups across the domain. These can be used by multiple people — such as a Sales or Marketing Department — for organizing and standardizing a calendar or even tasks.

When synchronizing to a mobile device, or some desktop clients, using protocols such as EAS and EWS, shared items can be available on those devices and in those clients. Each device and client acts a little differently, however, so not every shared resource may be available to you due to limitations of the device/client or even a limitation of the protocol being used. For example, when using the Gmail client on an Android device, there's no way to get shared Tasks. In addition, some clients act differently based on the type of permission given to a shared item. Generally, shared items will synchronize if the item is shared with Full permissions, as opposed to Read Only or Availability (for calendars). Clients such as eM Client and Outlook generally reject any share with any other permission type.

Users can share the following areas with other organizational members:

- Email Folders - parent folders as well as child (sub) folders
- Calendars - primary and secondary
- Contact Lists / Address Book - primary and secondary
- Tasks - primary and secondary
- Notes - primary and secondary

Domain administrators can configure Public Folders for the following:

- Calendars
- Contacts
- Tasks
- Notes

That leaves areas like Online Meetings, News feeds and File Storage as the only areas without conventional sharing options. However, both online meetings and File Storage are collaborative by their very nature. So, they can be "shared", just not the same way as contacts, tasks, etc.

Shares, Synchronization and MAPI & EWS

Any client connecting to SmarterMail using MAPI & EWS will have instant access to any shared resources regardless of whether those shares are mapped in webmail. The MAPI & EWS protocols act differently than webmail in that both protocols automatically "see" any resource shared with the user connecting. Therefore, there may be some inconsistency between shares in webmail and in a MAPI & EWS client. While shares are automatic in webmail, there may be instances where a share doesn't show in webmail but it's available in Outlook for Windows that's connecting via MAPI. In those instances, the user simply needs to verify the share is properly mapped in webmail.

Shares via WebDAV

In a broad sense, WebDAV is a network protocol for creating interoperable, collaborative applications. In terms of a mail server, WebDAV is broken down into 2 protocols created for specific features: CalDAV for calendars, and CardDAV for contacts. Both protocols were created for collaborative software, client or server, that need to maintain, access or share specific items. (I.e., calendars and contacts, respectively.)

Both CalDAV and CardDAV are supported by a variety of different clients and applications, as well as web-based services, because they both are robust, and free, solutions for sharing items. For example, some scheduling services can connect to a user's calendar over CalDAV so that a user's availability is known by the service, and any appointments created using the service can be added to a user's calendar.

To share items via either CalDAV or CardDAV, a user simply needs the WebDAV URL for their account. Whomever that link is shared with can then use the link for calendar apps, contact apps, or even email clients so that they have access to any shares made available by the user. To find the WebDAV link, a user simply logs into their webmail account, and navigates to Settings > Account , then copy the link on their WebDAV card.

How to Share

There are a couple of different ways to share items: from within an area itself or from the Sharing page in your user settings. One of the important things to know about sharing is that when you either initiate a share with someone, or revoke that share, those actions are automatic. That means that the other person — or those other people — don't have to do anything. They will either see the shared item or it will be removed. The same holds true when something is shared with you, or if that share is revoked: it will simply appear or disappear.

Sharing Individual Folders

Whether you're sharing an email folder, a calendar, a task list, or any other item, the process is essentially the same. The only real difference is that SmarterMail allows you to share individual email folders versus calendars, task folders, etc. which are, essentially, all-or-nothing shares as there aren't any embedded items in those areas. For example, email folders can contain sub-folders, which can then contain their own sub-folders. Calendar and Task folders are self-contained and do not have any sub-folders.

Regardless of how you get to a folder's sharing option, you're presented with the following:

• Users - This area allows you to share the item with one or more user, and each user you add to the share can have their own permission level. These are:

• None - This permission acts as a "negater" and is, therefore, only available for users. For example, let's say you have a User Group set up for your Marketing Department. However, you don't want to share Notes with Henry because he ate your piece of cherry pie last week. You add Full Control access to the Marketing Department user group, you'd add Henry's username under Users and set his access to "None". That way, you're sharing Notes with everyone in Marketing EXCEPT Henry as you've negated his permission.

• Availability - Used exclusively for calendars, this permission means that the user with this permission can see whether a person is available for scheduling purposes, but it doesn't allow for the viewing of a calendar or its appointments/events.

• Read-only - This means that the user can only view the items in the share (calendar entries, contact lists, etc.), they have no control over editing entries, adding entries, etc. A read-only share would be good, say, for a colleague who needs access to a contact list, but who doesn't need to manage those contacts in any way.

• Manage - This access allows others to add, edit and/or delete any items within the share. (But, importantly, NOT the share itself.)

• Owner - This access allows others to rename and/or delete the specific folder that's being shared. Basically, they use whatever is being shared just as if it were their own.

• User Groups - This area allows you to share the item with groups of users that have been set up previously. When sharing with a User Group, the same permission levels are available EXCEPT for None as that is a user-only permission.

Internet Calendars

Calendars are a little different when it comes to sharing. For example, they have their own permission: Availability. They're also unique in that a calendar folder can be shared publicly as an internet calendar, or "web calendar" (commonly known as a "Webcal"). An internet calendar is just that: it is a calendar that can be subscribed to via a basic URL. The URL is either copied from a calendar provider — sports teams generally have their game schedules available as an internet calendar — or it's sent out to people via email. SmarterMail gives users the ability to make any of their calendar folders available as internet calendars.

To get your internet calendar URL, do the following:

• First, go to the Share Folder modal by either selecting a calendar folder and right-clicking it, or using the folder icon at the bottom, left of the calendar interface.
• When the Share Folder modal opens, click on the Webcal tab.
• Toggle the setting "Allow others to subscribe to this calendar using Webcal".
• The Webcal Shareable Link will appear — copy this link. (There's a handy copy icon to the right of the URL.)
• Save the change.

You can then send that Webcal link to whomever you want, publish it on your website, or do whatever you want with it. And, if you decide you no longer want that calendar shared with the internet, simply repeat the steps above and disable the toggle. The calendar will cease to be shared and will be removed from the calendars of whoever used the shareable link.

Using the Sharing Page

It's also possible to share items using the Sharing page that appears in a user's settings. This page is more than just a way to share items as it gives users an understanding of all of the shares associated to their individual account: what they've shared with others, what's been shared with them, and any Delegation accounts they've set up.

However, using the "Shared With Others" tab, it IS possible to share items. Simply click the New button at the top of the content pane. This opens a new modal and offers the following options:

• Folder - The type of share you want to create, based on the "folder", or item, you want to share. All of the items you have available to be shared are listed in this dropdown: all calendars, all email folders, all address books, all notes, and all tasks.

• Users - This area allows you to share the item with one or more user, and each user you add to the share can have their own permission level. These are:

• None - This permission acts as a "negater" and is, therefore, only available for users. For example, let's say you have a user group set up for your Marketing Department. However, you don't want to share Notes with Henry because he ate your piece of cherry pie last week. You add Full Control access to the Marketing Department user group, you'd add Henry's username under Users and set his access to "None". That way, you're sharing Notes with everyone in Marketing EXCEPT Henry as you've negated his permission.

• Availability - Used exclusively for calendars, this permission means that the user with this permission can see whether a person is available for scheduling purposes, but it doesn't allow for the viewing of a calendar or its appointments/events.

• Read-only - This means that the user can only view the items in the share (calendar entries, contact lists, etc.), they have no control over editing entries, adding entries, etc. A read-only share would be good, say, for a colleague who needs access to a contact list, but who doesn't need to manage those contacts in any way.

• Manage - This access allows others to add, edit and/or delete any items within the share. (But, importantly, NOT the share itself.)

• Owner - This access allows others to rename and/or delete the specific folder that's being shared. Basically, they use whatever is being shared just as if it were their own.

• User Groups - This area allows you to share the item with groups of users that have been set up previously. When sharing with a User Group, the same permission levels are available EXCEPT for None as that is a user-only permission.

As you can see, the process for sharing contacts, calendars, tasks, and even email folders is essentially the same and relatively simple: you select the item you want to share, add the users and/or user groups you want to share to, and set the permissions for each. Once you've saved your settings, the people you've shared with will have those items automatically mapped to their users.

Email

Email Overview

SmarterMail users can send and receive email messages, view their calendars and create appointments, create or review tasks and more, from anywhere in the world, using any computer or mobile device and a simple web browser. In addition, SmarterMail is fully compatible with any desktop email client such as Microsoft Outlook or Apple Mail, or mobile email, contacts and calendar apps on Android and iOS. To log in to SmarterMail simply use the link to the webmail interface login page provided by

whoever set up your SmarterMail mailbox. Once on the login page, type your full email address and password in the appropriate fields to access your account.

This page covers a number of areas pertaining to email, in general, and the webmail interface. These include:

- • Default and Custom Folders
- • Messages View
- • Selecting Messages
- • Searching Messages
- • Sorting Messages
- • Filtering Messages
- • Email Actions

Navigating Email

When you go to the Email section of SmarterMail you'll generally start with your Inbox as it's the primary location all new email resides. While you can have content filters set up that route email to different folders or locations, your Inbox is, by default, the starting point for anyone using webmail. Once here, you'll see that the interface is separated into various sections.

Show/Hide Icon

At the top of the folders view you'll see the show/hide icon. This allows you to hide or show your list of folders, which is extremely beneficial when viewing your Inbox on smaller devices, such as tablets and phones.
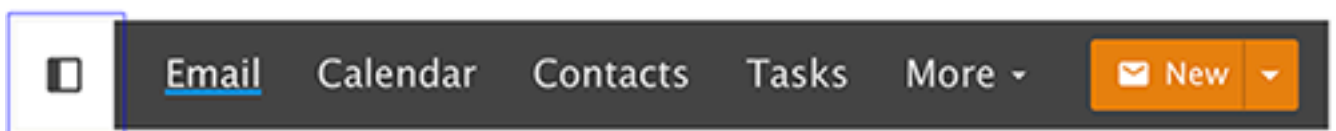
Default and Custom Folders View

The left side of the interface displays your folders. Here, you'll see the default folders listed at the top:

- • Inbox
- • Drafts
- • Deleted Items
- • Junk Email
- • Sent Items

These folders are created for every mailbox within SmarterMail.

Below the default folders are the custom folders that a user creates. If additional folders are embedded within a main parent folder, an icon is displayed to the left of that folder's name. Clicking the icon will expand that folder and display the additional, embedded folders. Clicking it again will hide those folders.

At the bottom of the custom folders list is the Shared With Me area. Here you'll be able to see any folders other users have shared with you. As for your own shared folders, these are denoted by a sideways V shape to the left of the folder. Folders shared with you are always displayed in the Shared With Me area, while folders YOU share remain in their natural order — they simply have a sharing symbol next to them.

Read more about Managing Folders in SmarterMail.

Messages View

To the right of your folders is the Messages view. Here, you'll see a list of all of the messages in your inbox or that reside in whichever folder you're currently in.

At the top of the messages view are buttons or icons representing various ways to interact with the messages in your list:

- Select
- Search
- Sort
- Filter
- Actions (□)

Email Interactions

There are a number of different ways to interact with messages in SmarterMail. Buttons such as New are fairly self-explanatory, but others have multiple different options.

Selecting Messages

It's possible to select/deselect individual messages, all messages, or even all concurrent (one-after-the-other) messages. You can do this using the options below, or by using keyboard shortcuts. For example, holding the Ctrl key (on Windows) or the Command key (on macOS) allows you to select individual messages. Using the Shift key allows you to select multiple concurrent messages. However, you can also use the select options from the dropdown:

- Select All - Selects all messages in the All Messages view.
- Deselect All - If any or all messages are selected in the All Messages view, this unselects them.
- Enable Select Mode - This allows users to select multiple different messages, individually, one at a time. Use this method for selecting different messages that are separated or scattered throughout your messages list so they can be moved, deleted, or otherwise handled the same.

Searching Messages

Using the standard search of your list of messages allows you to type in a domain name, full email address, or keywords to quickly find information. SmarterMail also offers an advanced search option. For more information, see Searching Email Messages .

Sorting Messages

To sort messages, click on the Sort icon and select the field, or fields, you want to use for the sort order for your messages. For example, clicking the Sort icon and selecting "Size" will sort items in order of their size. (This includes the size of a message plus attachments.) To change the "direction" of the sort, either Ascending or Descending, select that option from the Sorting icon menu as well.

In general, the following sort options are available:

- Date - The date and/or time the mail system received the email.
- From - The sender of the email message.
- Subject - The subject of the email message.
- Size - The size of the email in kilobytes.
- Reverse Order - This reverses the sort order to either Descending or Ascending.

Filtering Messages

This includes read status (Read vs. Unread), whether or not you've replied to a message, whether a message is flagged, linked to a task, or has an attachment. It's also possible to filter messages based on message Category. Think of using a filter as a way to display only those messages that correspond to the criteria you've selected. If you filter messages with attachments, ONLY messages with attachments will be displayed.

Using a filter allows you to organize messages in your list based on specific criteria, ore one or more Categories. Whereas sorting arranges ALL of the messages in a folder based on the criteria selected, filtering only displays messages based on the criteria or categories that are selected. It's then possible to sort those messages using one of the sorting options, mentioned below.

Filters offers the following options:

- All - Will display all messages. (The default filter.)
- Unread - Will display only messages marked as Unread.
- Read - Will display only messages marked as Read, hiding any unread messages.
- Replied - Will display only messages that have been replied to.
- Not Replied - Will display only messages that have no replies.
- Flagged - Will only display messages marked for follow up, or "flagged".
- Linked to Tasks - Will only display messages that are associated with Tasks.
- Attachments - Will only display messages that have one or more attachments.

Below these options is a list of categories that are available for filtering. All Categories is checked, by default, but it's possible to limit the filter to one or more specific categories as needed.

Manage Categories

You can also manage your categories from the Filtering menu. Clicking Manage Categories opens a modal window with all current categories listed. It's possible to do things like change a category name, change its associated color, or even add new categories using this modal. Once categories are changed or modified, those changes or modifications are carried over to any area categories are available. (E.g., Calendars.)

Email Actions

Using the Actions (□) button allows you to perform the following:

• Move - Allows you to Move the Message to a Folder. When you select Move, you are prompted to select a Folder where you want the Message to be placed. Alternatively, you can select the message from the all Messages view and drag it to the folder of your choice. Note: You can also drag-and-drop messages to an available folder.

• Invite All to Appointment - This initiates the creating of a new appointment, and automatically adds the addresses in the To: and CC: fields as attendees. (Bcc: addresses are excluded.)

• Add Task - Allows you to add a Task that is associated with that message. This is a good way to keep task details aligned with the message that initiated the task in the first place.

• Print - Brings up the print menu for the message.

• Trust Sender - Adds the address to your Trusted Senders list, meaning any future emails from this address will bypass most antispam options enabled for the server. For a detailed explanation, see Trusted Senders . Note: SPF and DKIM still run against any address in the Trusted Senders list to prevent phishing.

• Untrust Sender - This removes this address from your Trusted Senders list. This means future emails from this sender will no longer bypass spam filters and will be checked according to the server's standard anti-spam settings.

• Block Sender - Prevents the sender of the selected message(s) from sending any more messages to the account.

• Download EML - This allows you to download a copy of the message as an EML file (the default file type for email messages) and save it to your desktop or other location using File Explorer. Multiple files can be downloaded, and they're saved as a .ZIP file. There is a 1GB limit per download.

• View HTML - Changes the message to display all of its HTML formatting.

• View Text - Removes any HTML formatting and displays the message as "text only."

• View Header - Lets you view the full email header and raw message content. This shows the original, unformatted version of the message, including technical details in the header, like where the email came from, how it was delivered. Viewing this information

Move

Invite All to Appointment

Add Task

Print

Trust Sender

Block Sender

Create Content Filter

Add Sender to Content Filter

Download EML

✓ View HTML

View Text

View Header

Reply - Selecting Reply means you will reply to the sender only.

• Reply All - Selecting Reply All addresses a response to the sender and everyone else who received the message. This includes all email addresses listed in the To and Cc fields, except your own email address.

• Forward - Selecting Forward allows you to send the message to an address other than what's in the To and Cc fields. It is also possible to add email addresses to the To and Cc fields when you Reply or Reply All to a message. In addition, it's also possible to forward multiple emails to other addresses. To do this, simply select the messages from the messages list, then use the Forward option. This will create a new message with the selected emails attached as EML files.

• Move - Moves the selected message(s) to any available folder. Note: You can also drag-and-drop messages to an available folder.

• Flag / Unflag - Either marks or unmarks the selected message(s) for follow-up and changes the color of the follow-up flag appropriately. Alternatively, users can click on the flag icon next the message to add or remove a flag.

• Mark Read / Mark Unread - Marks the selected message(s) as read or unread and changes the

status indicator appropriately.

• Move to Junk - Moves the email to your Junk Email folder, and also helps the system recognize the sender and message contents as possible spam.

• Trust Sender - Adds the address to your Trusted Senders list, meaning any future emails from this address will bypass most antispam options enabled for the server. Note: SPF and DKIM still run against any address in the Trusted Senders list to prevent phishing.

• Untrust Sender - Only available of the sender is on your Trusted Senders list; This removes them from that list.

• Block Sender - Prevents the sender of the selected message(s) from sending any more messages to the account. When you block a sender, a new Internal Blocked Senders Content Filter is created. Any user you block is added to that list, and their email is, by default, deleted.

• Unblock Sender - Allows the sender of the selected message(s) to begin sending messages again by removing the address from the Internal Blocked Senders content filter.

• Download EML - This allows you to download and preserve the message in the format it was received by the mail server. EML files can be used for troubleshooting delivery issues, or sent to others and opened using any desktop email client.

• View Raw Content - Allows you to view the message in its raw, unformatted state and includes the header of the message. Viewing the raw content or just the header can assist with diagnosing potential issues with viewing the message.

• Delete - Deletes the selected message(s).

Read More

There's much more to interacting with email apart from how you manage it from the All Messages view. So read more on:

- Reading Email Messages
- Composing Email Messages
- Searching Email Messages
- Using Advanced Search
- Deleting Email Messages
- Flagging Email for Follow-up
- Linking Email to Tasks
- Managing Email Folders

Reading Email Messages

SmarterMail displays whether you have unread email in your inbox, or in any folders — even shared folders — a number of different ways.

- The number displays in the Email menu.
- The number displays next to its folder. (E.g., Inbox)
- A number appears in the browser tab, surrounded by parentheses.
- Unread messages display as bold in the All Messages view.
- A notification will temporarily display in your browser, as long as browser notifications are turned on.

To view the contents of a message, simply click the desired message and it will open in the Preview Pane. You can also double-click the message and it will open in a separate pop-up window. If you do NOT have a Preview Pane showing for your messages, double-clicking the message is the only way to open it and read its contents.

Single Message Actions

Reply ⌄ | Delete | Move to Junk | Mark ⌄ | ⋮

In general, the following options are available when viewing a message, either within the webmail interface or when it's been popped out into a separate window:

- Reply to a message - There are three (3) options when replying to a message:

- Reply - Selecting Reply means you will reply to the sender only.
- Reply All - Selecting Reply All addresses a response to the sender and everyone else who received the message. This includes all email addresses listed in the To and Cc fields, except your own email address.
- Forward - Selecting Forward allows you to send the message to someone other that someone in the To and Cc fields. Note: It is also possible to add email addresses to the To and Cc fields when you Reply or Reply All to a message.
- Delete - Selecting the Delete button will move the message to the Deleted Items folder. Note: This is the default action taken when a message is deleted. Depending on your settings, the delete action may be different. For more information, see Deleting Email Messages .
- Move to Junk - Using Move to Junk moves the email to your Junk Email folder, and also helps the system recognize the sender and message contents as possible spam. This information is used to help train new HAM/SPAM settings that are available to system administrators.
- Mark - Just as with Reply, there are several options available for marking messages:

- Flag / Unflag - Flags a message for follow-up or, if already flagged, removes that flag.
- Mark Read / Mark Unread - If not automatically marked, marking a message as "read" removes its highlight in the all messages view. If you've already read a message but want to

keep it for review later, it can be marked as "unread" and highlighting is added. (Unread messages also display in the indicators mentioned above. E.g., message counts in webmail and on any synced email clients.)

• Categories - It's also possible to add one or more categories to a message. This allows you to retrieve those messages using filters in the all messages view.

• Actions (☐) - The Actions menu allows you to do just that: perform some action on a message. These include:

• Move - Allows you to Move the Message to a Folder. When you select Move, you are prompted to select a Folder where you want the Message to be placed. Alternatively, you can select the message from the All Messages view and drag it to the folder of your choice. Note: You can also drag-and-drop messages to an available folder.

• Invite All to Appointment - This initiates the creating of a new appointment, and automatically adds the addresses in the To: and CC: fields as attendees. (Bcc: addresses are excluded.)

• Add Task - Allows you to add a Task that is associated with that message. This is a good way to keep task details aligned with the message that initiated the task in the first place.

• Print - Brings up the print menu for the message.

• Trust Sender - Adds the address to your Trusted Senders list, meaning any future emails from this address will bypass most antispam options enabled for the server. Note: SPF and DKIM still run against any address in the Trusted Senders list to prevent phishing.

• Block Sender - Prevents the sender of the selected message(s) from sending any more messages to the account.

• Create Content Filter - This options opens the Content Filtering area. Here, you can use information contained within the email message, such as the From Address, Subject, etc. and create a new Content Filter based off that information.

• Add Sender to Content Filter - This option opens a modal window that lists all of your existing Content Filters. You simply select the filter you want this sender added to, and they're immediately added.

• Download EML - This allows you to download a copy of the message as an EML file (the default file type for email messages) and save it to your desktop or other location using File Explorer. Multiple files can be downloaded, and they're saved as a .ZIP file. There is a 1GB limit per download.

• View HTML - Changes the message to display all of its HTML formatting.

• View Text - Removes any HTML formatting and displays the message as "text only."

• View Raw Content - Allows you to view the message in its raw, unformatted state and includes the header of the message. Viewing the raw content, and especially the message's header, can assist with diagnosing potential issues with viewing the message, with message delivery, etc.

When viewing messages in the content pane (as opposed to them being popped out in their own window), other options are available:

> • View Next / View Previous - These up and down "arrows" (or carets) will move you up and down the all messages area.
> • Pop out - This will pop the message out into its own window.

Sender Verification Shield

Next to the sender's name and/or address is the Sender Verification Shield. By default, SmarterMail checks a number of things to attempt to validate that the sender is who they say they are. Things like DMARC, DKIM, SPF, trusted sender status, whether the user is authenticated on the server, and whether they're listed in your Contacts are all used to verify that Tom@@Business-A.org, for example, IS actually Tom from Business-A.org. Moving your mouse over the shield opens a window that tells you whether the sender is likely the sender or not, and what checks were performed and their status.

The shield is color coded based on the sender's validity score:

> • Green - The email passed DMARC, DKIM, and SPF, and is either an existing contact (in your Contacts) or is part of your domain.
> • Gray - The email was sent from an address that failed one or more of the checks, or passed them but is NOT an existing contact or part of your domain.
> • Red - The email may not have been sent from an authentic account.

Now, this simply attempts to validate the sender. It's no indication that the person sending the message is doing so with bad intent or that the message itself is okay. It is an indication of the status of the sending server and the sender's address. Things like improperly configured or missing DKIM and/or SPF records can lead to a red shield. In addition, even if a sender displays a green shield, it doesn't mean the message is NOT spam.

The Sender Verification Shield is just another tool at a user's disposal, hopefully letting them know to take extra care when clicking links or downloading an attachment from an email from a suspect sender.

Viewing External Content

External content is considered to be any image, video, animated gif, etc. that has an external source and is contained in an email. When remote content is included in an email, that content is hidden by default and must be manually displayed. The good news is, you can either view the content in that one message, or you can allow content from the sender so future emails won't show any warning.

To view external content, click on the Show images or always show images from this sender text that appears at the top of the email message. Once you do this, the remote content will be displayed on that email going forward. Clicking on "always show images from this sender" will add an exception for that email address to the "Allow Inline Images From" list, which is found on the Webmail card in your Account settings. When an exception has been made for an email address, emails from that sender will display all remote content automatically. Note: Emails from Trusted Domains and Trusted Senders will always display remote content automatically.

To bypass this step, and allow remote content to be automatically displayed from all senders and sources, simply enable the Show images from external websites setting that appears as a toggle on the Webmail card in your Account settings.

Unsubscribe

Messages that are from outside senders, especially messages that are potentially unsolicited, are advertisements, are newsletters, or are of a kind where the footer of the message offers recipients a way to unsubscribe from them will include a more obvious "Unsubscribe" button in the message's header.

Clicking this button essentially automates the unsubscribe process for the recipient. This saves them from having to hunt down the unsubscribe link(s), clicking them, navigating through the various questions asked, confirmation of the unsubscribe request, etc. and simply ensures that the unsubscribe request is sent. Once clicked, a green toast notification appears confirming that the unsubscribe request was sent.

Email Trackers

Email trackers are generally small, transparent images that are embedded into a message for the sole purpose of knowing when a message is opened by a recipient. The idea is that, if there is a "hit" on that image, it was downloaded by the user when the email was opened. However, not everyone wants to be "tracked" like this. By default, SmarterMail will block all trackers for convenience. If a message does include an email tracker, text is displayed at the top of the message letting the user know. Users can click on that message and see who the tracker is from (e.g., Salesforce) and, if they so desire, accept the tracker for that message.

Downloading Email Attachments

If a message has any attachments, a paperclip will display in the Messages List for that message. In addition, the message itself will show a small icon in the message header with text that tells you how many attachments there are. For example, "2 Attachments are included with this email." Clicking on the linked text will open a modal window that displays the file name(s) of the attachment(s) as well as

the file size of each. It also displays, where possible, a preview of the attachment as an icon. Generally, this will only happen when an attachment is an image file. Other file types will display a more generic icon. Attachments are downloaded individually by simply clicking on the attachment. However, it is also possible to download all attachments in one convenient ZIP file.

It's worth noting that there may be instances where there is no paperclip displayed for a message in the message list, but text on a message itself noting that attachments are present. Generally, this happens with messages that have embedded images, such as images that are pasted into a message, logos and/or icons that are part of a sender's signature, etc. These are NOT displayed in the messages list as these are so common that virtually every message in a user's inbox would have an attachment icon on it, thereby diminishing its effectiveness. In addition, when filtering messages in a folder by "attachment", these types of messages are not included.

Composing Email Messages

It's very easy to create new messages in SmarterMail as well as reply to existing messages or forward messages on to other individuals or groups. Below you'll find a brief walkthrough of each scenario.

Jump To:

- Composing the Message
- AI Assistance
- Sending the Message
- Replying to Email Messages
- Forwarding Email Messages
- Forwarding Multiple Messages

Setting To, From, Subject, etc.

Creating a new message will pop-out the compose window. SmarterMail uses a pop-out window because it allows you to reference other areas of SmarterMail or easily navigate to other browser tabs if you're using other websites for information to include in your new message.

The following fields appear in the new message window:

- From - If you have more than one account set up, or one or more domain aliases, you have the ability to select the address from which the message will be sent. Otherwise, the message is sent from the one user you have set up. If multiple users are available, the From: line will have a down arrow. Simply click the arrow and select the address from the dropdown.
- Signature - If you have more than one signature set up, or if the domain administrator has set up a default signature for you, you have the ability to select the signature used for the message.

Note: If the domain administrator has disabled the ability to override domain-level signatures, you will not be able to choose the signature.

• To - Type the email address for each primary recipient you want to receive your email. Multiple addresses can be used, simply separate each with a comma or semicolon. When entering addresses into the To, Cc, and Bcc fields, SmarterMail will auto-complete addresses by referencing your contacts list, mailing lists, your auto-complete list , aliases or the Global Address List.

• Cc - Carbon Copy (Cc) recipients are those who should be included as part of the conversation, but are not necessarily primary recipients.

• Bcc - Blind Carbon Copy (Bcc) recipients are hidden from those people listed in the To and Cc fields. In addition, in a Reply All scenario, Bcc users do NOT receive a copy of the reply. For this reason, it is common practice to use the Bcc field when addressing a very long list of recipients or a list of recipients that should not (necessarily) know each other.

• Subject - Type a descriptive subject or title of the email.

Selecting Contacts

In addition to simply typing in the address you want to send to, it's possible to select contacts to populate the To, Cc, and Bcc fields. To do this, simply click the filed name. (I.e., To:, Cc, and/or Bcc.) This option opens a modal window and, from here, you can select the contacts based on a folder (i.e., Contacts, Global Address List, shared Contacts, etc.) or even display contacts based on a category. When a choice of folder or category is made, contacts associated to the selection are listed in the modal. One or more can then be selected, saved, and then added to the To, Cc, or Bcc field(s) as needed.

Composing the Message

Below the Subject line is a complete HTML editor that you can use to write and format your message. A number of formatting options are available, from selecting a font color to inserting multimedia elements to a message.

While it's possible to format a message using the buttons/tools available with the HTML editor, it's also possible to create a customized, HTML-rich message using an outside product or service, and then paste that code into the compose window of SmarterMail. Ideally, you'd switch SmarterMail's editor from "design view" — where you're using the toolbar to format your message — to "code view" with the "<>" button. Using code view, you create or edit the actual HTML tags that are used for formatting the message. When creating a message using an outside editor, pasting the code that's generated into the code view of the compose window ensures your original formatting is used for the message. You can then swap back to design view and see how the message renders. Once the message is created, it's ready to be sent.

Using AI Assistance

With the new AI feature, you can easily adjust your message to lengthen or shorten it, proofread the entire message or just a section, translate the message, or even change the tone. For more information, see the AI Assistance page .

Sending the Message

Prior to sending the message, it's possible to add attachments, add "actions" for marking the message is some way, and more. The following actions are available for a new message:

- • Send - Sends your message to the designated recipients.
- • Cancel - Cancels your message. However, SmarterMail has an auto-save setting, so it's possible that a draft of your message will be saved automatically. If this happens, you'll see a number appear next to your Drafts folder. Clicking Cancel will display a window asking whether you want to save a draft of the message.
- • Save Draft - Saves the message in its current state to the Drafts folder without actually sending it. This is useful if you need to continue writing the message at a later time. Note: By default, SmarterMail has an auto-save frequency of 2 minutes.
- • Attach (Paperclip) - Allows you to attach one or more files to the message. See below for more information.
- • Actions (□)

- • Message Priority - Set to High, Normal or Low. Specifies the importance of the message. By default, messages have a normal level of priority.
- • Request Read Receipt - Sends an email confirmation back to the sender when the recipient opens the message.
- • Request Delivery Receipt - Sends an email confirmation back to the sender when the message is successfully delivered to the recipient.
- • Flag - Marks the message for follow-up. For more information, see Marking Email for Follow-ups .
- • Link File - Uses SmarterMail's File Storage feature to insert a link to a file saved on the mail server or to a file located in a connected file storage account , such as Dropbox or OneDrive. Either way, the links can be sent to recipients who can then download the linked file(s). Note: Linking to a private file in File Storage will enable public access on that file with no set expiration date.

Attaching Files

In addition to using the Attach button when composing a message, you have the ability to drag-and-drop files to be attached to your message. When files are attached to an outgoing message, a file

manager will display at the bottom of the new message window. The file manager will display the name, size, and upload status of the file. Attachments must reach an upload status of 100% before the item is actually attached to the message. Note: To remove an attached file prior to sending the message, just click the X in the top, right corner of the file.

To display an image within your message body, use the Insert Image button from the toolbar editor.

Replying to Email Messages

SmarterMail gives users two options for replying to a message:

- Reply - Addresses a response to the sender only.
- Reply All - Addresses a response to the sender and everyone else who received the message. This includes all email addresses listed in the To and Cc fields, except your own email address.

When replying to a message, SmarterMail automatically fills in the address fields with the email addresses of the recipients from the original message, the subject field with the subject from the original message preceded by "Re" (which means "regarding" or "in regards to"), and the text box with the text from the original message. It is possible to edit any of these pre-filled fields, however, as needed. All other message options are the same as when composing a new message.

Forwarding Email Messages

You may also want to simply forward a message to a third-party or to someone not already copied on the original message. This is very easy to do:

- Forward - Allows you to send the message to a third party, or to an address that is not in the To or Cc fields.

Messages can be forwarded individually or in bulk. When forwarding multiple messages, the EML file of the email will be attached to a new compose window. SmarterMail automatically fills in the subject field with the subject from the original message preceded by "Fwd" (which means "Forward"), and the text box with the text from the original message. It is possible to edit any of these pre-filled fields, however, as needed. All other message options are the same as when composing a new message.

In addition, SmarterMail has an auto-forward option, which can be found in a user's Account Settings, that will forward a copy of all messages sent to a user's Inbox (as well as messages routed to other email folders via content filters or plus addressing).

Forwarding Multiple Messages

On occasion, users may want to forward multiple messages to someone. Instead of forwarding each

message individually, SmarterMail allows users to forward multiple messages at once and includes them as attachments to a single message.

Follow these steps to forward multiple emails at once:

- Log into SmarterMail as a user.
- Click the Email icon.
- In the navigation pane, click the folder containing the messages you wish to forward. The messages in the folder will load in the content pane.
- Select the desired messages. This can be done by selecting them individually, using the Sort button to look for messages with attachments, etc., it can be done by doing a search and then selecting all of the search results, etc.
- Click the arrow next to the Reply button.
- Select Forward in the drop-down. (This should be the only Reply option available to you.) This will open a new message window that you will use to compose a message to the desired recipients. The messages that you wanted to forward will be attached as .eml files to the new message.
- Compose the message and click Send .

AI Assistance

Integrating AI, particularly OpenAI's ChatGPT, into SmarterMail's Marketplace enhances the email experience with a powerful AI Assistance. SmarterMail's AI Assistance provides intelligent suggestions for composing emails, helping users communicate more effectively while saving time on drafting. This integration streamlines responses and follow-ups, making workflows smoother and boosting overall productivity.

AI Assistance offers four key actions:

- Shorten - will shorten the selected text.
- Lengthen - will make the selected text longer.
- Proofread - will check the selected text for spelling and grammar.
- Translate - which will add an "AI command" to the top of the text. All you have to do is add the language you want that text translated to.

Jump To:

- Creating an Email with AI Assistance
- Proofreading an Email with AI Assistance
- Translating an Email using AI Assistance
- Modifying the Tone of an Email using AI Assistance

Creating an Email with AI Assistance

AI Assistance goes beyond just creating emails, it can generate a wide range of content to streamline communication. Users can compose full emails, draft event invitations with specific dates, times, and locations, or create informational messages containing key details on a given topic. For example, you can instruct AI Assistance to: Write an email to all staff informing them that the company fridge in the break room will be cleaned out every Friday afternoon. Any items left in the fridge at that time will be discarded.

This command provides AI Assistance with clear parameters: the subject , timing , and action , ensuring accurate and efficient message creation.

> • To get started, in SmarterMail, click on New button. A dropdown menu will appear, select Email or simply click New to open a pop-up window. This will launch the email composition window (ensure pop-ups are enabled in your browser). In the editor toolbar, find and click the AI Assistance icon.
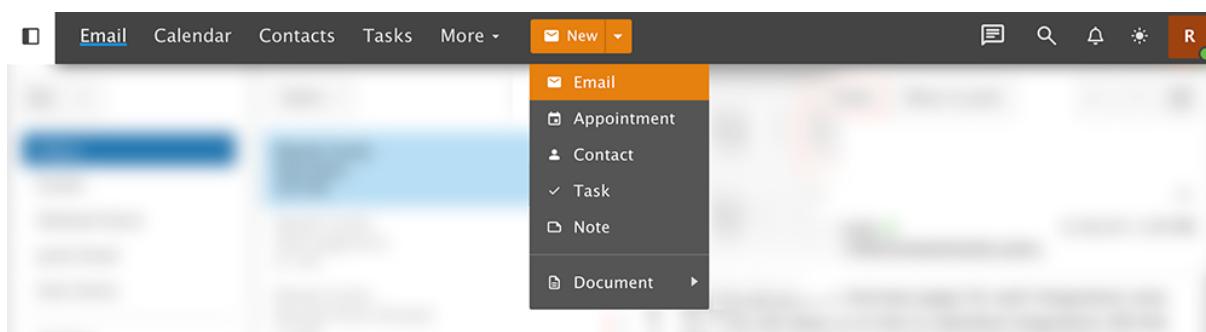
• The AI Assistance modal will pop up, you will notice that the Select Command field is empty, but the Input Text box is pre-filled with "Write me an email about..." this is where you specify what AI Assistance should generate. You can define any parameters to customize the output. In this example, AI Assistance is instructed to draft an email notifying employees about the company fridge cleanup. Simply provide the subject, content, and desired tone, then click the Generate button. The AI-generated email will appear in the Generated Text box, ready for review and use.

• Review the AI generated email to see if the content, clarity, and tone all work for you. If anything needs adjusting, just type your changes in the Input Text box above, hit the Generate button, and your updated message will appear in the Generated Text box. Once approved, click the Insert Button .

• Your AI generated message will be displayed within the body of the email, along with a subject line that you can easily copy and paste. If necessary, adjust the formatting, such as font, color, or style to

your preference. Once you're satisfied with the appearance of your email, simply click the Send button, and you're all set!
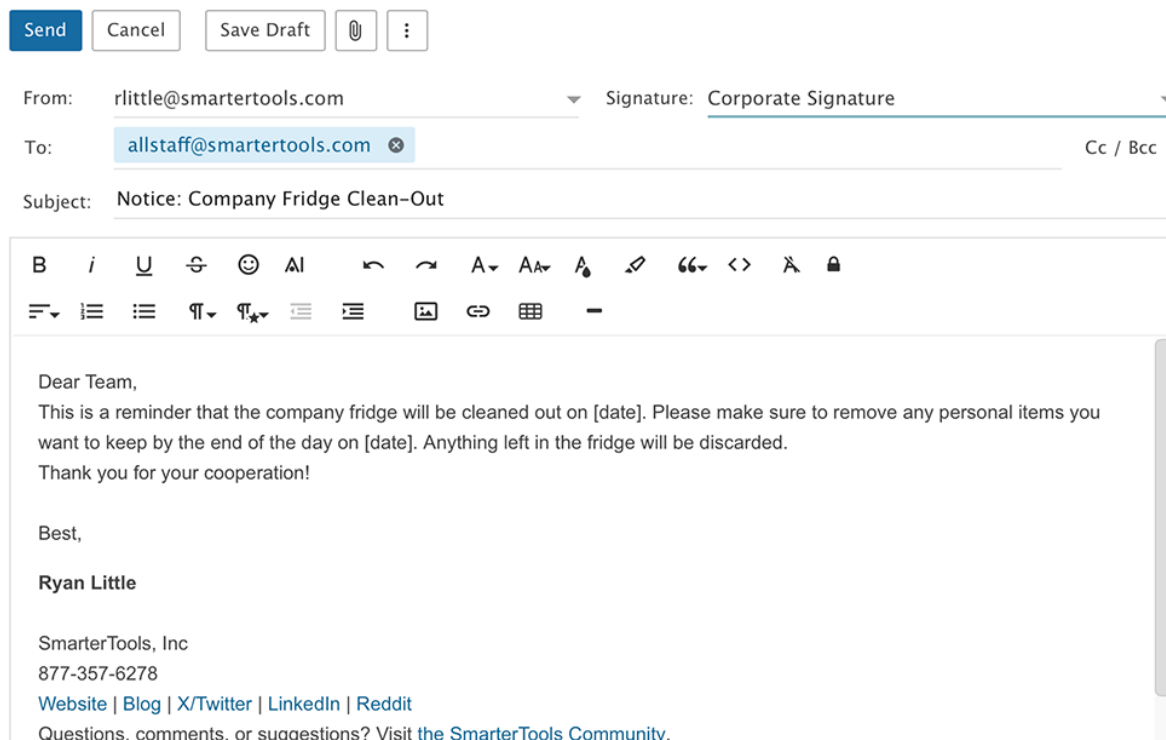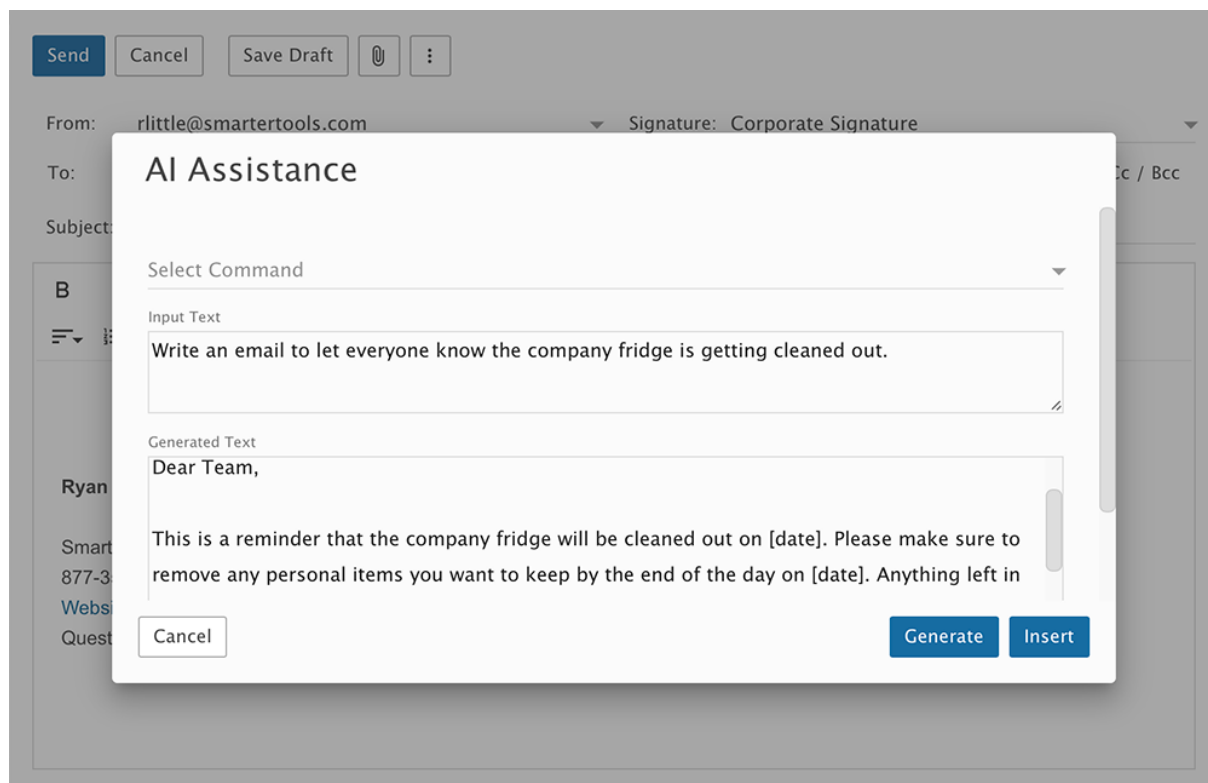
Proofread an Email with AI Assistance

Before hitting Send (especially when emailing an important client) it's always a good idea to double-check your message for clarity and professionalism. That's where SmarterMail's AI Assistance comes in with its Proofread feature. Simply highlight your text, click Proofread , and let AI Assistance do the heavy lifting. It'll check for grammar, spelling, and readability to make your message clearer and more polished. With AI Assistance's Proofread tool, you can ensure your emails are mistake-free, professional, and impactful, helping you communicate with confidence every time.

• To get started, in SmarterMail, click on New button. A dropdown menu will appear, select Email or simply click New to open a pop-up window. This will launch the email composition window (ensure pop-ups are enabled in your browser). In the editor toolbar, find and click the AI Assistance icon.
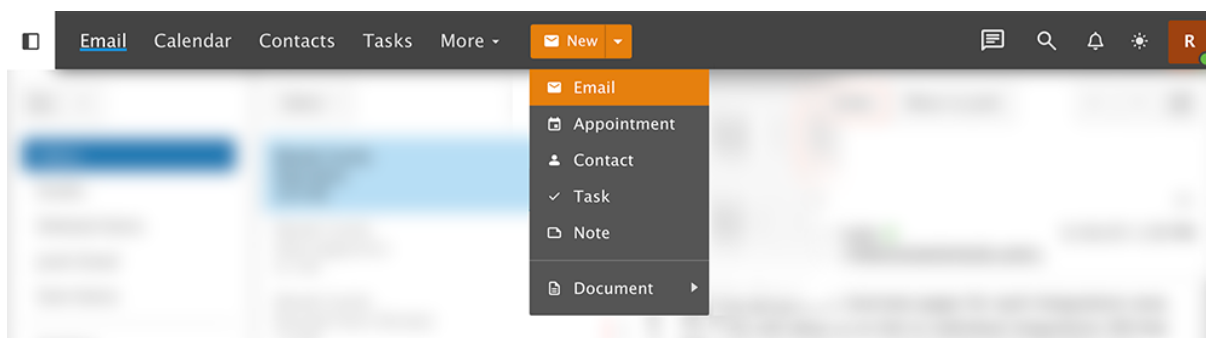
• The AI Assistance modal will pop up, you will notice that the Proofread option is already selected. The Instructions box will contain the pre-set command: "Review and correct the following text for grammar, spelling, and punctuation errors." Click Generate to apply the necessary corrections.

• Review the AI generated response to see if the content, clarity, and tone all work for you. If anything needs adjusting, just type your changes in the Input Text box above, hit the Generate button, and your proof-read message will appear in the Generated Text box. Once approved, click the Insert Button .

• Your AI generated proof-read message will be displayed within the body of the email. If necessary,

adjust the formatting, such as font, color, or style to your preference. Once you're satisfied with the appearance of your email, click the Send button, and you're all set!
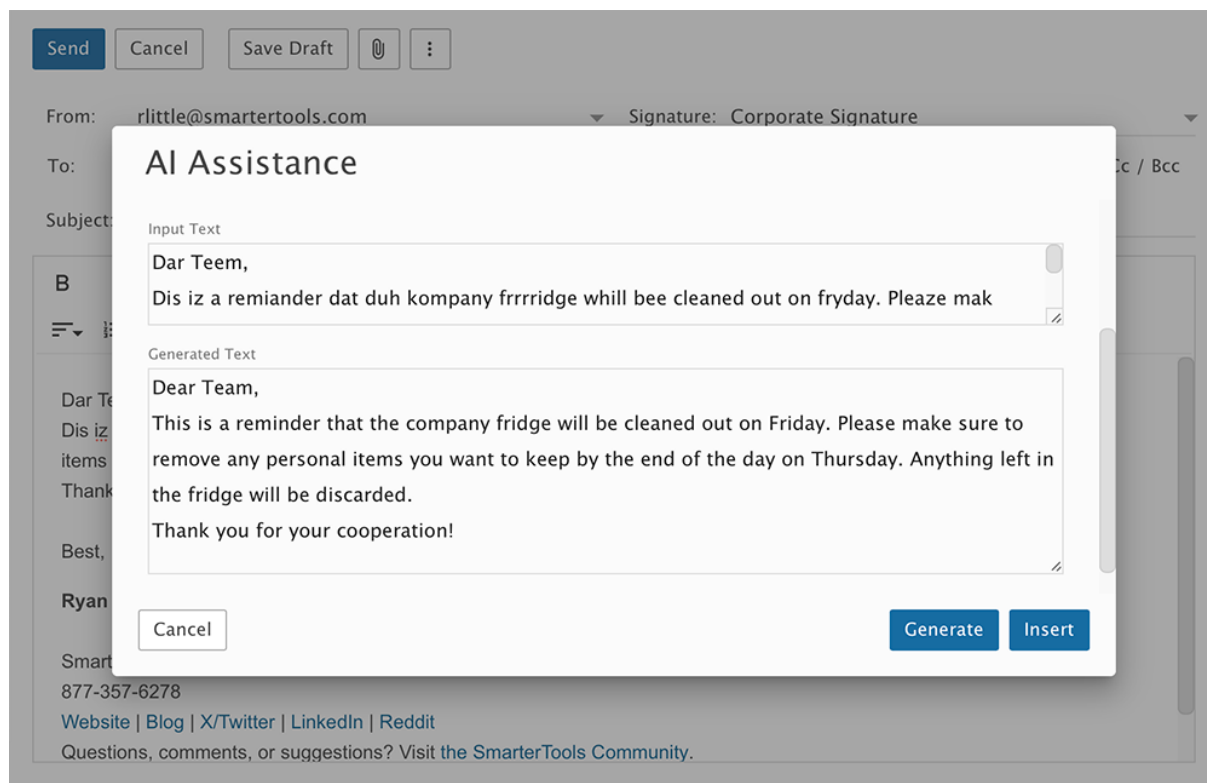
Note: Results generated by AI may contain errors and should be reviewed for accuracy.
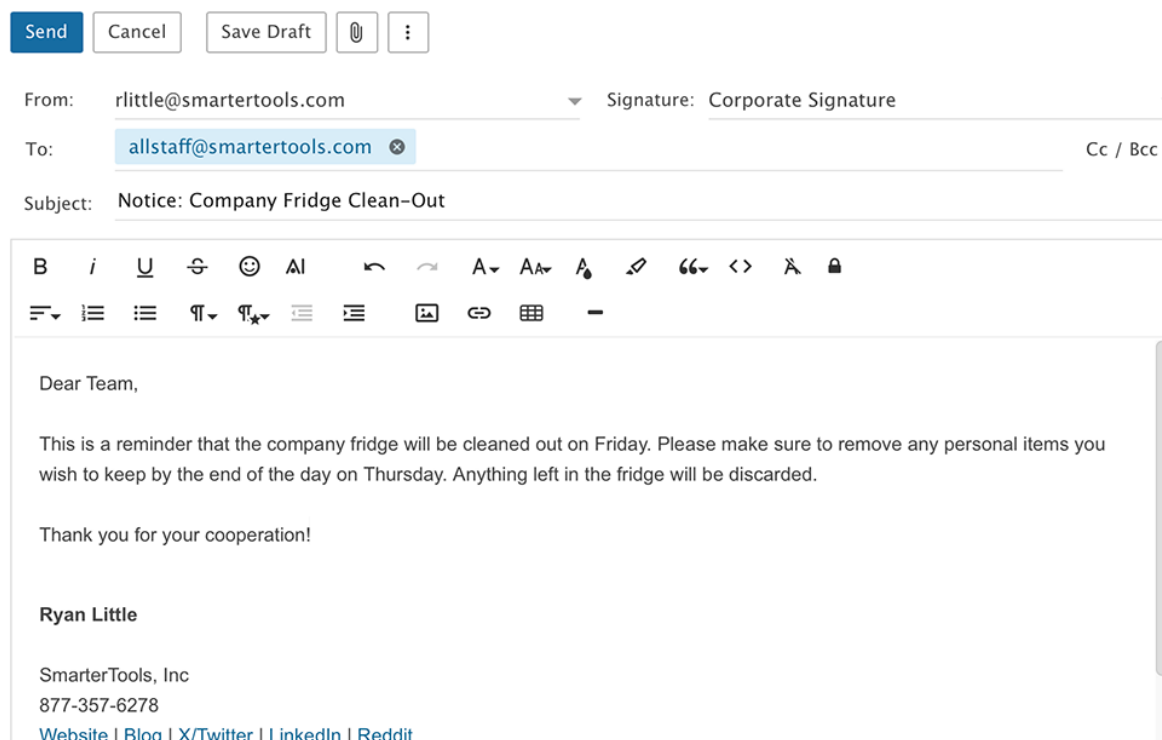
Translate an Email with AI Assistance

In today's global business world, clear communication across languages is more important than ever. SmarterMail's AI Assistance makes this easy with its Translate feature, allowing users to quickly and accurately translate emails into multiple languages. For example, we asked AI Assistance to: "Write an email to all staff letting them know that the company fridge in the break room will be cleaned out every Friday afternoon, and any leftover items will be tossed."

Since this organization is based in France, we need to translate the message into French. The first draft was written in English, so we use AI Assistance's Translate feature to seamlessly convert the message into French while maintaining clarity and tone. Simply select your text, choose Translate , and let AI Assistance handle the rest.

> • To get started, in SmarterMail, click on New button. A dropdown menu will appear, select Email or simply click New to open a pop-up window. This will launch the email composition window (ensure pop-ups are enabled in your browser). In the editor toolbar, find and click the AI Assistance icon.
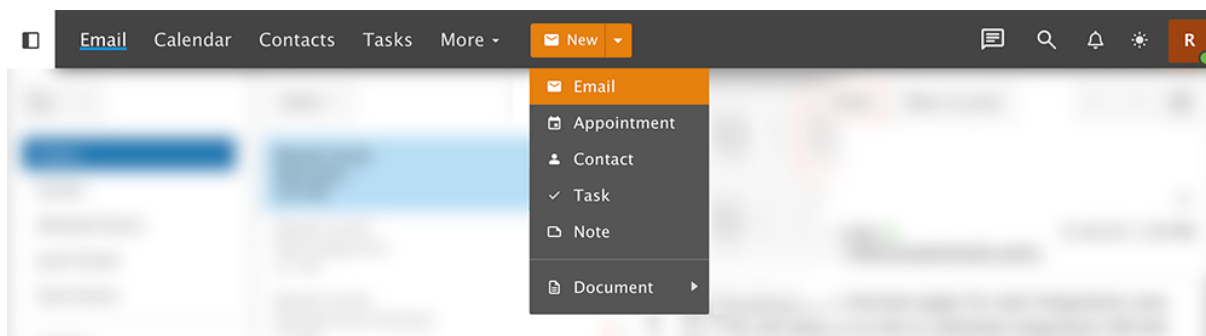
• The AI Assistance modal will pop up, you will notice that the Proofread option is already selected. Click the Select Command option to display your command options, in this case we're selecting Translate .

• The Instructions box will contain the pre-set command: "Translate the following text into [insert language here] while preserving the meaning." Type in your desired language. For this example, we've type in French . After typing in your desired language, click Generate for AI Assistance to translate your message.

• Review the AI translated email. Once approved, click the Insert Button.
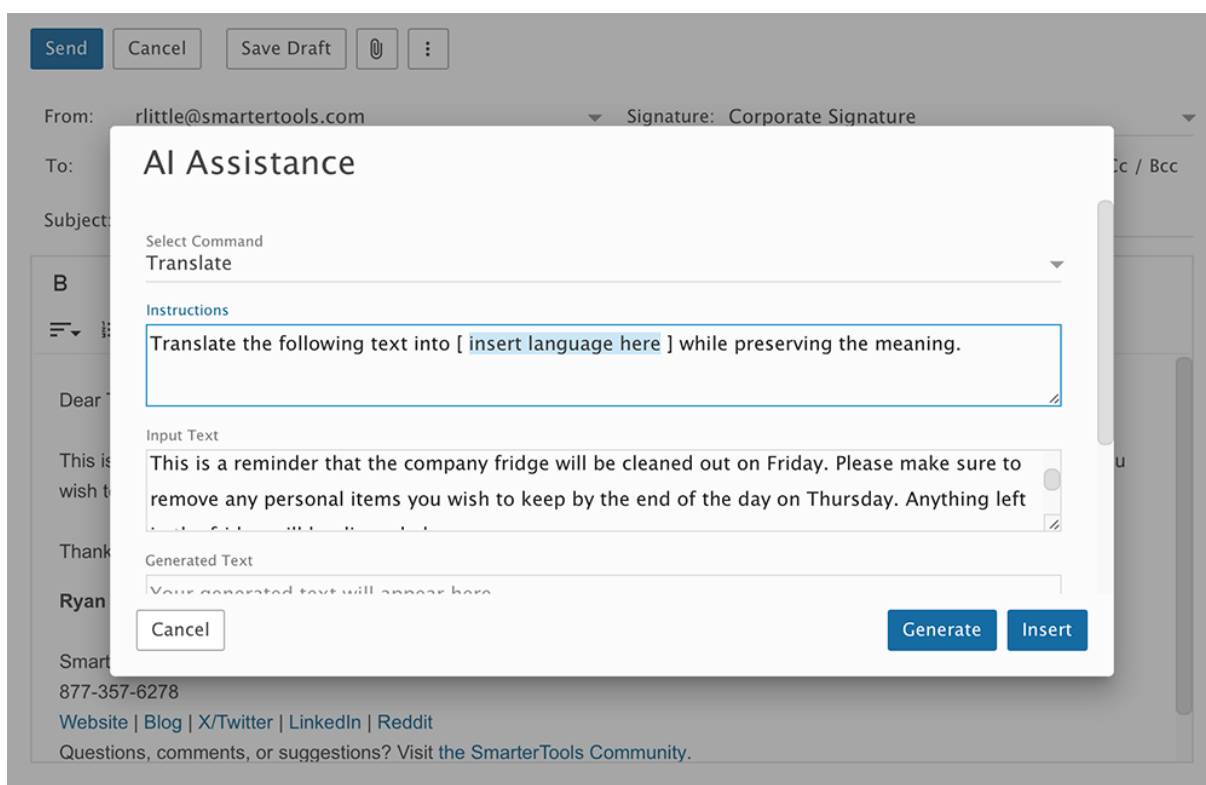
• Your translated message will be displayed within the body of the email. If necessary, adjust the formatting, such as font, color, or style to your preference. Once you're satisfied with the appearance of your email, simply click the Send button, and you're all set!
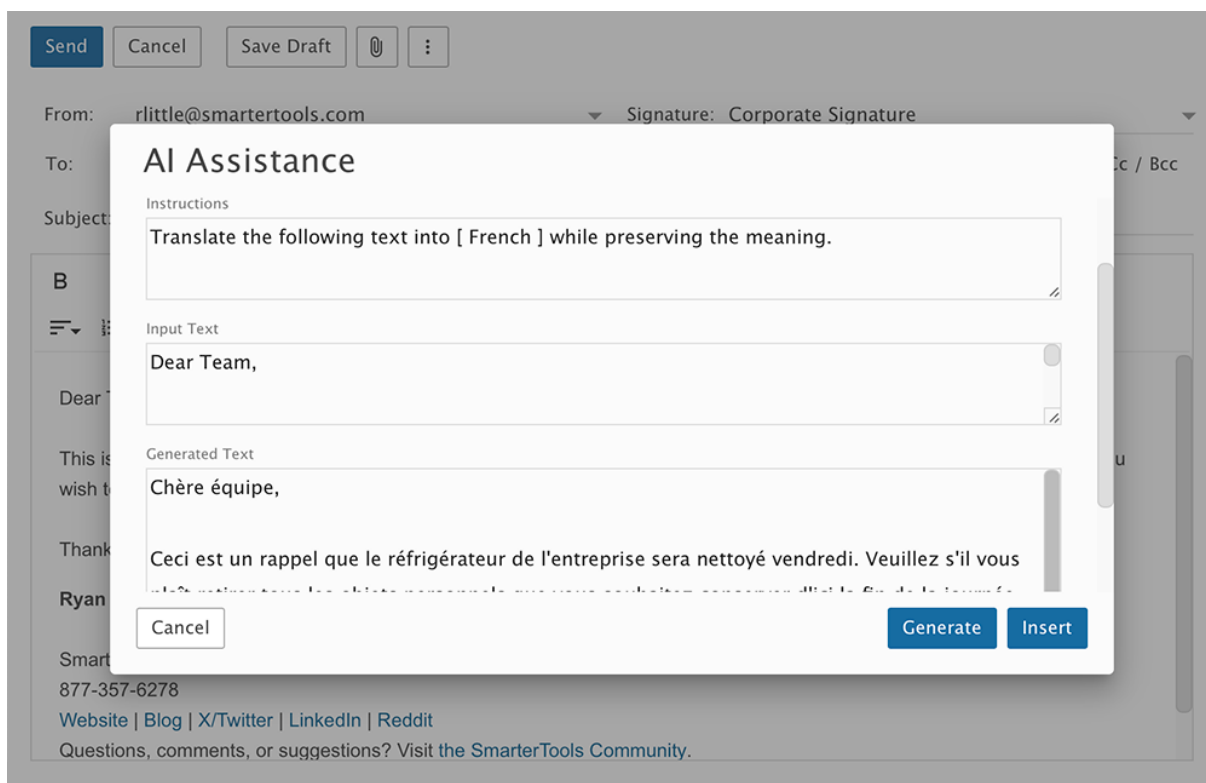
Note: Translations generated by AI may contain errors and should be reviewed for accuracy before use.
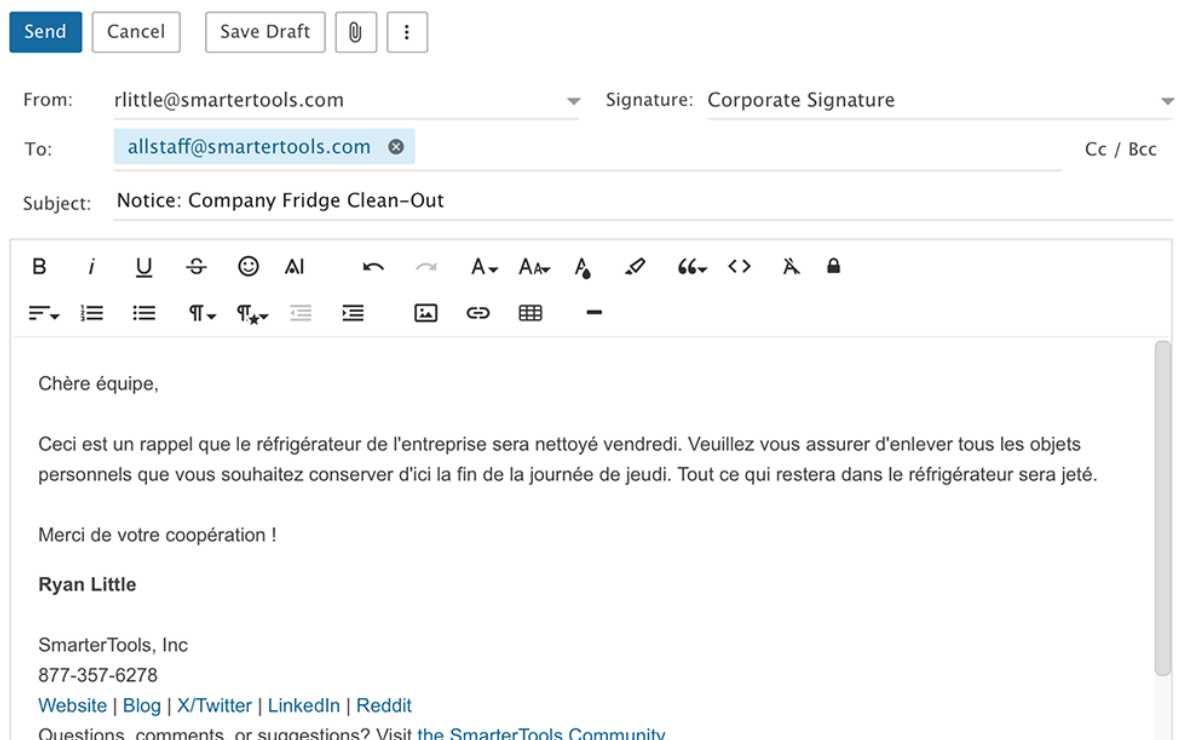
Modify the Tone of an Email with AI Assistance

Tone is everything in communication, but in the digital world, it can easily get lost, after all, we're reading words, not hearing them. SmarterMail's AI Assistance makes it easy to fine-tune your message by rewriting it in a specific tone: professional, casual, or business. The tone of an email sets the overall expression; formal, friendly, professional, or something in between, helping you ensure your message comes across exactly as you intend. For example, we asked AI Assistance to: "Write an email to all staff letting them know that the company fridge in the break room will be cleaned out every Friday afternoon, and any leftover items will be tossed."

The first draft comes off a bit serious, so we use AI Assistance to adjust the tone to something more casual. The result was a message that feels more friendly and approachable while still getting the point across.

> • To get started, in SmarterMail, click on New button. A dropdown menu will appear, select Email or simply click New to open a pop-up window. This will launch the email composition window (ensure pop-ups are enabled in your browser). In the editor toolbar, find and click the AI Assistance icon.
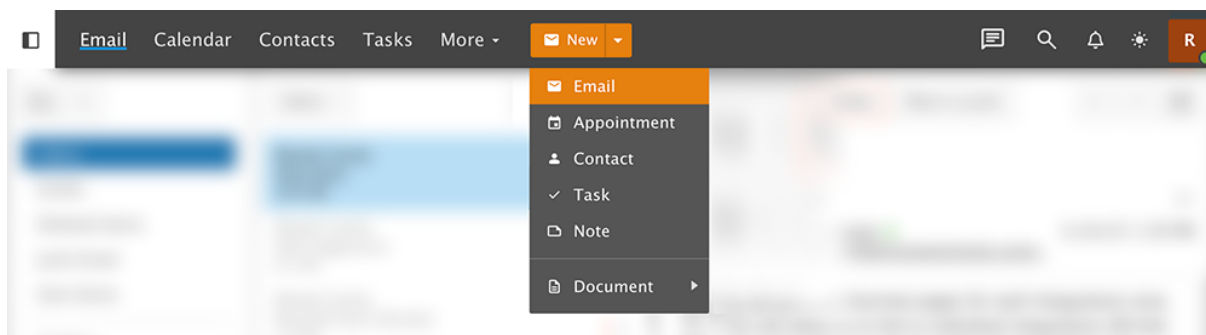
• The AI Assistance modal will pop up, you will notice that the Proofread option is already selected. Navigate down to Modify Tone .

• The Instructions box will contain the pre-set command: "Adjust the tone of the following text to match a [insert tone here, Professional, Casual, etc]." For this example, we're typed in Casual Tone . Click Generate for AI Assistance to generate the tone for your message.
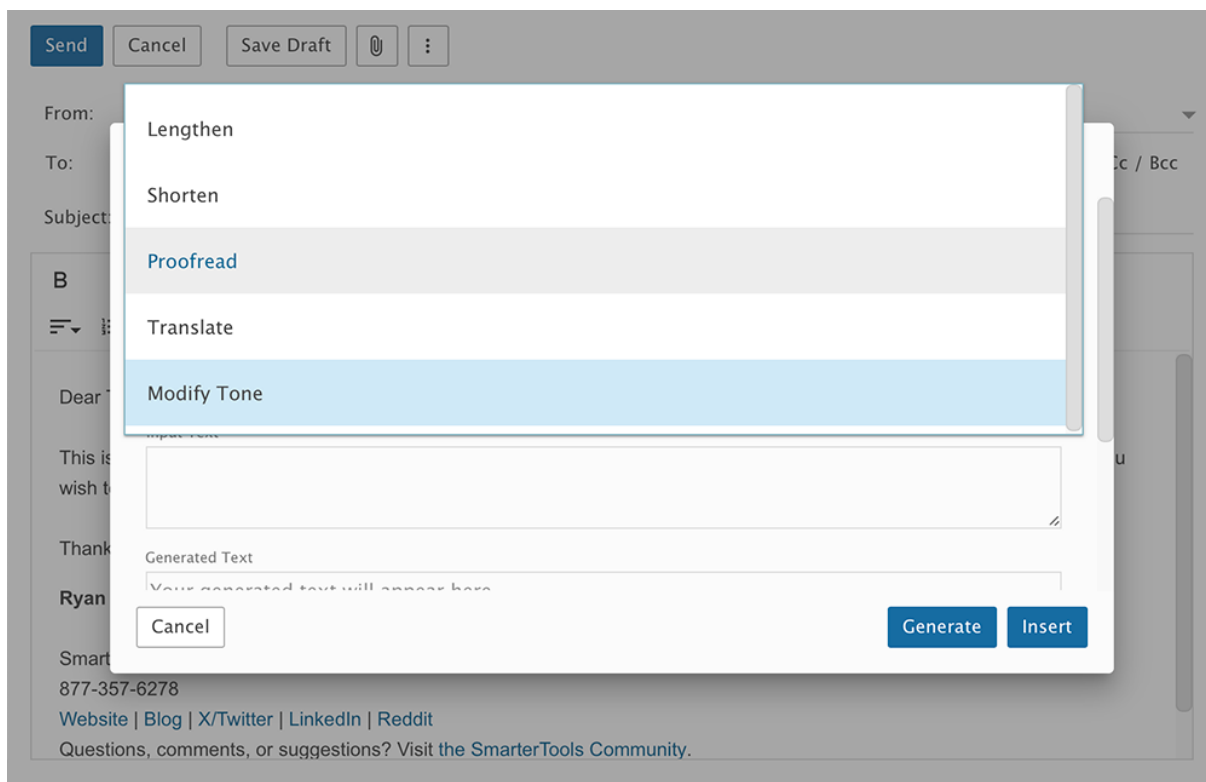
• Review the AI generated message to see if the content, clarity, and tone all work for you. If something needs adjusting, just type your changes in the Input Text box above, hit the Generate button, and your updated message will appear in the Generated Text box. Once approved, click the Insert Button .
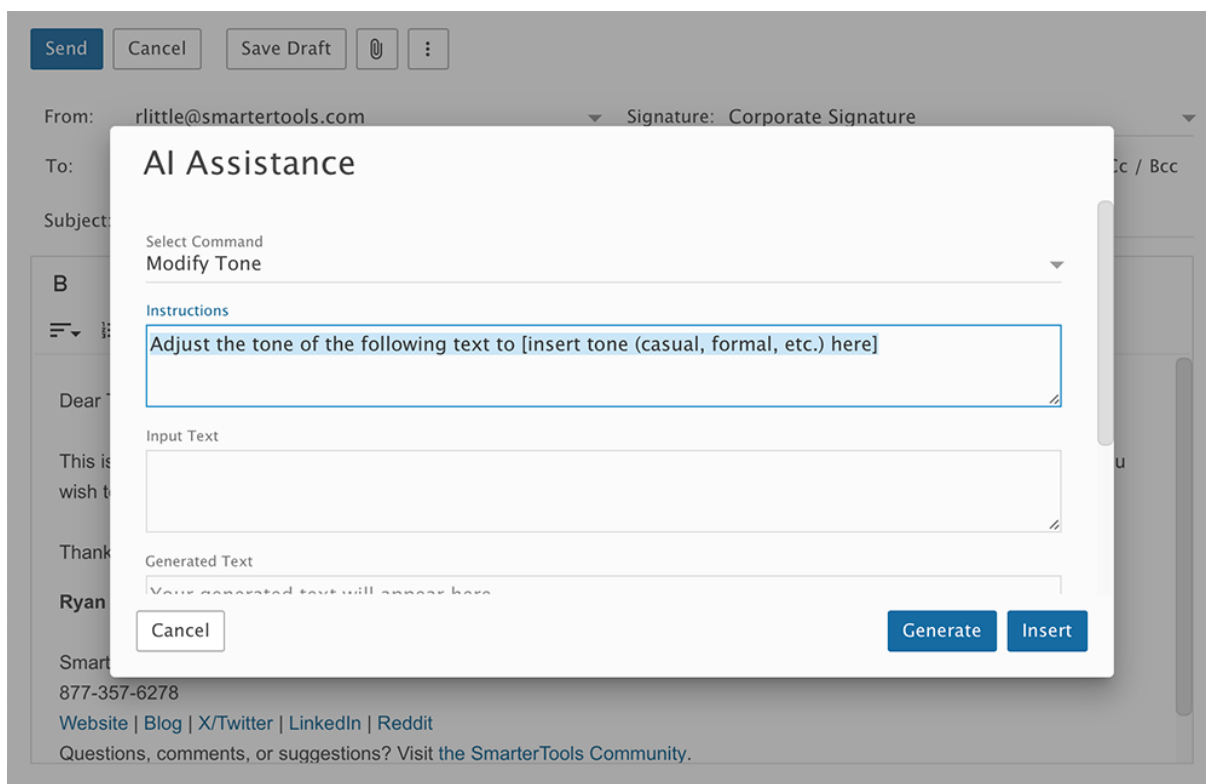
• Your AI generated message will be displayed within the body of the email. If necessary, adjust the formatting, such as font, color, or style to your preference. Once you're satisfied with the appearance of your email, simply click the Send button, and you're all set!
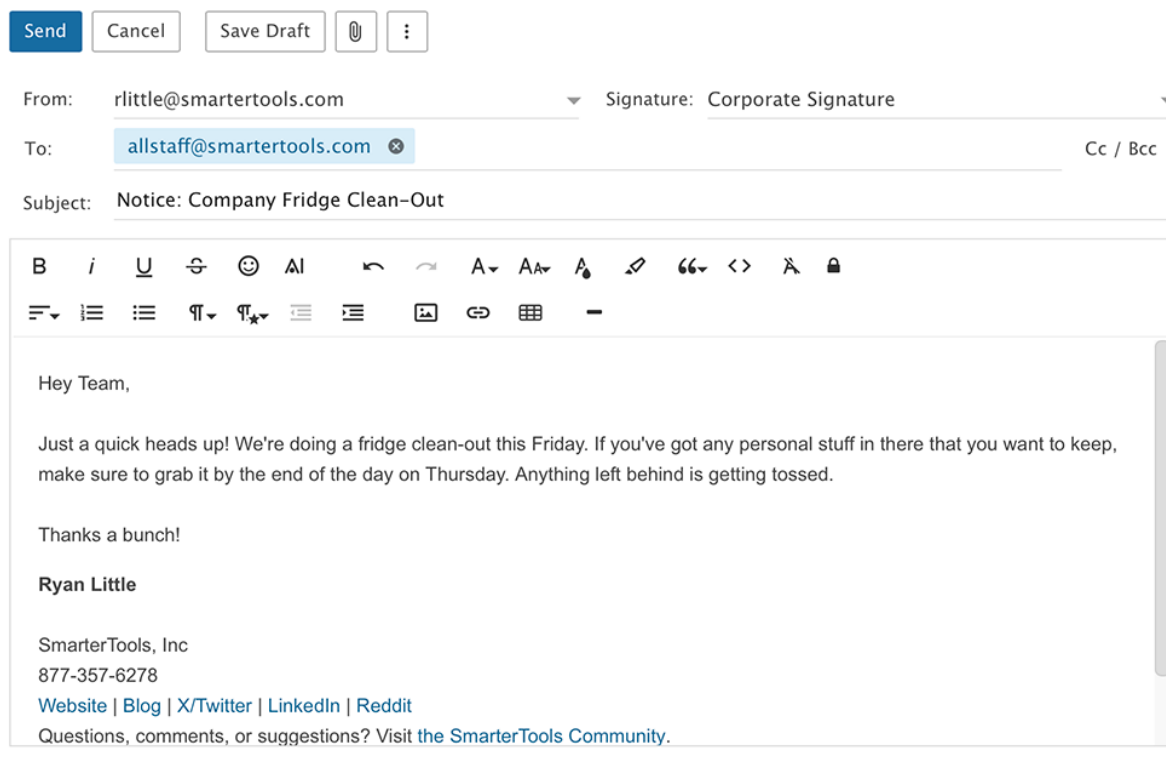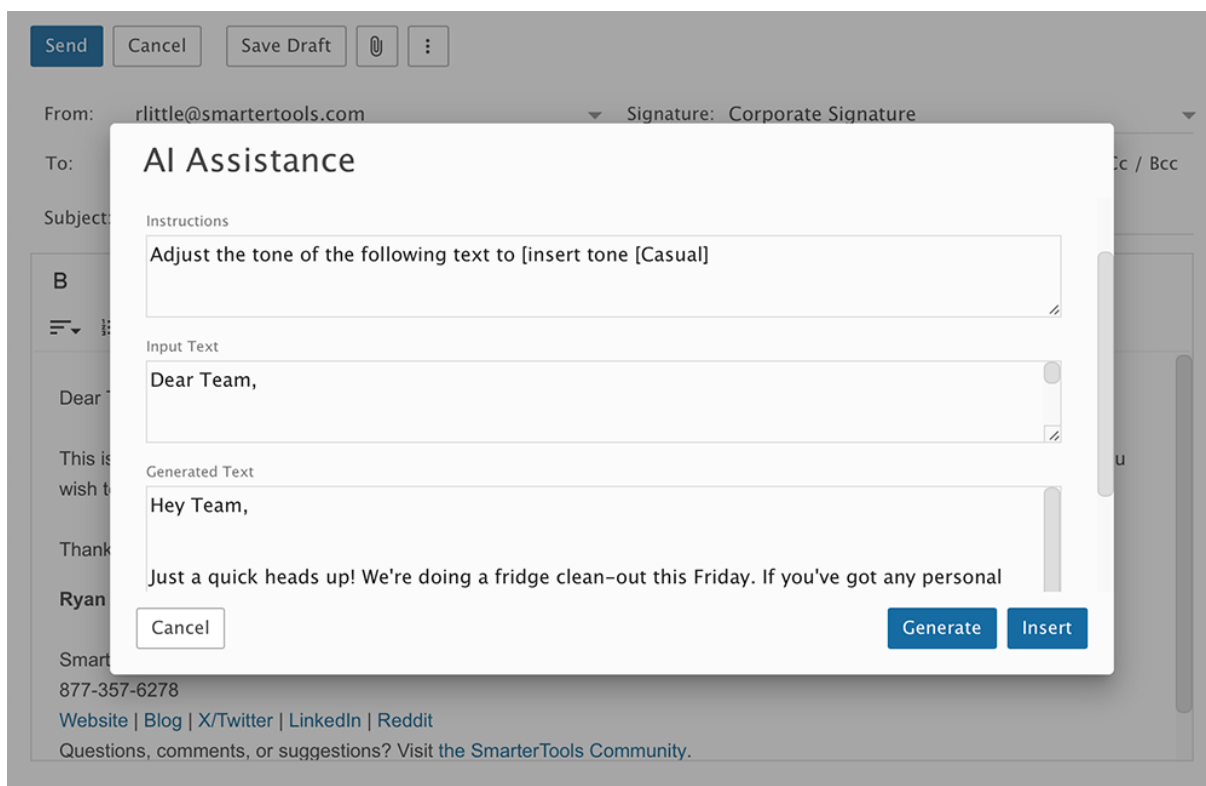
Searching Email Messages

SmarterMail indexes all of the messages you receive, regardless of how you organize them in your folders. As long as the message hasn't been deleted and purged from your account, the search tool will find emails quickly and easily. SmarterMail also offers an Advanced Search feature that allows you to search across all of your folders in addition to adding search criteria such as To and From addresses, search strings and more.

To perform a search, first go to the folder you want to search in. This can be your Inbox, Sent Items, Drafts, any of the custom folders you create for organizing your messages, or shared folders. Next, type the search criteria in the search bar located near the top of the messages view for that folder. Then use the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the messages within the folder you are viewing for matches and display the results. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."

It's also possible to use the Sort and/or Filter options on messages that were returned by your search so you can view messages that have attachments, that were replied to, that are flagged, that are linked to tasks or more. While not technically a "search", being able to sort and filter your messages using specific criteria can assist with finding the messages you need.

Advanced Search Overview

SmarterMail users can take advantage of SmarterMail's powerful and comprehensive indexing to search ALL folders within their mailbox. This includes folders outside of just "email" folders, such as in Contacts, Notes, Calendars, and Tasks. In addition, Advanced Search is performed outside of the mail interface, so users can continue using SmarterMail while the search progresses as well as view results once it completes. Search results are displayed with complete details (date/time, folder, etc.) making it easy to find the information you are looking for.

Advanced Search differs from a standard search as it allows users to add criteria to their search parameters so that specific items are returned. This criteria includes search words or phrases, To and From addresses, company names and addresses, birthdays, modification dates, start and end dates, and more.

Performing Advanced Searches

Once Advanced Search is selected, a modal window appears. Here, you select "where" you want to search: Everywhere, or within a specific area of SmarterMail. If you set Everywhere as your criteria, you simply enter your search string and SmarterMail will search throughout all areas. If you select a

specific area to perform your search, such as Contacts, you'll want to add search criteria to help narrow down your results.

Using the Add Criteria dropdown, you pick the criteria you want to use for your search. This is based on where you're searching, and so it can include:

Searching Email

- Search String: The words or phrases you want to search for. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."
- Folder: The specific Folder to search. If left blank, all folders are searched.
- Cc: The address a message was Carbon Copied TO.
- Contains Attachments - Whether the email must (or must not) have an attachment.
- From: The address a message was sent FROM.
- Received After The Year and Month after which the message was sent. For example, if May 2012 is entered, only results AFTER May 31, 2012 will be returned.
- Received Before The Year and Month before which the message was sent. For example, if January 2015 is entered, only results BEFORE January 1, 2015 will be returned.
- Subject: The complete or partial Subject of the message that was sent.
- To: The address a message was sent TO.

Searching Notes

- Search String: - The words or phrases you want to search for. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."
- Folder: The specific Folder to search. If left blank, all folders are searched.
- Color - The color designation of the note.
- Subject - The note's subject.
- Last Modified Before - The last modified date. For example, if January 2015 is entered, only "last modified dates" BEFORE January 1, 2015 will be returned.
- Last Modified After - The last modified date. For example, if May 2012 is entered, only "last modified dates" AFTER May 31, 2012 will be returned.

Searching Contacts

Using advanced search on Contacts gives you the ability to set up criteria based on every aspect available for a contact — over 20 different criteria in all — from their birthday through the website associated with the contact.

Searching Calendars

> • Search String: - The words or phrases you want to search for. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."

> • Folder: The specific Folder to search. If left blank, all folders are searched.

> • Calendar - The specific calendar you want to search. This can be your primary calendar, a shared calendar, a domain calendar, etc.

> • Ends After - The Year and Month after the appointment/event is set to end. For example, if May 2012 is entered, only results AFTER May 31, 2012 will be returned.

> • Ends Before - The Year and Month before the appointment/event is set to end. For example, if January 2015 is entered, only results BEFORE January 1, 2015 will be returned.

> • Starts After - The Year and Month after which the appointment/event is set to start. For example, if May 2012 is entered, only results AFTER May 31, 2012 will be returned.

> • Starts Before - The Year and Month before which the appointment/event is set to start. For example, if January 2015 is entered, only results BEFORE January 1, 2015 will be returned.

> • Subject - The name of the appointment/event.

Searching Tasks

> • Search String: - The words or phrases you want to search for. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."

> • Folder: The specific Folder to search. If left blank, all folders are searched.

> • Due After - The Year and Month after which the task is due. For example, if May 2012 is entered, only results AFTER May 31, 2012 will be returned.

> • Due Before - The Year and Month before which the task is due. For example, if January 2015 is entered, only results BEFORE January 1, 2015 will be returned.

> • % Complete - The completion percentage of the task.

> • Priority - The task's priority.

> • Starts After - The Year and Month after which the task is set to begin. For example, if May 2012 is entered, only results AFTER May 31, 2012 will be returned.

> • Starts Before - The Year and Month before which the task is set to begin. For example, if January 2015 is entered, only results BEFORE January 1, 2015 will be returned.

> • Status - The current status of the task.

> • Subject - The name of the task.

Once all choices have been made, use the Search button to initiate the search. The search results display in a separate pop-out window, with results listed in order. It's then possible to click on individual messages and open them in their own pop-out windows. (Messages must be opened

individually — it's not possible to check the box next to multiple messages and have them all open at once.) You can also select a message, right click on it, and download the raw EML file. Finally, it's possible to delete one or more messages by checking the box next to the message and using the Delete button. Messages deleted from Advanced Search will use whatever default deletion behavior you have chosen for your account. (I.e., moved to the Deleted Items folder, marked as deleted or marked as deleted and hidden.)

Deleting Email Messages

SmarterMail offers a few different methods for deleting messages:

- You can delete them using the Delete button in the webmail interface,
- You can right-click on the message(s) and select "Delete" from the context menu that appears, or
- You can use the Delete key on your keyboard. (Not the Backspace key, but the Delete — or Del — key.)

The action SmarterMail takes when you delete a message depends on the option you choose for the Delete Action on the Webmail card for your Account . These options include:

- Move to Deleted Items Folder - When items are deleted they are moved to the Deleted Items folder. If the Deleted Items folder does not exist, it will be created automatically the first time you delete a message.
- Permanently Delete - This option will permanently purge the messages after deleting them. note: When permanently deleting messages, the action is final. You will not be able to retrieve these messages later.
- Mark as Deleted - When the message is deleted with this option, the message remains in the current folder, but will be crossed out and marked as deleted. Once the Purge Marked as Deleted option is chosen from the Delete button dropdown in your inbox, all items marked for deletion will be permanently removed. Note: Messages deleted from the Junk Email folder are always permanently deleted and do not follow the Delete Actions that are set.)

It is important to note that the action taken for deleted items will ONLY be taken when deleting items through webmail. Deleting an item from Outlook or another email client will NOT use the setting that you choose. Note: When your email client connects to SmarterMail via POP3, any emails that are marked as deleted are automatically purged. To prevent this from happening, select the Move to Deleted Items folder option to avoid accidentally purging deleted items.

Undeleting Messages

Didn't mean to delete a message? You can retrieve deleted messages from your Deleted Items folder as long as the system hasn't been purged yet. Just open the Deleted Items folder and select the desired message(s). Then, simply click the arrow next to the Delete button in the webmail interface and select Undelete from the dropdown. You can also right-click on one of the selected messages and choose "Undelete" from the contextual menu that appears. Note: Your system administrator can permanently remove the messages in your Deleted Items folder at any time without warning, so don't delete messages if you might want them later. After the system purges any items marked for deletion, you can't retrieve the deleted messages.

Effects of Folder Auto-clean

Your system administrator may have established auto-clean policies that may delete older junk email, deleted items, and/or sent items when these folders get too large. However, they may have left the option available for you to override auto-clean settings. For more information, see Folder Auto-clean .

Flag Email for Follow Up

One method for managing email messages in SmarterMail is by flagging them so that they can be dealt with at a later time. For example, if you can't respond to an important message right away, you can flag that message as soon as you read it. This allows you to easily see that the message requires follow-up action.

There are a few ways for users to flag a message. The first is to simply click on the flag icon at the far right side of the message list in the All Messages view. Secondly, users can flag messages by selecting the option from the Actions (…) menu. You can also right-click on a message and select "Flag" from the context menu. Regardless of which method you choose, the flag icon will turn red and the message will also appear in the follow-up view, giving you easy access to all messages that require a further action.
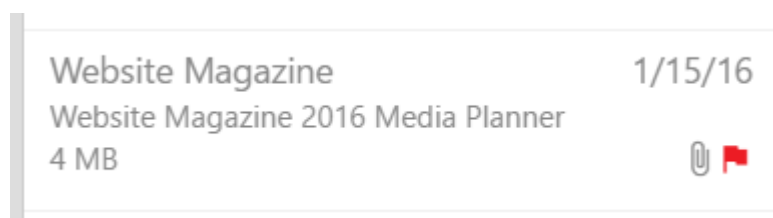
It should be noted that the ability to flag messages in SmarterMail is primarily intended to help users easily identify messages that need follow up. The functionality is supported through the IMAP

protocol and some sync protocols, such as MAPI/EWS and EAS, so that flagged messages will sync with email clients like Outlook and eM Client, as well as email clients on mobile devices.

Finding Flagged Messages

Although flags help messages stand out in a list, it may be difficult to find a specific flagged message if you have a lot of messages in your inbox. To quickly view all messages marked for follow up, use the Filter option. Filtering based on the flag status will display ONLY messages that are flagged for follow up.

Microsoft Outlook "Follow Up"

Within Microsoft Outlook, users have the ability to add a "Follow Up" flag to a message. They can then schedule that follow up for the same day, the next day, or various other periods. When this is done, Outlook places that in the "To Do List" area of Outlook. When using EWS/MAPI and synchronizing SmarterMail to Outlook, any message marked for Follow Up in Outlook is also flagged in the SmarterMail web interface. However, that message is not added as a Task in webmail. When the To Do List task is completed, the flag is removed.

Removing a Follow-up Flag

To unmark a message for follow up simply click on the flag icon or right-click the message and select "Unflag" from the context menu. It's also possible to remove a flag from the Actions (□) menu.

Linking Email to Tasks

Email conversations often result in the need to create one or more tasks. For example, an email exchange with a vendor may require updates to price sheets or shipping requirements. Perhaps an email from a significant other mentions an upcoming birthday or anniversary. Because of this, SmarterMail includes the ability to create a new task right from within an email message. This is called "linking" an email message to a task.

There are a couple of ways to add tasks to a message:

> • First, you can open and view the desired message. Once the message is open, simply select Add Task from the Actions (□) menu.
> • Another way is to select the message in the All Messages view, then right-click on the message and select "Add Task" from the context menu.

Follow these steps to generate and link a task from an email message:

> • Log into SmarterMail as a user and go to your Inbox, or whichever folder contains the email message you wish to link to a task.

• Select the message.

• From the Actions (☐) dropdown menu, select Add Task .

• A new window will pop out. In it, you can create the Task by filling out the pertinent details. Once saved, the task is created and automatically assigned to the email.

• On the email itself, a new Tasks tab will appear. On that tab is a brief overview of the task that was associated to the message, including the task's title, start and due dates. Clicking on those details will pop out the task details.

Finding Messages with Linked Tasks

To quickly view all messages that are linked to tasks, simply filter messages in the folder by selecting Linked to Tasks . Filtering in this way will only display emails that have been linked to tasks.

Managing Email Folders

On first glance, SmarterMail users will notice that their mailbox has five special-purpose, permanent folders that can't be removed or renamed. These folders will reside at the top of the folders list as well as being listed with any other folders a user creates. These include:

• Inbox - All incoming messages automatically go to your Inbox folder. You can read your mail in the Inbox, then delete it, move it to another folder or leave it in the Inbox. When creating folders, it's not recommended to create them within the Inbox as many email clients, especially mobile clients, have difficulty syncing folders created within the Inbox. Note: If you have set up content filtering for your mailbox, incoming messages may bypass your Inbox per your content filtering settings.

• Drafts - This folder holds messages that you've composed but haven't sent yet. A message saved in your Drafts folder stays there until you either send it or delete it.

• Deleted Items - When you delete messages, by default they're moved to the Deleted Items folder. (Just know that, this default action can change based on your settings - see Deleting Email Messages for more information). Messages in the Deleted Items folder can be deleted at any time without warning depending on any auto-clean settings your system administrator has in place, so it's best if you don't delete messages if you think you'll want them later. The Deleted Items folder is the default folder SmarterMail creates for deleted items. When migrating from other email systems to SmarterMail, the migration may create a different folder for deleted items based on what that email system uses as its default.

• Junk Email - Messages SmarterMail believes to be junk mail bypass your inbox and go to the Junk Email folder. You should periodically check this folder to ensure that valid messages were not accidentally delivered to the Junk Email folder. If you find valid emails in your Junk Email folder, you can move them back to your Inbox by either dragging them to the Inbox or using the

right-click context menu. If the sender is someone you know, you can also add them as a Trusted Sender using the right-click menu, thereby skipping most spam checks for messages from that sender in the future.

• Sent Items - All outgoing messages are automatically saved to your Sent Items folder, making it easy to review or resend a message if necessary. Note: Messages sent from a third-party client such as Outlook may or may not be saved in the Sent Items folder. It is dependent on the protocol used to connect that client.

The folder icon at the top of the folders view contains the following actions:

- New Folder
- Share Folder
- Run Content Filter
- Disposable Address
- Delete All in Folder

When you right-click a folder, bringing up its context menu, or when you select a folder and click the Folders icon, you will see a list of available actions (which might vary depending on the type of folder):

- New Folder
- Move Folder
- Edit Folder
- Delete Folder
- Share Folder
- Manage Shares
- Run Content Filter
- Disposable Address
- Delete All in Folder

Creating a New Folder

To make your email easy to manage, SmarterMail lets users create as many personal mail folders as they want. Personal folders help users organize incoming and outgoing messages in ways that make sense to the individual user. That being said, creating a very large number of folders that have large numbers of sub-folders can impact the performance of any email server, not to mention syncing with email clients. Note: When creating new folders, DO NOT create sub-folders within your Inbox. While technically possible, many third-party email clients and most mobile devices can not accurately and reliably sync sub-folders that are part of a user's Inbox.

To create a new Folder:

- Click the Folders icon at the top of your folders list.
- Select New Folder from the dropdown menu. Or, you can right-click anywhere in your list of folders and choose New Folder from the context menu.
- A New Folder window will open.
- In the Parent Folder field, choose an existing folder to create a sub-folder under it, or select Root Folder to create a new top-level folder.
- Type the name of your new folder.
- Click Save .

To make your SmarterMail folders available from a third-party email client such as Microsoft Outlook, when you set up your client you will need to set it up using IMAP as your incoming mail server type, or use one of the add-on protocols: EAS and/or MAPI & EWS. If you use POP mail, you only have access to your SmarterMail inbox, not any personal mail folders you created to organize messages. note: SmarterMail does not allow the following characters to be used in folder names:

```
? | | : * ? " . u000 (a unicode null character) and leading/trailing spaces
```

When importing folders, it's likely SmarterMail will replace those characters with an underscore (_). For example, if a folder is named "Problems?", the folder would show up as "Problems_" in webmail after import. (Quotation marks are not part of the folder name in the example.) Folders in webmail can be renamed to remove the underscore characters, but none of the restricted characters can be used in the rename.

Moving Folders

Once a folder is created, it's possible to move it to a new location. For example, say you have a folder for each month of the year, and you move messages received in a particular month into its particular folder. Then, at the end of the year, you want to move those monthly folders into a new Year folder. (E.g., You move January - December folders into a 2022 folder.) It's very simple to do that. NOTE: You can only select one email folder at a time, so each folder needs to be moved individually.

Simply right-click on a folder and select Move Folder from the context menu. The Move Folder modal opens, and you simply select the folder you want to move TO from the "Move To" dropdown. Once you've selected the proper folder, click the Move button. Then, you can do the same for each folder you want to move.

Moving Messages to Another Folder

Moving messages between folders in SmarterMail is easy. You can either move them using the Actions menu or right click on one message, or a selected group of messages, and use "Move" from the context menu. It's also possible to drag one or more messages from one folder and drop them into another.

Editing and Deleting Folders

You can change the name of a personal/custom mail folder anytime by simply editing it, or delete a folder (and its messages) completely when you no longer need it. note: It's not possible to rename any default folders.

To rename a folder, select the appropriate folder in the navigation pane. Use the Folders icon (or use the right-click context menu) and select Edit Folder from the pop out menu. In the New Folder Name field, type the new folder name you want to use.

To delete a folder, select the appropriate folder in the navigation pane. Click the Folders icon (or use the right-click context menu) and select Delete Folder . Deleting a folder also deletes all messages within that folder.

Sharing Folders

There are 3 ways to share email folders, two of which are available right from the Email page in the webmail interface:

- Using the Folders icon,
- Using the right-click context menu, and
- Using the Sharing page of your Settings.

When using either the folder icon or the right-click context menu, you simply select a folder, then click on the folder icon or right-click on the folder name. Either way, you select Share Folder from the menu.

When you do this, the Share Folder modal opens. Here, you can add in Users or User Groups to share the folder with, then set the permissions for each share you create. For more information about sharing, and the permissions available for users and User Groups, see the Sharing Overview page of this help documentation.

Manage Shares

Opens the Sharing page of your settings. This allows you to see and manage those items shared with you, items you've shared with others, and any Delegation settings.

Run Content Filters

Opens a modal window that allows you to run one or more content filters against the messages in the folder. For more information, see My Content Filters .

Disposable Address

A Disposable Address is a randomly generated address, completely independent of a user's current email address. This address acts as a timed alias, forwarding mail to a specific folder for however long specified. When the time limit has been reached, the address is no longer valid and mail will not reach the mailbox — it simply bounces back to the sender. This is useful when you only need a temporary sign up or don't want to give out your email address and possibly get inundated with spam messages.

Creating a Disposable Address

You can create a Disposable Address using the menu option at the bottom of the navigation pane, or by right-clicking on a specific folder and selecting Disposable Address from the context menu. When you create the address, SmarterMail will automatically create the username, but you have the ability to select the folder where the messages to that address are delivered, plus the length of time you want to use the address. At any time you can either extend that timeframe or disable the address entirely.

Disposable addresses are created using a randomly generated character set. As such, it's important to copy the address so it can be used as needed. If you forget the address, you can see it again by clicking on the linked text in the notification discussed below. Only one Disposable Address can be used at any one time.

Locating a Disposable Address

When you have a Disposable Address in use, you'll be reminded of it with a notification that appears at the top of your custom folders list with the following message: "A disposable address is active on this account. Expires in X." The "X" in the message is the amount of time the address will be in use. Clicking on the message opens a modal with the details of the disposable address, including the address itself, it's time remaining, the folder being used for the address, and the ability to Revoke (delete) the address or extend its time.

If you need to edit the address, you can simply click the linked text in the notification to open the Disposable Address modal.

Delete All in Folder

Deletes all contents of the selected folder. This includes messages, sub-folders, etc. Note: This action cannot be reversed, so be sure you want to perform this action before you actually carry it out.

Message Archive Search

This feature is only available in SmarterMail Enterprise edition.

Message archiving is a method of storing all email traffic for a domain — either incoming messages, outgoing messages, or both — in a separate location on the mail server. Typically, this is a feature

used for companies that need mail servers to be in compliance with certain regulatory guidelines, such as the Sarbanes-Oxley Act of 2002 .

When archiving is set up, messages are automatically archived as soon as they hit the spool and before they are handled by any spam and/or content filters. This means that all messages are archived, not simply those that are delivered to a user's mailbox. (The exception to this rule is messages rejected due to SMTP Blocking. If a message is rejected due SMTP Spam blocking, it will never hit the spool and, therefore, will not be archived.) On a nightly basis, SmarterMail zips up archived messages and stores them to conserve disk space on the mail server. However, zipped messages are still searchable.

By default, SmarterMail does not archive any messages. To specify which domains are archived, the system administrator will need to create archiving rules. Rules can be set up for the system as a whole, so all domains are archived, in the system's General settings, or archiving rules can be set up on a domain-by-domain basis on each domain's Configuration tab.

Search Results

If message archive searches have been performed, they'll be listed when navigating to this page. Otherwise, this page will be blank and a new search needs to be initiated. If there are searches that have been completed, you will see the following:

- Summary - Here, the general details of the search is listed. This includes the search parameters including things like whether the search is for "messages sent to:" a particular user, "messages sent by:" a particular user, the domain or user, and the dates searched.
- Matches - The number of items than matched the search parameters.
- Status - Whether the search completed or not, and date and time the search was performed.

Each set of results can be viewed by simply clicking on it, and the results are displayed. Searches can be manually deleted as well by simply selecting a search and clicking the Delete button.

Searching Message Archive(s)

When performing a message archive search, the following search strings will be available: filter for all domains or a specific one, date range, the sender's address, the recipient's address or the subject.

SmarterMail's archiving feature saves any inbound message, outbound message, or both, depending on the Rules that are set up for the domains. That means any spam message, junk message, messages that are eventually deleted, etc. are all saved. That means the ability to find messages, and then perform some action on those messages once found, is extremely important. This is especially true in environments that have compliance guidelines that need to be followed.

When message archiving is set up for a specific domain, that domain's administrator can find a Message Archive Search within the domain's Settings . System administrators can search across any and all domains, regardless of the Rules that are set up. Regardless of whether a domain administrator or system administrator is performing a search, the following is available for search criteria:

- Start and End - The start and end dates for the search.
- From - The email address the message is sent from.
- To - The email address the message is sent to.
- Subject - A word or phrase that would be in the subject line. If a person wants to find all messages From or To a particular address, this can stay blank.

After a search is performed, and results are found, there are a few actions that can be taken on one or more of the search results:

- Download / Download All - This will download a copy of individually-selected messages, or all messages. Whichever is chosen a .Zip file gets downloaded. The messages are saved in their original .eml format and can be opened by an email client, email utility or any other standard program that can open emails. Note: Downloads are limited to 2GB in total size. Therefore, if you choose "Download All", should the total size of the .Zip file be over 2GB, the download may not complete. If this is the case, it may be necessary to change your search to limit the results, or break your search up into multiple queries. For example, breaking a full year's search into quarterly searches.
- Copy to Mailbox / Copy All - In certain instances, it may be necessary to move messages to a separate mailbox. For example, in a situation where an outside organization, like an auditing company, requires access to certain messages. In these cases, a separate user can be set up for the organization, and any messages found via Archive Search can be moved to that new user for later review. Messages can even be moved to a specific folder, or specific folders, within that new user so they're contained and easily organized. Individually selected messages can be copied using Copy to All, or all results can be copied using Copy All.

Search Results

Results from archive searches persist for as long as they're needed. Each set of results appears in a grid so they can be retrieved as often as necessary. Once they're no longer needed, they can be closed out, and removed from the list.

Calendar

Calendar Overview

SmarterMail's calendar feature takes the burden out of organizing your schedule and is accessible simply by using a standard web browser on any desktop, laptop or mobile device. Calendars can also sync to desktop and mobile email clients, calendar apps, and more. SmarterMail's calendar system is extremely flexible and includes many options that make it easy to keep track of important events, including:

- The ability to create and sync multiple personal calendars.
- Fully configurable appointments with optional recurrence rules.
- Email notification and notification within SmarterMail of upcoming appointments.
- Overlay view to display multiple calendars, tasks and conference rooms on the same calendar.
- Invitation send status. (I.e., a banner appears on an appointment if the invitation has not been sent.)
- Attendee and invitation status tracking.
- Conference room availability and scheduling.
- Attendee availability information.
- Online meeting creating and scheduling, which means you can create an online meeting to be used for a meeting as part of creating and sending the meeting invite.
- Complete integration with Outlook (for Windows and macOS), eM Client, mobile apps, and more.

To view multiple calendars or tasks at once, simply click the checkbox next to the resource you want to show/hide. The options available are based on a user's personal calendars and task list plus any shared calendars, task lists or conference rooms that have been shared with you and subsequently mapped to your calendar.

Navigating Your Calendar

By default, when you first access your calendar, the Agenda view will be displayed. This view displays all of the meetings and appointments that are scheduled for the following 2-week period, beginning with the current day. You can change this view to whatever you like, and when you close your browser, SmarterMail will store which view you were last using, then open that view the next time you open your calendar. If you delete browser cookies, the calendar view will reset to the Agenda view. Essentially, there are five (5) different Views that toggle between the different ways that SmarterMail displays your events:

• Month - The monthly view displays all appointments and tasks scheduled for the month, with the current day highlighted. It serves as an at-a-glance type of calendar that outlines a general idea of the upcoming events over the next 30 days.

• Week - The weekly view is intended as more of an agenda-type view and displays all appointments scheduled for the week. If configured, this view also displays the start and due dates for tasks.

• Day - The daily view is a planner-type view that displays all appointments scheduled for the day. If configured, this view also displays any applicable start or due times for tasks.

• Agenda - The Agenda view mimics the Month view, but instead of displaying all appointments and events as a calendar, a rolling 14 days is presented in list form, starting with the current day. Shared calendars and resources can be shown or hidden, and the list can then be printed out and handed to a personal assistant or other individual.

• Schedule - A horizontal view of your subscribed calendars with the time of day arranged vertically. This allows you to organize your day by seeing the appointments you have at what time, and on which calendar. The current time is shown with a horizontal red line.

• Timeline - Similar to Schedule view, but the time of day is arranged horizontally and each of your subscribed calendars is arranged vertically. The current time is shown as a vertical red line.

• Grid View - The Grid View displays all events in your calendar, each on its own line. Every event and appointment is listed only once: recurring tasks are denoted with a check mark in the "Recurring" column. The All Appointments view makes it easier to find appointments and events as virtually everything in your calendar is listed in one area and easily searchable. Note: Tasks, availability-only shared calendars and conference rooms are not displayed in the All Appointments view. Recurring events that have expired (will no longer recur) are displayed with a checkmark in the Recurring column but will show an (Expired label on the End Date).

There are a few ways to distinguish between the various types of appointments and events:

• Each calendar source has its own color, so you can easily distinguish which calendar the event belongs to. These colors can be customized at any time.

• All-day appointments only appear at the very top of your calendar when viewing appointments by Day or Week, or viewing your Schedule.

• Recurring events are denoted with circular arrows to the right of the appointment listing.

In general, the following options are available when viewing calendars:

• View Selector - Allows you to select how you want to view your calendar: By Month, Week, or Day, or viewing as an Agenda, Schedule, Timeline, or Grid.

• Choose Date - Allows you to select a specific day, then go to that day.

• Filter - Allows you to filter the events in a specific calendar based on whether appointments have attachments, or by their category. For more information, see Categories .

• Actions (☐) -

• Add to Outlook - Select Add to Outlook to import all calendar appointments to Microsoft Outlook for Windows. note: Add to Outlook is not available for Outlook for Mac.

• Subscribe to Calendar - This allows you to subscribe to internet/web calendars, such as a sports teams' schedule, the payroll calendar from your payroll provider, a holiday calendar you find on the internet, and more. Note: When viewing subscribed calendars on a mobile device synced via EAS, that calendar may allow edits. However, those edits do not sync back to the web calendar, and while they may appear on the user's calendar who edited the item, that edit will be overwritten the next time the subscribed calendar updates from the source.

• Import ICS File - An ICS file is a calendar file that's saved in a universal format that can be used in several email and calendar programs, including Microsoft Outlook, Google Calendar and Apple Calendar. When moving from one of these applications, SmarterMail can import your existing ICS so you'll have any and all events and appointments set up in your previous calendar app.

• Print - Prints the data displayed in the current calendar view.

• Day/Week/Month Navigation - At the top, right of the calendar view are Previous and Next arrows that allow you to move your view forward and backward. That means, to the previous/next day, week or month, depending on which view you're using. There is also a Today button that returns you to the current day, or to the week or month where the current day is located.

Viewing Calendar Event Details

When looking at your calendar in webmail only the barest details are initially displayed in order to save space. However, there may be times when you want to view more information about a specific appointment.

Mousing over an appointment will open a modal window (no clicking is required) that shows you more detail about a given appointment. This gives you a quick, all-encompassing view of the appointment with details such as the date/time of the appointment, the location, and the organizer. Additionally, you can click on the calendar item. This opens the item in a pop out window, giving you all of the information about the appointment. This includes information like the list of attendees, a description of the event (if one was written), the event's location, the ability to view and/or download any attachments that were added to the appointment, and much more.

Sharing and Shared Calendars

SmarterMail gives users the ability to share their primary or secondary calendars with others who share the same domain name. Shared calendars — whether you've shared them or they're shared with you — are automatically "mapped" to the people they're shared with. So nothing needs to be done once a calendar is shared.

Shared calendars appear under the Calendar View area. By default, each user has a personal calendar called "Calendar." This is where you create your appointments. You have the ability to share this calendar with others, or you can create additional calendars and share those as well. Any calendars shared with you will also appear in this list. For more information on how to share your calendar, or map to a shared calendar, take a look at the Sharing Overview page in this help documentation.

Sharing and Shared Tasks

Just as with Calendars, SmarterMail gives users the ability to share their tasks with others on the same domain. In addition, users can "map" tasks that others share. The difference is that tasks do not necessarily need to appear in your calendar. The ability to display task start and end dates, as well as completed tasks, is set in the Calendar Settings area.

If tasks are set to display in your calendar, then Tasks, the default task list created for you, and any shared and mapped tasks, appear under the Shared Calendars area. For more information on how to share your tasks, or map to shared tasks, take a look at the Sharing Overview page in this help documentation. Note: Even though tasks may be displayed in your calendar, if you are syncing your calendar with a desktop and/or mobile email client, the task will not show up on your calendar. Instead, they will generally be considered notifications and will display in mobile and/or desktop clients accordingly.

Improving Calendar Responsiveness

For the best calendaring experience, a user's calendar files should not exceed 3 - 4MB. SmarterTools recommends that users enable Calendar Auto-Clean to keep past calendar events from cluttering up their calendar views and exceeding the recommended size limit.

System administrators can set the default Calendar Auto-Clean setting for a domain within the domain's configuration settings. The User Defaults template can then set a user's Calendar Auto-Clean setting to use that Domain Default or set it to Never, 3 Months, 6 Months or 12 Months. Domain administrators may also modify this setting per user in the user's configuration options. Please Note: that although system and domain administrators can enable Calendar Auto-Clean for a user by default, the user may still adjust the setting or turn it off within their Calendar Settings. Therefore, it is

important to monitor user' calendar files periodically and contact users that are exceeding the recommended limit.

Creating New Calendar Appointments

It's very easy to create a new calendar appointment in SmarterMail:

- • Use the New button in the menu bar,
- • Select Appointment from the New menu dropdown, or
- • Just select a day/time you want to create the event in your calendar. Alternatively, you select ANY day/time in your calendar, then just change them as needed.

Regardless of how you decide to do it, creating a new event pops-out the new event window.

Saving Appointment Details

When you add a new appointment to your calendar, you can save as much or as few details about the appointment as you like. In general, appointment details are handled by a few different cards:

General Details

The first card carries the actual details of the appointment or event you're creating. It can be a lunch or dinner, a meeting, an anniversary or birthday, or virtually any other type of event you want to keep organized in your calendar. To create an Event, you will need to include the following information.

- • Subject - The subject is the friendly name for the event you're creating, such as "Lunch with Joan" or "Weekly Marketing Meeting".
- • Location - This is where the event will be taking place. The location can be a room or building, an address, or even some descriptive text, such as "via Webex". Regarding "Conference Room" versus "Location", these are mutually exclusive, yet compatible fields. That said, while the Location is something you enter on your own, the Conference Room will be a shared resource that was set up by your domain administrator.
- • Description - This space is used for details about the meeting: Agenda items, web conferencing log-in details, etc. Anything typed in the Description will also be added to the appointment so attendees can see the detail as well. The description card uses an HTML editor so that items like hyperlinks can be included. Note: The Subject, Start and End dates are the only fields required to save an appointment.

Date and Time

This card allows you to actually set the date and time of the appointment. If need be, the time zones can be changed so that appointments can be created in a specific attendee's time zone.

• All Day Appointment - Enable this if the appointment you're creating will last the entire day. When enabled, the Appointment will move to the very top of your calendar list when viewing in Week or Day view. On Month view, it will be the first Appointment shown for the specific day.

• Show Time Zones - Enable this setting to allow yourself the ability to create Appointments in a time zone different than your own. When enabled, a Time Zone drop down appears beneath the Start and End dates for the Appointment, allowing you to set the proper day and time based on the Time Zone selected.

• Start and End Dates and Times - A Start Date is required to save the event. By default, Events start as the current date and time and end 1 hour later. These fields are fully customizable.

Recurrence

Use this card to set how often this particular appointment will occur: Once, Daily, Weekly, Monthly or Yearly. Note: When setting the End date for a recurring Appointment, SmarterMail, Outlook for Mac, and eM Client all treat the "end by" date as the LAST day that a recurring instance can happen. However, Mac Mail seems to treat it as the first day that the recurrence cannot happen. That means in Mac Mail, the last occurrence of that event will be the day BEFORE the date you put in the "End By" area in SmarterMail. You will want to take that into consideration when creating recurring appointments.

SmarterMail also offers some flexibility when setting up recurrence rules. For example, it's possible to set the event Frequency based on some criteria. For example, an event can be scheduled to occur on a specific day, or a certain day of the month like the last Tuesday, on the fourth Friday of the month, etc.

Regarding the creation of recurring appointments that happen on the "last day" of the month, or "last week/weekend day", while it IS possible to create these types of recurrence rules in webmail, they may not sync to various mobile and/or desktop clients due to limitations of syncing protocols. (Exchange is the same, so it's not a SmarterMail limitation.) For example, testing a few (but not all), we found the following:

• iOS - iOS Calendar does provide a way to create "custom" monthly repeating events by last day, last weekday, or last weekend day. However, it does not properly sync the recurring information through EAS.

• Windows Mail - Does not provide an option to sync last day, last weekday or last weekend day.

• Standard Android Calendar - Does not provide an option to sync last day, last weekday or last weekend day.

• Outlook Mobile - Does not provide an option to sync last day, last weekday or last weekend day.

Online Meeting

This card allows organizers to have an online meeting space created, automatically, to be used for the appointment that's being set up. The online meeting will use the appointment's Subject as its name, and the meeting will appear in the Online Meetings area of the organizer.

Once clicked, a few options are available, some of which can be customized for the meeting. (The Meeting Link cannot be changed.) These include:

• Online Meeting Password (optional) - By default, meetings do not have passwords. However, if you want to secure the meeting, a password can be added, the confirmed.
• Allow attendees to start the meeting - Use this toggle if you want attendees to be able to start the meeting before you, the organizer, arrive.
• File upload permissions - By default, meetings are created to allow only organizers to upload files. However, this can be changed to allow just authenticated users or "Everyone" (i.e., guests) to upload files.
• End behavior - This setting is for how you want the online meeting handled once it ends. It can be ended and archived, it can be deleted, or it can be "kept active", which means the online meeting can be used again at a later time. Note: If an appointment that has an online meeting associated to it is cancelled or otherwise deleted, the meeting is not deleted immediately. Instead, SmarterMail runs a nightly routine that will remove online meetings associated with deleted/cancelled appointments.

Attendees / Resources

Attendees are the people you want to invite to your event. When adding Attendees, each will receive an event invitation that they can either accept or reject. You will receive notifications back regardless of whether attendees accept or reject the invitations. In addition, it's possible to see whether your invitation was sent or not: When viewing an appointment in your calendar, if it has NOT been sent, there is a banner at the top referencing this fact. This allows you to re-save the appointment and send the invitation to your attendee(s).

To add attendees, simply start typing their email address. SmarterMail will suggest contacts from your various contact lists, including the Global Address List (GAL), as well as cycle through contacts you have listed in categories. You can finish typing the address or select the proper address from the options available.

If your domain administrator has added any shared resources, like conference rooms or equipment, they will be listed in this dropdown. Just as with attendee availability, if a conference room, or piece of equipment, is already reserved for a specific day and time an Event is to be set, this information will display in the Conflicts field of the new appointment window. Conference room and equipment

availability will also show when users select View availability on the Attendees card. In fact, both conference rooms and equipment will have internal addresses created, based on their name. These do not count as actual user accounts, so there's no licensing impact. Some protocols, like MAPI, require these resources to be actual attendees of a meeting or event. In addition, having actual addresses for each resource makes it easier to gauge availability for these resources.

As for whether an invitee or shared resource is available or not, once you've added in one or more attendees, or selected your resource, you can use the "View Availability" to let you know whether attendees are available on the day and time you're planning your event, and/or if the conference room and/or equipment you want to use is available. If there are conflicts, either with an attendee or with a resource, a yellow warning will appear on the New Event window letting you know so you can use "View availability" to see the conflicts. If a resource was reserved for an event, when clicking on that room reservation in your calendar you can see who made the reservation. Generally, this will correspond to the organizer of the corresponding event. Note: Availability is only offered for users of the same domain as the event organizer. External domains, as well as information for users of free email services such as Gmail or Microsoft 365, is not accessible. This also helps with availability requests: if a resource is unavailable, the meeting organizer will receive notification letting them know the resource is unavailable.

People / Equipment Icons

	In addition to simply typing in the name/address of an invitee, it's possible to select invitees from a list. To do this, simply use the "people" icon. This option opens a modal window and, from here, you can select invitees based on a folder (i.e., Contacts, Global Address List, shared Contacts, etc.) or even display contacts based on a category. When a choice of folder or category is made, contacts associated to the selection are listed in the modal. One or more can then be selected, saved, and then added as invitees as needed.
	This same idea works for Rooms and/or Equipment as well. Simply use the "equipment" icon to see a list of resources available for reservation for your meeting or event. Resources can be selected and added to the invitation as needed.

Options

　　• Source - Use the dropdown menu to select which calendar the event is for. The default calendar can be chosen in Calendar Settings .

　　• Availability - Here you can set your own availability - either Busy or Free. Setting your status as Busy will be reflected if others within your Global Address List try inviting you to their own events.

　　• Reminder - Setting a reminder will make a notification window appear in webmail at whatever reminder interval you set. Reminders are also synced to any email or calendar app you have synced to your SmarterMail account.

　　• Email Notification - Enabling this will send an event reminder to the organizer's email address based on the time interval set by the reminder. This email is in addition to the notification in webmail or any synced client.

　　• Private event - This setting can be used for those who share their calendar with other users. Events marked as private will only be shown to those with Full Access. Those with Availability-Only or Read-Only permission will instead see "Busy Time" and cannot view appointment details.

Attachments and Categories

It's possible to add attachments to any new appointment you create. Attachments can include, but are not limited to, PDF files, presentations, spreadsheets, or any other type of attachment that the attendees of the appointment may require. To add one or more attachments, simply click the paperclip button at the top of the new appointment window. This allows you to browse your device for any file(s) needed.

A category provides a way to organize your Events into manageable groups. To add a category, simply use the Mark button. When clicked, a dropdown appears that lists all of the categories that are available for the account. For more information, see Categories .

Using AI Assistance
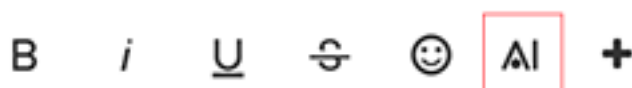
Using the AI Tools icon you can use the AI provider that's configured for your user to generate text for an appointment. This is especially useful for crafting the description and/or details of the appointment. For example, you can use the following Input Text to create a description of your meeting: "Generate a description of this meeting pertaining to marketing strategy for Q2 of this year". Clicking on the Generate button will offer something like this: The meeting will focus on developing a comprehensive marketing strategy for Q2, emphasizing key initiatives to enhance brand visibility and drive customer engagement. Participants will review performance metrics from Q1, identify target audiences, and discuss innovative campaign ideas across various channels, including digital, social media, and traditional marketing. Additionally, the agenda includes budget allocation, collaboration opportunities among teams, and setting measurable goals to assess the effectiveness of the implemented strategies. Action items will be assigned to ensure timely execution and follow-up.

You can then insert that text as the meeting description, or edit it as you see fit. From there, you can select that text and use preset commands to lengthen or shorten it, translate it to another language, or more.

Receiving Calendar Invitations

When someone sends you a calendar invitation, it appears in your inbox just like any other email message. The invitation will contain the details of the appointment such as the day and time, a subject, maybe some additional details, a reminder option, etc. and you will need to act on the message. The actions available to you are displayed as buttons at the top of the invitation, and the action you select will determine how that invitation is handled by SmarterMail. The following actions are available within webmail, and most, if not all, are also available in an email or calendar app you use may use on your desktop or mobile device:

> • Accept - This will add the event to your calendar and let the "event organizer" — the person who sent you the invitation — know that you have accepted the invitation and the event was added to your calendar.
> • Tentative - This will add the event to your calendar but displays it with a dashed outline to shows its tentative status. Tentative acceptances are generally made when you're unsure whether you'll be able to attend the event or not.
> • Decline - This does NOT add the event to your calendar and it will let the event organizer know you have declined the invitation.
> • Details - This displays the details of the event in a modal window that aligns with SmarterMail's New Appointment modal.

Propose Changes

Proposing changes to an invitation can be used when you may have a conflict come up, but you're unsure whether the conflict will occur or not. This allows you to propose a new date and/or time for the event, and sends the proposed changes to the event organizer. Another example is when a particular item is required for the event, such as a delivery from a third-party, but that delivery was delayed. Proposing a new time allows you to align the delivery with the proposed event. note: Propose New Time will be displayed as a link beneath the start and end time fields.

When proposing a change to an invitation, you have the ability to suggest a change to the date of the appointment, the time, or both. If you're unsure, you can use the left and right buttons on the modal to check your availability on a specific day, and make your suggestion based on that. You can also select a "Reply Action", which gives you the ability to reply with "Accept", "Decline",or "Tentative". Proposing a new time, and replying with a specified action, works just like the actions available to you on the original invitation.

A nice feature of Propose New Time is, when interacting with others on your domain, you can see your availability and anyone else's availability to you can propose a new day or time what works with most, if not all, other attendees.

Responding to Invitations

Regardless of the action chosen when responding to an invitation, once the reply is sent the original invitation is moved to your Deleted Items folder.

Adding a Reply

On occasion, you may have the ability to add a reply to your invitation response. This will generally appear as a text box at the bottom of the invitation. Here, you can type in things like a reason for declining an invite, information on why you're proposing changes, etc. On the sender's end, this reply will appear in plain text (usually) in the confirmation they get once your action is taken.

Editing a Calendar Source

SmarterMail's powerful calendaring feature gives users the ability to use a single calendar for their own events and appointments, PLUS the ability to share their calendars with others or even map the calendars of others so that those events and appointments can be seen in one, singular interface. Having access to all of those calendars, and all of those appointments and events, can be somewhat tedious, unless you have a way of keeping them separated in your calendar view. That's where the ability to edit a calendar source comes in handy.

Each calendar you have access to is customizable. That means you can modify the color scheme for appointments in that calendar, modify the name of the calendar and more. To edit a calendar source, simply right-click on the calendar name to open its context menu, then select Edit Folder . When you do, the Calendar modal will open.

There are a few options available for editing the calendar source:

- Display Name - This is how you want the calendar to display in the Calendar Source view. A calendar that you've mapped will generally have a default name, like "Calendar on JSmith" or something similar. However, you can modify the name to whatever you like.
- Color - Set to the side of the Display Name, this is the background color used for appointments and events created on that calendar. It's a good idea to have different colors set for each individual calendar you have so that you can easily distinguish between the events and the calendars those events belong to. You can select the color by clicking on the color swatch next to the Display Name, or by clicking on the color swatch.

Editing Folders Shared With You

It is possible to change the color of calendar folders that are shared with you. However, that's all that you are able to change. To do this, right-click the shared folder and select Properties from the context menu.

There are a few options that appear in the editing modal that are displayed, but not editable. These include a Shared by , which is the display name or username for your particular user or the username of the person sharing their calendar with you, and the Access that's been granted to you for that calendar. For more information on the different types of access available, head over to the Sharing and Collaboration section of Help.

Sharing a Calendar

SmarterTools provides users with the ability to share primary and/or secondary calendar folders that they create. Sharing a calendar with another SmarterMail user, a User Group, or even those outside of SmarterMail is easy to do. To share a calendar, do the following:

- Log in to your SmarterMail mailbox and go to your calendars.
- Select the calendar you want to share, then click the Folder icon and select Share Folder from the dropdown. Alternatively, you can right-click the folder and select Share Folder from the context menu.
- The Sharing tab will be selected, by default.
- To share that calendar with another user of your domain, simply start typing their email address in the Users area. SmarterMail's autocomplete will fill in names based on what is typed.

You can simply select that user from the suggestions or fully type their address. It's also possible to share a calendar with a User Group by selecting the group from the dropdown.

• Next, select the type of access you want to grant to that user:

• None - This is used, primarily, to exclude some member of a group when the group is granted another permission level.

• Availability - This allows the person or group to view whether you're busy at a specific day/time.

• Read-Only - This allows the person or group to view the full details of events on your calendar, but not interact with them.

• Manage - This allows the person or group to fully manage your calendar, including adding appointments, changing appointments, etc.

• Owner - Delegates ownership of the item to the person or group.

• You can add another user or user group, and when done simply save your changes.

<u>Sharing Calendars Outside Your Domain</u>

Along with sharing a calendar with other users on your domain, it's possible to share a calendar outside of SmarterMail. Customers can subscribe to a calendar and have it appear in their email client, webmail client, and even in services like Google calendar. To do this, you simply need a shareable link:

• Log in to your SmarterMail mailbox and go to your calendars.

• Select the calendar you want to share, then click the Folder icon and select Share Folder from the dropdown. Alternatively, you can right-click the folder and select Share Folder from the context menu.

• Select the Webcal tab.

• Enable Allow others to subscribe to this calendar using Webcal . This will give you a "Webcal Shareable Link".

• Copy that link manually, or use the copy icon to the right of it, and send that to anyone outside of your domain. This will allow them to add your calendar as an internet calendar to their email client, calendar service, etc. NOTE for iCal: In order to share your calendar as an iCal link for services such as Google Calendar, simply change webcals:// to https:// prior to sending out the link. It will then work with any client/service that uses the iCal format.

Subscribing to an Internet/Web Calendar

Many organizations and services make their calendars available for public or private consumption. For example, you can subscribe to your favorite sports team's seasonal schedule, subscribe to a payroll calendar, subscribe to a holiday calendar and more.

To subscribe to a web or internet calendar, do the following:

- Log into SmarterMail and go to your calendars.
- Select Subscribe to Calendar from the Actions (□) dropdown menu.
- A modal window opens with the following options:

- Name - This is the friendly name you want to give this calendar, such as "PTO Schedule" or "Suns Schedule".
- Color - This is the background color used for appointments and events created on that calendar.
- Calendar URL - This is the url provided to you by the calendar's owner. Generally, this URL will be formed using "webcal://" as the prefix.
- Update Interval (minutes) - This is how often you want the calendar to update. By default, this is set to 60 minutes. For most things, the default interval will be perfectly fine.
- Once all the items are filled out, be sure to Save the subscription. The items from this calendar will show up on whichever calendar you've added the subscription to. In addition, when syncing this calendar to an email or calendar app, events on the subscribed calendar will also sync!

Creating New Calendars

SmarterMail allows users to create multiple personal calendars in order to better organize appointments. Along with being able to add as many calendars as needed, users can choose their own custom color for the calendars available, giving them the ability to identify the calendar for the appointment at a glance. Furthermore, users can sync their additional calendars to email and calendar clients and apps using EAS, MAPI/EWS, and CalDAV. All calendars can also be shared with others within the same organization as well.

When multiple personal calendars are created, users can even use a custom folder as the default for any new appointments. To do this, use the Default Folders card in Account Settings.

Follow the steps below to create additional personal calendars:

- Log into SmarterMail and go to your calendars.
- Click the Folders icon, then select New Folder from the dropdown.
- A modal window will appear. Here, you can edit the new calendar's details.
- Enter the Display Name you want to use for the calendar. You can then set the color used for new appointments on the calendar.
- Be sure to Save your changes.
- The new calendar will be displayed below any existing calendar sources in your list. If you need to edit the calendar — for example, change its color — simply right-click on its name and select Edit Folder and its details modal will open again.

Managing Calendar Appointments

To view the details of an appointment, select it from any calendar view. (I.e., Month/Week/Day view, etc.) The appointment details will load in a popup window.

Editing Appointment Details

Select the appointment you want to edit. To change the calendar that the appointment is assigned to, simply change the appointment's Source , which is found on the Options card. Make any other appropriate changes and be sure to Save your edits.

When you edit an appointment, it updates on your calendar and, if the edits are "significant", any attendees will receive a new invitation notifying them of the change. However, in some cases, only certain attendees will be notified. For example, if you add someone to an existing appointment, only the person added will receive an invitation. When removing someone, only that person receives the cancellation. "Significant" changes are basically any change to an event other than things like changing reminders/alarms, changing availability, etc. Note: Editing a recurring appointment will update all instances of the appointment on your calendar. If you need to edit a single instance of a recurring appointment you will need to select that specific appointment and make your edits. Only the organizer can edit appointments.

Deleting an Appointment

On occasion, you may need to delete a calendar appointment. To delete and remove an appointment from your calendar, select the appointment from any calendar view. The appointment details will load in a popup window, and from here the appointment can be deleted. You can also right-click on an appointment and delete it from the context menu.

Once deleted, the appointment will no longer appear on your calendar and any attendees will receive a notification that the appointment has been cancelled. Note: For recurring events, you have the option of deleting all instances from your calendar or just a single instance.

Deleting an Instance

When creating an appointment, it's possible to create it as a recurring event. That means the appointment will occur at a specific interval for a specific amount of time. The most common types of recurring appointments are weekly or monthly meetings. However, there may be a time when a recurring meeting needs to be cancelled due to unforeseen circumstances. That's where deleting an "instance" of a meeting comes in handy.

Deleting an instance of a recurring event allows you to delete a single meeting from a recurring sequence. That meeting can then be formally cancelled or re-scheduled for a later day and time.

Deleting an instance of a meeting will not affect any future or past instances - only the instance you delete.

Duplicating an Instance

The ability to create a recurring appointment is crucial for any user. However, recurring appointments generally follow a set of rules: Every Wednesday, or every third Monday, or the last Friday of each month. What if your recurring appointments are non-standard days? That's where duplicating appointments comes in.

Let's say you have a monthly sales meeting that happens on the last Friday of each month. The Wednesday prior to that meeting, though, you want to make sure you have all of your sales metrics in place and ready to present to the CEO and any other attendees. The problem here is that you can't create a standard recurring appointment as there aren't any dynamic rules available for those. You can't use the "last Wednesday" as your rule as there could be another Wednesday AFTER the last Friday throughout the year. Sure, you could go through each month and manually create an event, but that means re-typing a bunch of info. Thankfully, you can duplicate events and make sure they occur the exact day you want, without having to manually recreate each appointment.

Basically, in order to duplicate an appointment, you first want to open the appointment you want to duplicate. Then, you can make whatever changes to the appointment you want and then select Save as new item from the Actions (☐) dropdown. This creates a NEW appointment based on the one you're duplicating, and only the info you change would be different.

Tentative Appointments

SmarterMail utilizes tentative meeting requests to help prevent meeting requests or event invitations from getting lost or overlooked. When a meeting invitation is sent, a tentative appointment will be automatically added to the calendar. The appointment can then either be accepted or declined from the email request or directly within the calendar interface. In addition, if a meeting or event is tentative, the reminder will still be sent if one was added to the invite!

To manage a tentative meeting request from the calendar, select the appointment to load its details in a popup window. After viewing the appointment details, you can choose to Accept or Decline the meeting. Tentative meeting requests are denoted with a dashed line around the appointment window at the day/time the event is scheduled.

It should be noted that if you delete a meeting invitation BEFORE you either accept or reject it, the tentative meeting will be removed from your calendar.

Forwarding Appointments

Generally, every effort is made by an organizer to make sure they invite anyone necessary when creating an appointment. However, there are times when others need to be included. For example, a small group of friends plan a dinner party, so the organizer sends out an invite. However, one attendee decides they want to bring a date. Rather than having the organizer edit the original appointment, which would update ALL attendees, the one attendee simply forwards their invite to their unexpected date so it can be added to the date's calendar.

This is a pretty basic example, but forwarding invitations saves time without inconveniencing the event organizer or other invitees with multiple updates and meeting changes. When the new invitee accepts the invitation, they're added to the meeting and the organizer receives a notice that their original invitation was forwarded and was, hopefully, accepted, and a new person added to the event.

Attachments

Occasionally, when viewing an appointment's details, an file of some sort is attached. Generally, attachments are added to appointments when the appointment is initially created in an email client such as Microsoft Outlook. However, attachments can be added via the SmarterMail webmail interface as well. Attachments can be downloaded to a local machine, or device, as needed. Attachments for appointments are handled just as attachments are handled in other areas of SmarterMail: the file's name and file extension are displayed and, if possible, a thumbnail of the attachment is displayed. (This most commonly occurs with image files.)

Add to Outlook

Calendars and contact lists can be loaded into Outlook and displayed side-by-side with your existing Outlook calendar and contacts. This allows you to see your current appointments and contacts from SmarterMail right in Outlook.

To use the Add to Outlook connection:

- In SmarterMail, navigate to your Calendar or Contacts.
- Select Add to Outlook from the Actions (☐) dropdown menu.
- A modal appears that provides you with additional instructions. You'll be prompted to select the version of Outlook you're using, which calendar or contact list you wish to sync, and then you have the option of changing the default Description and/or add in a Display Name for the item you're syncing.
- Click OK to initiate the connector.
- A security popup will appear from Outlook, explaining that an external source wants to attach to Outlook. Selecting Yes allows the connector to attach.

• The resource is now available in Outlook. Note: If you change the password on your email account, the connections will be broken and will have to be reestablished.

Limitations of Add to Outlook

While it may work for some, there are significant limitations to using the Add to Outlook plug-in: it will only sync "Owned" folders (i.e., folders where the user has Owner permissions on the folder), user shared folders, and the GAL. Other folders, with non-owner permissions, will not sync as they do when using other protocols.

Contacts

Contacts Overview

SmarterMail features an online contact manager that helps users organize and communicate with the people in their life. Users can view and manage their contacts from any computer with internet access, anywhere in the world, using the webmail interface.

Navigating Your Contacts

When you view your SmarterMail contacts for the first time, chances are they'll be empty: you won't have any contacts to display. This may not be true if you've migrated to SmarterMail from another email platform or service. Regardless, the layout of contacts is the same whether you have migrated or not. To view or hide different contact folders, such as the Global Address List, shared lists, or mapped resources, simply click the eye icon to the right of the resource name.

In general, the Contacts page is divided into two sections:

• The folders view displays all of your contact folders. These are how your contacts are organized. These folders include the default "Contacts" folder, which are contacts you add or migrate over to SmarterMail, and any folders that contain shared contact lists, such as a Global Address List (GAL).
• The content pane. Here you'll see individual cards that represent every contact and Contact Group you have displayed or, when in grid view, a list of your contacts and their details displayed as rows and columns.

Contact Views

There are two ways to view contacts, and these views are managed using the "Card/Grid View" button at the top of the content pane:

• Card View - This displays each contact as its own card, and displays their contact image or monogram, and some details about the contact like their display name, company, job title, etc., if present.

• Grid View - This displays each contact in a text grid and displays contact details as columns, such as First Name, Last Name, Email Address, etc.

Content Pane

In general, the following options are available when viewing your contacts in Card View :

• Select - Allows you to select more than 1 contact at a time. To select multiple contacts, click Select and then click on one or more cards. To exit Select mode, click the Select button again. To de-select a contact, simply click on it again. Alternatively, click the down arrow and you're presented with the following options:

• Select All - Selects all contacts in the list you are viewing.

• Deselect All - Deselects the selected contact(s).

• Enable Select Mode - This allows users to select multiple different contacts, individually, one at a time. Use this method for selecting different contacts that are separated or scattered throughout your list of contacts so they can be exported, deleted, or otherwise handled the same.

• Sort - Sorts contacts by display name, email, or company in ascending or descending order.

• Filter - This gives you the ability to display contacts based on the category(-ies) that are assigned.

• Actions (☐)

• New Contact Group - Contact Groups are a convenient way to organize multiple contacts so that you can simply sent a message to the group rather than having to send the message to each person in the group individually.

• Add to Outlook - Connects SmarterMail to Microsoft Outlook and synchronizes contact information. Note: This feature is only available in SmarterMail Enterprise.

• Send Email - Addresses an email message to the selected contact(s).

• Send vCards - Allows you to send an email with the selected contact(s) electronic business card(s) (vCards) attached.

• Import - Allows you to import contacts from another email system into your contact database. SmarterMail can bulk import contacts in either vCard or CSV format.

• Export all to vCard - Exports all of your contacts in vCard format.

• Export all to CSV - Exports all of your contacts in CSV format.

In general, the following options are available when viewing your contacts in Grid View :

• Delete - Deletes the selected contact(s).

• Filter - This gives you the ability to display contacts based on the category(-ies) that are assigned.

• Actions (☐)

• New Contact Group

• Add to Outlook - Connects SmarterMail to Microsoft Outlook and synchronizes contact information. Note: This feature is only available in SmarterMail Enterprise.

• Send Email - Addresses an email message to the selected contact(s).

• Send vCards - Allows you to send an email with the selected contact(s) electronic business card(s) (vCards) attached.

• Import - Allows you to import contacts from another email system into your contact database. SmarterMail can bulk import contacts in either vCard or CSV format.

• Export all to vCard - Exports all of your contacts in vCard format.

• Export all to CSV - Exports all of your contacts in CSV format.

Attachments

Occasionally, when viewing a contact's details, a file of some sort is attached. Generally, attachments are added to contacts when the contact is initially created in an email client such as Microsoft Outlook. However, attachments can be added via the SmarterMail webmail interface as well using the paperclip button. Attachments can be downloaded to a local machine, or device, as needed. Attachments for contacts are handled just as attachments are handled in other areas of SmarterMail: the file's name and file extension are displayed and, if possible, a thumbnail of the attachment is displayed. (This most commonly occurs with image files.)

Manage Categories

You can also manage your categories from the Filtering menu. Clicking Manage Categories opens a modal window with all current categories listed. It's possible to do things like change a category name, change its associated color, or even add new categories using this modal. Once categories are changed or modified, those changes or modifications are carried over to any area categories are available. (E.g., Calendars.)

Individual Contacts

In addition to working with all of your contacts, each individual contact has some actions that are available. To view these, simply click the Actions (☐) on each card. When you do, these actions are available:

• Send Email - Addresses an email message to the selected contact(s).

• Send vCard - Allows you to send an email with the selected contact(s) electronic business

card(s) (vCard) attached.

• Export to vCard - Exports only the selected contact(s) in vCard format.

• Export to CSV - Exports only the selected contact(s) in CSV format.

You can also click on a contact and open it in its own window. Opening a contact gives you the ability to update or edit the contact's information. You can also delete the contact or Mark it by assigning it one or more Categories.

Contacts as Trusted Senders

By default, SmarterMail "sees" any contacts you add as "Trusted Senders." What that means is that any email you send to, or receive from, a contact bypasses any spam filters that are set up for your domain. While SmarterMail doesn't add your contacts to the "Trusted Senders" list you will find in your Spam Settings , they're handled the same way. However, unlike the email addresses or domains you add to your Trusted Senders list, messages sent to or received from contacts are not counted in any reports that list or detail messages to or from Trusted Senders. Therefore, while a contact is treated like a Trusted Sender, it's not counted as one in reports.

Sharing Contacts

SmarterMail gives users the ability to share multiple things within their account. More information on sharing, and how to share items, can be found on the Sharing Overview page of this help documentation.

Sending vCards

SmarterMail users can send single vCards or multiple, as needed. Below are instructions on sending a single vCard as well as multiple different vCards.

To send a single vCard:

• Go to the Contacts area.

• Find the specific contact in your list, either by scrolling through your contacts or using the Search bar.

• Select the contact, then click Actions (□)

• From the dropdown menu, select Send vCard .

• SmarterMail will open a new message window with the vCard(s) attached.

• Type the recipient's email address in the To field and compose a message. Then click Send .

To send multiple vCards:

• Go to the Contacts area.

• Click the Select button and choose Enable Select Mode. This allows you to select multiple

different contacts by simply clicking on them.

• Once you've selected the desired contacts, click Actions (□)

• From the dropdown menu, select Send vCards .

• SmarterMail will open a new message window with the vCards attached.

• Type the recipient's email address in the To field and compose a message. Then click Send .

When sending a vCard, it can be useful to use the Category selectors to help narrow down your contacts. Using Categories as well as the Select button even allows you to send vCards for all contacts in one or more categories. To view contacts from a specific category, use the Sort icon. From here, choose Category Filters and select the proper category(-ies) you want to use for filtering your contacts.

Creating New Contacts/Contact Groups

There are several ways to add new contacts, or contact groups, to SmarterMail, depending on whether you want to add a contact from an email message, import contacts from another provider or add a contact by manually typing the name and other information directly in SmarterMail.

Interacting With a Sender's Address

SmarterMail includes "touch and go" functionality that highlights all email addresses in the header of the message. Clicking on an address in the message header opens a small context modal with a few ways to interact with that address:

• Send Email - Opens a pop out window so you can send a new message to the address.

• Add Contact - Opens a pop out that allows you to create a new contact based of this email address.

• Invite to Appointment - Opens a pop out that allows you to create a new appointment, with this person automatically added as an attendee.

• Trust Sender - Adds the address to your Trusted Senders list, meaning any future emails from this address will bypass most antispam options enabled for the server. note: SPF and DKIM still run against any address in the Trusted Senders list to prevent phishing.

• Block Sender - Prevents the sender of the selected message(s) from sending any more messages to the account. When you block a sender, a new Internal Blocked Senders Content Filter is created. Any user you block is added to that list, and their email is, by default, deleted.

• Create Content Filter - This options opens the Content Filtering area. Here, you can use information contained within the email message, such as the From Address, Subject, etc. and create a new Content Filter based off that information.

• Add Sender to Content Filter - This option opens a modal window that lists all of your existing Content Filters. You simply select the filter you want this sender added to, and they're immediately added.

For information on adding new contacts by importing contacts from another email service, see Importing and Exporting Contacts .

Contact Details

Regardless of how you add a contact to SmarterMail, you can input as many or as few details about the person as you like. In general, contact details are separated using various cards. These include:

- Personal Info - These are the "personal" details of your contact, including their display name, title (Mr., Mrs., etc.), first name, middle name, last name, their personal website (or "home page"), and birthday. You can also add a photo, avatar or icon for your contact by simply clicking on the grey circle next to the contact's Display Name. (Images have a max file size of 5MB.) This picture is available within the webmail interface and for anyone using CardDAV or the EAS add-on to sync their contacts with email clients and/or mobile devices. Unfortunately, pictures will not sync for customers using Add to Outlook for synchronization. Note: The Display Name is the only required field to save a contact.
- Phone Numbers - You can add one or more phone numbers associated with your contact, like their home phone, mobile number, etc.
- Email Addresses - Just as with phone numbers, you can add one or more email addresses for your contact. If a contact has more than one email address, you can select which address to send to when typing the contact's name in the TO: field for a new message.
- Home Address - The contact's home address.
- Work Info - The contact's place of work, including their work Title (CEO, Marketing Director, etc.), should they have one, their company's website address, etc.
- Work Address - The street address, city, state and zip for the contact's place of business.
- Categories - Categories are a great way to organize your contacts. Using categories, you can organize business, personal or any other type of contact into tidy circles, keeping people separated based on whatever criteria you want. Contacts can be in multiple categories or none: It's up to you. For more information, see Categories . Note: Categories are only a way to organize contacts. They are NOT ways to send emails to a group of individuals.
- Other - Additional pieces of information about the contact such as their nickname, their spouse's name, their assistant's name, etc.

Contact Groups

Users also have the ability to create Contact Groups from within webmail. Contact Groups are a convenient way to organize multiple contacts so that you can simply send a message to the group rather than having to send the message to each person in the group individually. Most email clients support Contact Groups, but there are some notable exceptions: Microsoft Outlook for macOS. Due to a limitation of Outlook for macOS, you can create "Contact Lists" that are stored locally, and not

synced to the server. This is not a SmarterMail issue, but the way Microsoft has decided Outlook for macOS should work.

When creating a Contact Group you're presented with the following options:

- Display Name - The friendly name of the group you're creating.
- Source - The group can be created using contacts from any folders you have in the Contacts area of SmarterMail. Simply select the folder to use from the dropdown. Contacts can be added from multiple folders as needed. (NOTE: GAL contacts cannot be added to a Contact Group.)
- Notes - If you want to add any notes for the group, such as describing the group or adding in a note on how the contacts where chosen for the group, add them here.
- Members - Clicking the New Member button opens a modal. Here, you can begin typing the name of the contact you want to add, and options will be displayed. Simply select the member you want to add, or continue typing a full email address to add the contact. (It IS possible to add members who are not already contacts.)
- Categories - If you want to add a category, or multiple categories, to the Group, simply use the Mark button and select the category(-ies) from the list provided.

In addition, when syncing with email clients such as Microsoft Outlook using protocols like EWS and/or MAPI, contact groups (a.k.a. "Distribution Lists" in products such as eM Client) created within that/those client(s) will sync back to webmail, and any contact groups created within webmail will sync back to your clients. That way, any group can be used from whatever you're using for sending/receiving email, on your desktop or mobile device.

Attachments

Occasionally, when viewing a contact's details, a file of some sort is attached. Generally, attachments are added to contacts when the contact is initially created in an email client such as Microsoft Outlook. However, attachments can be added via the SmarterMail webmail interface as well using the paperclip button. Attachments can be downloaded to a local machine, or device, as needed. Attachments for contacts are handled just as attachments are handled in other areas of SmarterMail: the file's name and file extension are displayed and, if possible, a thumbnail of the attachment is displayed. (This most commonly occurs with image files.)

New Contact Folders

Similar to how you can create folders for storing/organizing emails, it's possible to store Contacts in folders as well. By default, SmarterMail creates a folder called "Contacts" to house any contact you create in webmail. However, if a user wanted more granularity in their contacts, they can create individual folders for specific types. For example, "Business Contacts", "Personal Contacts" or even

folders of contacts based on specific companies or businesses. There is no limit to how folders can be used.

Using Folders is a great way to share groups of contacts with others within your organization. Rather than sharing individual contacts, one or two at a time, they can be organized in a folder, than that folder can be shared.

Creating a New Folder

To create a new folder, click on the folder icon and do the following:

- Select New Folder .
- A modal window appears.
- Add a Name for the folder.
- Be sure to save your changes.

Editing a Folder

If you want to change the settings of a folder, it's very simple: simply click on its name, then click the Folder icon and select Edit Folder . Alternatively, you can right-click the folder name and select Edit Folder from the context menu.

Searching Contacts

If you have a large number of people in your contacts list, finding a specific contact can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find contacts quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of your contact list. It's best if you have all views available, such as Contacts, Global Address List, etc. so that each view is searched. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the contacts list you are viewing for matches and display the results in the navigation pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."

Importing and Exporting Contacts

Because people often have multiple email accounts from different providers, SmarterMail makes it easy for users to securely transfer contacts to and from other online address books.

Importing/Exporting Contacts

To initiate the importing or exporting of contacts, use the Actions (□) button at the top of your list of contacts. From the dropdown, you'll want to focus on the following:

- Import - Allows you to import your contacts from an external email client, a separate email service like Gmail, or from another SmarterMail account.
- Export All to vCard - Exports all of your contacts in the standard vCard format for importing into an email client, separate service or to another SmarterMail account.
- Export All to CSV - Exports all of your contacts in a "comma separated values" format for importing into an email client, separate service or to another SmarterMail account. CSV files can also be opened using virtually any spreadsheet program such as Microsoft Excel.

Importing Contacts to SmarterMail

SmarterMail supports importing contacts from two different types of files: vCards (.vcf) and comma-separated text files (.csv). SmarterMail also supports importing from a .zip file containing any combination of these file formats. Regardless of the file type imported, each contact MUST have a Display Name in order for SmarterMail to accept the importing of the contact. Other information can be added at a later date.

Follow these steps to import contacts:

- Log in to your SmarterMail account and go to your Contacts.
- Select Import from the Actions (□) dropdown.
- The Import Contacts modal will load. Here, you can select which Contacts folder to import your new contacts to, such as the default Contacts folder or any new folders you've created.
- Next, you can either drag-and-drop a CSV or VCF file into the "add files" area, or you can click on the "add files" box to open a desktop window so you can select the file you want to import.
- Once you've added the file(s), click the Import button.
- If any conflicts occur, you will be asked to resolve them by performing one of the actions below:

- Add Contact - This option adds a completely new contact record with the information in the vCard.
- Replace - This option replaces the contact in the box with the new one being uploaded. To examine the properties of the close match contacts, however your mouse over the magnifying glass icon in the list at the bottom of the page.
- Skip - This option skips this contact and omits the uploaded contact information.
- Once all conflicts are resolved, the process is complete.

Exporting Contacts from SmarterMail

Contacts can be exported individually in vCard or CSV format. These files can then be imported into Microsoft Outlook or other email clients that accept these file types, or into another SmarterMail account.

To export a single contact:

  • First, go to your Contacts.
  • Next, find the specific contact in your list, either by scrolling through your contacts or using the Search bar.
  • Once you find it, in the top right corner of the contact's card you'll see Actions (□) . Click on that.
  • From the dropdown menu, select Export to vCard or Export to CSV .
  • A standard Save window will appear that allows you to rename the file, choose where you want the file saved, etc.

To export multiple contacts (assuming you're already logged in to your SmarterTools account):

  • First, go to your Contacts.
  • The Select button allows you to select multiple different contacts by simply clicking on them.
  • Once you've selected the desired contacts, click on Actions (□)
  • From the dropdown menu, select Export to vCard or Export to CSV .
  • Again, a standard Save window will appear that allows you to rename the file, choose where you want the file saved, etc.

To export ALL contacts:

  • First, go to your Contacts.
  • Use the Select button and choose Select All from the dropdown.
  • From the Actions (□) menu, select Export All to vCard or Export All to CSV .
  • Again, a standard Save window will appear that allows you to rename the file, choose where you want the file saved, etc.

Global Address List

The Global Address List, sometimes referred to as the "GAL," is most commonly identified with Microsoft Exchange. The GAL is essentially a directory service within SmarterMail that contains a dynamic list of all contact information for every user on your domain. While individual mailboxes are contained within the GAL, domain administrators can further manage what's included in the GAL in order to hide users that may not represent real people, such as any aliases and/or mailing lists.

Contact information for the Global Address List is pulled from the individual profiles of users. To update what appears in your own GAL entry, go to your settings area and click on Profile . Here you can edit your information. Note: If the Global Address List is enabled for your domain, all information you enter into your profile can be seen by all other members of your domain.

Other than the availability of the information within the Global Address List, it functions almost identically as Contacts. The difference is that anything in My Contacts is seen only by you.

Adding/Removing a User From the GAL

Domain administrators can actively manage the GAL by adding or removing users as needed. As mentioned, it may be worthwhile for a domain administrator to limit GAL entries to actual employees or users on the domain, excluding things like aliases or generic mailboxes that are used for departments, such as Billing or HR departments.

To change a user's GAL setting, you'll first want to be logged in as a domain administrator. From there, do the following:

- Go to the Domain Settings .
- Select Accounts from the navigation menu and ensure that the Users tab is highlighted.
- Click on the user to edit their settings.
- On the User card, enable or disable the Show in Global Address List setting as needed.
- Be sure to save the changes.

Global Address List Availability

The GAL is a feature available for any domain that's added to SmarterMail. While turned on by default when a domain is created, if domain administrators are not able to find the setting for any new or existing users — that is, add or remove the user from the GAL — they'll want to contact their system administrator to ensure that the Global Address List is actually enabled for their domain.

Tasks

Tasks Overview

SmarterMail's robust task system is designed to help users keep track of the things they need to do. From shopping lists to long-term tasks, users can create lists of items, set due dates, update status and completion percentage, and even prioritize tasks. And, as there are times when an email exchange leads to a task needing to be done, email messages can be the starting point for, or linked to, tasks so that all communication surrounding the task is kept organized.

By default, the Tasks source is displayed. If other task sources are being shared with you, they will appear beneath My Tasks once they've been mapped. (see Mapped Resources for more information on sharing resources.) Making multiple task sources visible will display all of the tasks, from each source, together in the All Tasks view.

Navigating Your Tasks

When you view your SmarterMail tasks for the first time, chances are they'll be empty: you won't have any tasks to display. This may not be true if you've migrated to SmarterMail from another email platform or service. Regardless, the layout of SmarterMail tasks is the same whether you have migrated existing tasks or not. To view or hide different task folders, such as shared tasks, or mapped resources, simply click the eye icon to the right of the resource name.

In general, the Tasks page is divided into two sections:

  • The folders view displays all of your task folders. These are how your tasks are organized. These folders include the default "Tasks" folder, which are tasks you add or migrate over to SmarterMail, and any folders that contain shared tasks, if there are any.
  • The content pane. Here you'll see individual cards that represent every contact and Contact Group you have displayed or, when in grid view, a list of your contacts and their details displayed as rows and columns.

Task Views

There are two ways to view tasks, and these views are managed using the "Card/Grid View" button at the top of the content pane:

  • Card View - This displays each task as its own card, and displays details about the task like its name/title, start and due dates, priority, status, etc.
  • Grid View - This displays each task in a text grid and displays details as columns, such as Subject, Start and Due dates, Priority, Percent Complete, etc.

Viewing Tasks

When you view your tasks in Card View , each task you have created or that's being shared with you will be listed on a separate card. Each card lists the following information, which is described in detail further down this page:

  • Select - Clicking select gives you the following options:

  • Select All - Selects all tasks in the list you are viewing.
  • Deselect All - Deselects the selected task(s).
  • Enable Select Mode - This allows users to select multiple different tasks, individually, one at a

time. Use this method for selecting different tasks that are separated or scattered throughout your list so they can be deleted, or otherwise handled the same.

• Sort - Sorts contacts by Subject, Due Date, % Complete, or Priority in ascending or descending order.

• Filter - This gives you the ability to display contacts based on Status and/or on assigned category(-ies).

• Actions (□)

• Add to Outlook - Connects SmarterMail to Microsoft Outlook and synchronizes tasks. Note: This feature is only available in SmarterMail Enterprise.

• Import ICS File - Exports the selected item as an iCalendar file, a plain text file that can include details such as a description, betting and end times, location, etc.

• Export All to ICS File

• Delete - Deletes the selected task(s).

In general, the following options are available when viewing your tasks in Grid View :

• Delete - Deletes the selected task(s).

• Filter - This gives you the ability to display contacts based on Status and/or on assigned category(-ies).

• Actions (□)

• Add to Outlook - Connects SmarterMail to Microsoft Outlook and synchronizes tasks. Note: This feature is only available in SmarterMail Enterprise.

• Import ICS File - Exports the selected item as an iCalendar file, a plain text file that can include details such as a description, betting and end times, location, etc.

• Export All to ICS File

<u>Viewing Individual Tasks</u>

It's also possible to view tasks individually. Simply clicking on a task, either in Card or Grid View, will open the task in its own window. When you do this, a few buttons appear at the top of the new window. These include:

• Save - Saves any changes made to the task.

• Cancel - Closes the window without saving any changes.

• Delete - Deletes the task.

• Attachment - Allows you to attach files to the task. NOTE: If Tasks are synced to a mobile or desktop client, these attachments may sync as well, depending on the protocol used.

• Mark - Allows the task to be assigned one or more Categories. (This button also allows users to manage the categories listed.)

Opening a task gives you the ability to update or edit its information. The information about a task is listed om various cards, which break down as follows:

- Subject/Description:
- Task Subject - This is the descriptive title of the task, such as "Fill out mortgage paperwork" or "Review New Website Content"
- Description - These are the details of the task. Using the HTML editor, a task's details can include bold text, lists, different fonts or fonts with different colors, pictures, links to websites or videos and more. You can be as creative as you like
- Details:
- Source - This tells you where the task came from> E.g., Tasks or a shared task list.
- Start and due times - The date and time the task is set to begin, and when it's due.
- Reminder - If you want a reminder when a task is coming due, use this toggle and set its date and time.
- Private Task - If you want this task to NOT display on your calendar, especially if that calendar is shared with others, toggle this setting.
- Priority - This allows you to set a level of importance for each task. A priority makes it much easier to sort tasks based on how important it is to complete those tasks.
- Status - Generally, these are:

- Canceled - The task was created, but it was eventually decided it wasn't necessary.
- Not Started - The task was created — perhaps more information is needed or it's dependent on a task from another user — so it hasn't been started yet.
- Completed - The task is finished.
- In Progress - The task is currently being worked on.
- % Complete - This allows you to periodically update where you are in terms of completing the task. This is especially helpful if the task is being shared with others within your organization. As an aside, once a task hits 100%, it's "Status" will automatically change to "Completed". Conversely, if a task was set to 100% and, therefore, Completed, if the Completion Percentage changes to less than 100%, the Status of the task automatically changes to "In Progress".
- Attachments:
- When available, if any attachments were added to a task, they'll be listed here. Each attachment can then be downloaded and viewed/used as needed.

Sharing Tasks

SmarterMail gives users the ability to share multiple things within their account. More information on sharing, and how to share items, can be found on the Sharing Overview page of this help documentation.

Tasks and Calendars

As tasks generally have a timeframe associated with them, you can choose to have your tasks displayed in your calendar, just as you do other events. You can opt to have the start time and/or the end times displayed. You can also hide Tasks from your calendar that have been marked as "Completed". To manage all this, go to your User Settings and open up Calendar Settings . On the Options card, you can enable or disable "Display task start times in the calendar view", "Display task due times in the calendar view" and "Hide completed tasks". As with any other calendar event, task start times and end times both trigger any notification you have set for the task.

Creating a Task

Creating a new task is extremely easy and simply involves adding in any relevant details for the task. These can include:

Subject - This is the simple name for the task, like "Create new blog post" or "Organize meeting notes".

Task Description - This is where you enter more details about the task. For example, a copy of any meeting notes or general notes necessary for the completion of the task. These can be updated at any time. Editing the description and keeping additional notes there is especially beneficial when participating in shared tasks. In addition, the task description area is fully HTML compliant with a rich editor so it's possible to stylize the description with different fonts and colors, links to outside resources, etc.

Then there are the Task Details , which include:

> • Source - Where the task is kept. By default, new tasks are stored within Tasks, but if you have shared tasks with others, you can save a task there as well so the person you're sharing with can keep track of the task's status.
> • Start - The date and time the task is supposed to start. Both areas have quick-select icons for setting the date as well as the time, but you can manually enter this information as well.
> • Due - The date and time the task is due. Again, both areas have quick-select icons for setting the date as well as the time, but you can manually enter this information as well.
> • Reminder - If you want to be reminded prior to the Start Date/Time
> • Private Task - Toggle this to keep details of the task private, especially when adding tasks to your calendar.
> • Priority - Priorities help you keep abreast of important tasks and organize your time. Important tasks, obviously, would take a higher priority whereas daily or monthly tasks may carry less weight. 0 priority would have less importance whereas 10 tasks would have the highest priority.
> • Status - The status of a task reminds you, and others if sharing tasks, where the task is in terms

of its progress towards the due date.

  • % Complete - Adding a % Complete further lets you, and others if sharing tasks, see how far along the task is in terms of meeting the due date.

Finally, there are Categories . Just like within Contacts and other areas of SmarterTools, it's possible to Mark a task with one or more categories. Adding categories is a great way to keep tasks organized. For more information, see Categories . It's also possible to add one or more attachments to the task using the paperclip button.

Using AI Assistance

Using the AI Tools icon you can use the AI provider that's configured for your user to generate text for a task. This is especially useful if you're unsure where to start with a task. Using AI can create a foundation that you can then build upon.

For example, you can use the following Input Text to create a basic outline of a task: "Generate a description of this meeting pertaining to marketing strategy for Q2 of this year". Clicking on the Generate button will offer something like this: Task: Set Up a Banner Campaign

  • Define Objectives:

  • Determine campaign goals (e.g., brand awareness, lead generation, sales).
  • Identify Target Audience:

  • Create audience profiles based on demographics, interests, and behaviors.
  • Set Budget:

  • Establish total budget for the campaign and allocate funds for each platform.
  • Choose Ad Platforms:

  • Select appropriate ad networks and platforms (e.g., Google Display Network, social media).
  • Design Banner Ads:

  • Create visually appealing ad designs with clear messaging and a call to action.
  • Ensure ads are compliant with platform specifications (size, format).
  • Create Landing Pages:

  • Develop dedicated landing pages for each ad to maximize conversions.
  • Implement Tracking:

  • Set up tracking pixels and analytics to monitor performance (e.g., Google Analytics).
  • Launch Campaign:

- Schedule the ads for launch, ensuring all elements are properly configured.
- Monitor Performance:

- Regularly review key metrics (impressions, clicks, conversions) to assess effectiveness.
- Optimize Campaign:

- Make adjustments based on performance data (e.g., tweaking ad copy, targeting).
- Report Results:

- Compile a report summarizing campaign performance and insights for future reference.

You can then insert that text as the task description, then add to it as needed. You can even select that text and use preset commands to lengthen or shorten it, translate it to another language, or more.

Editing a Task

To edit a task, simply click on the card of the task you want to modify. Once opened, you'll be able to edit any area of the task. Editing tasks is important, especially when tasks are shared with others, to add new notes, adjust due dates and % complete and more.

Tasks and Calendars

Depending on whether you have your calendar set up to display the start and/or end times for tasks, once the task is saved, it will appear on your calendar. Note: For more information, see Calendar Settings .

New Task Folders

Similar to how you can create folders for storing/organizing emails, it's possible to store Tasks in folders as well. By default, SmarterMail creates a folder called "Tasks" to house any task you create in webmail. However, if a user wanted more granularity in their tasks, they can create individual folders for specific types. For example, "Marketing Tasks", "QC Tasks" or even folders for tasks based on specific companies or businesses. There is no limit to how folders can be used.

Using Folders is a great way to share groups of tasks with others within your organization. Rather than sharing individual tasks, one or two at a time, they can be organized in a folder, then that folder can be shared.

Creating a New Folder

To create a new folder, click on the menu icon in the lower, left corner of the interface and do the following:

- Click the Folder icon and select New Folder .
- A modal window appears.

• Add a Name for the folder.

• Be sure to Save your changes.

<u>Editing a Folder</u>

If you want to change the settings of a folder, it's very simple: simply click on its name the click the Folder icon, or right-click the folder name and select Edit Folder from the context menu. The settings modal opens and you can change the Name and the color associated to the folder.

Searching Tasks

If you have a large number of tasks in your tasks list, finding a specific task can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find tasks quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the All Tasks view. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the tasks list you are viewing for matches and display the results in the navigation pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."

Notes

Notes Overview

SmarterMail's Notes feature provides users with the electronic equivalent of paper sticky notes. Use notes to jot down questions, ideas, reminders or anything else you would write on note paper. This feature is especially convenient when used to save bits of information you may need later, such as directions or text you want to reuse in other items or documents.

By default, the default Notes source is displayed when you access the Notes area. If other note sources are being shared with you, they will appear beneath My Notes once they've been mapped. (see Mapped Resources for more information on sharing resources.) Making multiple notes sources visible will display all of the notes, from each source, together in the notes view. You can then view or hide notes sources to either limit or expand the number of notes you're viewing.

Navigating Your Notes

When you view your notes for the first time, chances are you won't have any to display. This may not be true if you've migrated to SmarterMail from another email platform or service. Regardless, the layout of notes is the same whether you have migrated or not. To view or hide different notes folders lists, such as the default folder, shared folders, or mapped resources, simply click the eye icon to the right of the folder name.

In general, the Notes page is divided into two sections:

• The folders view displays all of your note folders. These are how your notes are organized. These folders include the default "Notes" folder, which are notes you add or migrate over to SmarterMail, and any folders that contain shared notes.
• The content pane. Here you'll see individual cards that represent every note you have displayed or, when in grid view, a list of your notes and their details displayed as rows and columns.

Notes Views

There are two ways to view notes, and these views are managed using the "Card/Grid View" button at the top of the content pane:

• Card View - This displays each note as its own card, and displays some details about the notes like their subject, details, and source.
• Grid View - This displays each note in a text grid and displays details as columns, such as Subject, Date Modified, Color, etc.

Viewing Notes

When you view your notes in Card View , each note you have created or that's being shared with you will be listed on a separate card. Each card lists the following information:

• Subject - The note's descriptive title. E.g., "Shopping List" or "Motivational Sayings"
• Color Indicator - If the Note was assigned a color, the line under the Subject will reflect the color assigned.
• Date / Time - The day, date, and time the Note was last edited.
• Description - The contents of the note. Using the HTML editor, a note's contents can include bold text, lists, different fonts or fonts with different colors, include pictures, links to websites or videos and more. You can be as creative as you like.
• Source - This tells you where the note came from, or, in cases where notes are shared with others, where you want the note saved. E.g., Notes or "Marketing Notes".
• Categories - If one or more Categories were assigned to a Note, the corresponding tag(s) display(s) on the same line as the Source.
• Attachments - If one or more Attachments were added to a Note, a paperclip displays on the same line as the Source.

In addition, when using Card View, several options are available for interacting with notes:

• Select - Clicking the down arrow presents you with the following options:

• Select All - Selects all notes in Grid View.

• Deselect All - Deselects the selected note(s).

• Enable Select Mode - This allows users to select multiple different notes, individually, one at a time. Use this method for selecting different notes that are separated or scattered throughout your list so they can be exported, deleted, or otherwise handled the same.

• Sort - Sorts notes by Date Modified, Color, or Subject in ascending or descending order.

• Filter - This gives you the ability to display notes based on whether they have attachments, or the category(-ies) that are assigned.

• Actions (□)

• Import - Allows you to import notes from another email system into SmarterMail.

• Export all to CSV - Exports all of your notes in CSV format.

• Delete - Deletes the selected note(s).

When viewing notes in Grid View , the following information is listed:

• Subject - The note's descriptive title. E.g., "Shopping List" or "Motivational Sayings"

• Date Modified - The date and time the note was initially created, or last edited.

• Color - The color assigned to the note.

• Categories - The color label for the category (-ies) assigned to the Note.

• Attachments - A checkmark indicates there's an attachment for the Note.

• Source - The folder the note resides in, such as the default "Notes" folder.

In addition, when using Grid View, several options are available for interacting with notes:

• Delete - Deletes the selected note(s).

• Filter - This gives you the ability to display notes based on the category(-ies) that are assigned.

• Actions (□)

• Import - Allows you to import notes from another email system into SmarterMail.

• Export all to CSV - Exports all of your notes in CSV format.

Sharing Notes

SmarterMail gives users the ability to share multiple things within their account. More information on sharing, and how to share items, can be found on the Sharing Overview page of this help documentation.

Creating New Notes

Starting a new note is extremely easy: simply click the New button. Once you do this, you'll be able to start entering your note details. These include:

- Subject - This is the simple name for the note, like "Shopping List" or "Meeting Notes".
- Description - This is where you enter the actual note contents. The note description area is fully HTML compliant with a rich editor so it's possible to stylize your note contents with different fonts and colors, links to outside resources, embedded videos, etc. note: Inline images over 200KB will cause the window to become unresponsive when using Code View. This is a known issue with the Froala editor.
- Source - Either the default Notes folder, any new or custom folders you've created, or, if other users have shared their Notes with you, you can select one of those as the Source for your new Note.
- Color - Note colors are a great way to keep notes of a specific type neatly organized. As a side note, the colors available match the colors of traditional paper sticky notes.

You can also add a Category to the new note using the Mark button, or add one or more attachments using the paperclip button.

Microsoft Outlook Limitations

When creating a new note using the SmarterMail webmail client, it's possible to use the HTML editor to add images to your note. You can also add attachements to note. (E.g., adding a PDF to it as reference.) However, when synching your notes to Microsoft Outlook, neither the embedded image or the attachment show up. This is because Outlook does not support inline images or attachments. This is not a limitation of SmarterMail.

Using AI Assistance

Using the AI Tools icon you can use the AI provider that's configured for your user to generate text for a note, or even edit existing text.

For example, you may have notes taken during a meeting or discussion that are then transcribed into a note in SmarterMail. You can paste that text into the editor, select the text (or a portion of it), and then use the a preset Command to proofread the text for you. You could shorten it, lengthen it, change the tone, or even translate it to a new language.

New Note Folders

Similar to how you can create folders for storing/organizing emails, it's possible to store Notes in folders as well. By default, SmarterMail creates a folder called "Notes" to house any note you create in

webmail. However, if a user wanted more granularity in their notes, they can create individual folders for specific types. For example, "Marketing Notes", "QC Notes" or even folders for notes based on specific companies or businesses. There is no limit to how folders can be used.

Using Folders is a great way to share groups of notes with others within your organization as well. Rather than sharing individual notes, one or two at a time, they can be organized in a folder, then that folder can be shared.

Creating a New Folder

To create a new folder, click on the Folder icon and do the following:

- Select New Folder .
- A modal window appears.
- Add a Display Name for the folder.
- Be sure to save your changes.

Editing a Folder

If you want to change the settings of a folder, it's very simple: simply right-click on its name and select Edit Folder from the context menu. The settings modal opens and you can change the Display Name.

Sharing a Folder

To share a folder, or to manage the sharing permissions on a folder, simply right-click on its name and select Share Folder from the context menu. Here you can elect to share the folder with one or more users or User Groups, and manage the permissions for each.

Searching Notes

If you have a large number of notes in your notes list, finding a specific one can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find notes quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the All Notes view. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search both the Subject and Description of every note for matches and display the results. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@@," "#" or "%."

Importing and Exporting Notes

SmarterMail allows users to create multiple different folders for various types of Notes. Users can create a folder for personal notes, for business notes, for notes about a particular topic and more. That

said, there may be times when users want to import notes to a folder, or even export notes to be used in other applications, etc.

Importing/Exporting Notes

To initiate the importing or exporting of notes, click the Actions (□) after clicking on a Notes folder. From the dropdown, you'll see the following:

- Import - Allows you to import notes from an external file.
- Export to CSV - Exports all of your notes in a "comma separated values" format for importing into another application or even another SmarterMail account. Note: SmarterMail exports Notes in their original HTML formatting. Therefore, opening or otherwise editing the exported file in another application may prevent you from being able to use that CSV in another application. Therefore, it's recommended that you NOT open exported notes in Excel or even a text editor — they should simply be exported then imported into another application.

Importing Notes to SmarterMail

SmarterMail supports importing notes from a comma-separated text files (.csv). Follow these steps to import notes:

- First, go to your Notes.
- Select a specific folder for the imported Notes. If need be, create a new folder for the imported notes.
- Select Import from the Actions (□) dropdown menu.
- The Import Notes modal will load. Here, you can select which Notes folder to import your new notes to, such as the default Notes folder or any new folders you've created.
- Next, you can either drag-and-drop a CSV file into the "add files" area, or you can click on the "add files" box to open a desktop window so you can select the file you want to import.
- Once you've added the file(s), click the Import button.
- The file will process, then you're presented with a Field mapping modal. Here, you'll map the Uploaded Field — the fields found in the CSV — to a corresponding Notes field. Whenever possible, SmarterMail will automatically map fields it recognizes, especially when importing SmarterMail Notes.
- Once all fields are mapped, the process is complete.

Exporting Notes from SmarterMail

Just as you can import notes from a CSV file, you can also export your own notes as a CSV file. These files can then be imported into other applications that accept these file types, or into another SmarterMail account. To export notes to a CSV file:

• First, go to your Notes.

• Select Export to CSV from the Actions (□) dropdown menu.

• A standard Save window will appear that allows you to rename the file, choose where you want the file saved, etc.

• Click the Save button and you're done.

As mentioned, SmarterMail exports Notes with all of their original HTML formatting. Therefore, opening or otherwise editing the exported file in another application may prevent you from being able to use that CSV in another application. Therefore, it's recommended that you NOT open exported notes in Excel or even a text editor — they should simply be exported then imported into another application.

News Feeds

News Feeds Overview

Real Simple Syndication (RSS) is a way for website owners to make their content available for people to read at their leisure using a centralized application, or Feed Reader. Websites publish lists of updated content via "feeds" that indicate when a new article, blog post or community thread is available. So, rather than regularly visiting a website, you can add a new feed to SmarterMail (also called subscribing to a feed) and then see when new content is available from that site. Any new content posted to your feeds will appear in the News Feeds section of your SmarterMail account, so you don't have to do a ton of clicking around or have multiple browser tabs open.

Using RSS makes it easy to stay up-to-date on information from news sites, blogs, social media outlets, Google alerts, new forum topics and much more, right from within SmarterMail.

Email   Calendar   Contacts   Tasks   News Feeds ▾   ✉ New ▾

| All Feeds | 246 |

1NYT Sports	69
Boing Boing	30
Daring Fireball	48
Engadget	25
SmarterTools Blog	74
Wired Health News	

Next Page

Musk's Twitter promised a purge of blue check marks. Instead he singled out one account

4/3/23 11:22 AM

Some VIP Twitter users woke up on Saturday expecting to have lost their coveted blue verification chec by Elon Musk. Instead, Twitter appeared to target a single account from a major publication Musk dislil a way that obscures why users are verified.

Source: 1NYT Sports

Study finds slightly higher risk of autism in areas with more lithium in drinking water

4/3/23 11:22 AM

A new study found a moderately higher risk of autism spectrum disorder in children born to pregnant p levels of lithium, but experts caution that this association does not show a direct link between the two.

Source: 1NYT Sports

Yale's Assure Lock 2 is down to its lowest price ever

4/3/23 11:20 AM

The Yale Assure Lock 2 can automatically open your door, takes voice commands and let guests in witl configuration of the smart lock is down to its lowest price since its debut, with a 17 percent discount th applies to the black finish only — the nickel finish is seeing a nine percent, or $15, discount and the bro model includes both WiFi and Bluetooth connectivity and has a touchscreen keypad for access for visit Best Buy is offering the same discount, so if you prefer shopping there, you can still save. We were imp high score of 87 in our review. In most cases, it only requires a Phillips head screwdriver to install and i

Source: Engadget

Navigating Your News Feeds

News Feed Layout

When you view your news feeds, the page is divided into two sections:

> • The News Feeds View displays all of the feeds you have added to SmarterMail. Any recent or unread updates to a specific feed are shown with a number to the end of the feed's name. To view the feeds, simply click the desired feed's name.

> • The content view displays a list of the articles, with a brief synopsis, in the RSS feed you are viewing. Simply click on the article to open it up in a new browser tab at the original source.

Adding a New News Feed

Adding a new feed is simple. However, you'll need to grab the proper feed URL from the site you want to add. Generally, a website will have an RSS feed listed somewhere on their website. Additionally, you can do a search for "Website A's RSS feed" in your favorite search engine and that site's feed URL should be one of the results. If you're unsure where to start, you can do a search for "best RSS feeds for news" or "best RSS feeds for tech reviews" and the results will be many.

Generally, an RSS feed URL looks something like "https://www.wired.com/category/gear/feed" or even "http://feeds.reuters.com/reuters/healthNews". On most sites, they're designated with an RSS feed icon.

If you were to click on an RSS link in your browser, you'll see the raw feed page, which is probably a XML page. Therefore, it will look like a bunch of oddly grouped blocks of text surrounded by XML tags. Fear not: the News Feed reader in SmarterMail can make perfect sense of what you're seeing.

Once you have a feed URL, it's time to add the feed to your News Reader. To do this, select Add Feed from the New Folder menu and a modal will open. Add the feed's name, then the feed URL, and select a folder, then save your change. Once you do, that feed name will show up in your feeds view and, once all of the new feeds are grabbed by SmarterMail, a number will appear next to the feed's name, telling you how many new items were retrieved. Continue doing this for any new feed you want to add.

You can also edit an existing feed — for example, you want to rename it or change the feed URL — and delete feeds using the same tree-bar (hamburger) button. You can also Refresh the feeds list to manually have SmarterMail retrieve your feeds for any new items.

Reports

Reports Overview

Using SmarterMail's extensive reporting engine and routinely generating and evaluating reports provides users, domain administrators and system administrators with the information they need to uncover issues before they become problems, discover and evaluate trends, identify the need for policy adjustment and much more.

Users

Users have access to a variety of reports that are directly related to their use of SmarterMail. These include disk usage reports that break out the disk space used by both email (by folder) as well as file storage (which includes the space used by files shared through group chat and online meetings) in addition to a variety of traffic reports, such as incoming and outgoing messages and more.

There is also a dashboard available to users that gives a quick overview of their overall mailbox which includes their incoming and outgoing messages, a breakdown of overall disk usage, and spam counts and viruses caught.
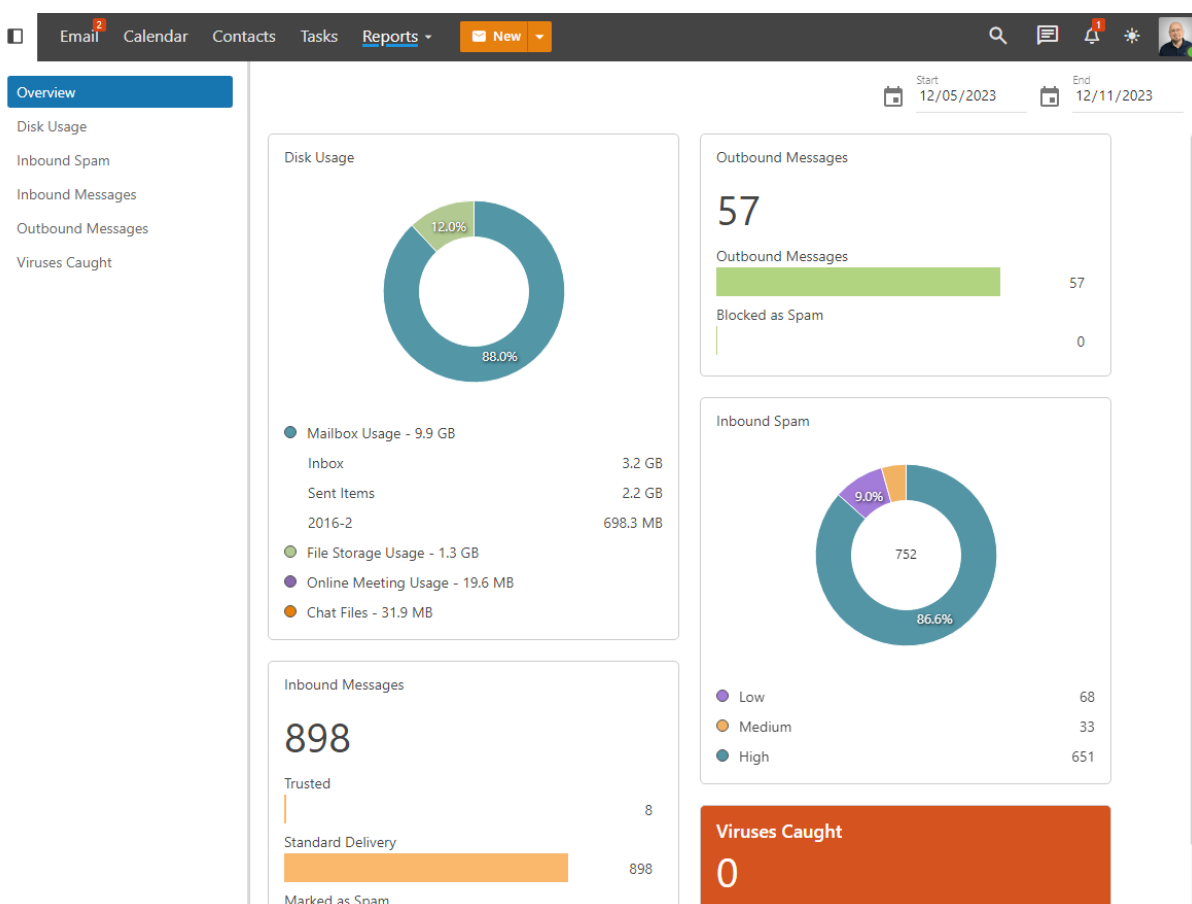
Domain Administrators

Domain administrators have access to all standard user reports in addition to reports that deal directly with the domain they are managing. For example, they can access trend reports relating to domain traffic as well as spam and virus reports. In addition, domain administrators can change a report's "Mode" to drill to into user statistics.

There is also a dashboard available to domain administrators that gives a quick overview of the domain usage as a whole. This includes the total incoming and outgoing messages, message bandwidth, a breakdown of overall disk usage, spam counts and viruses caught, and much more.
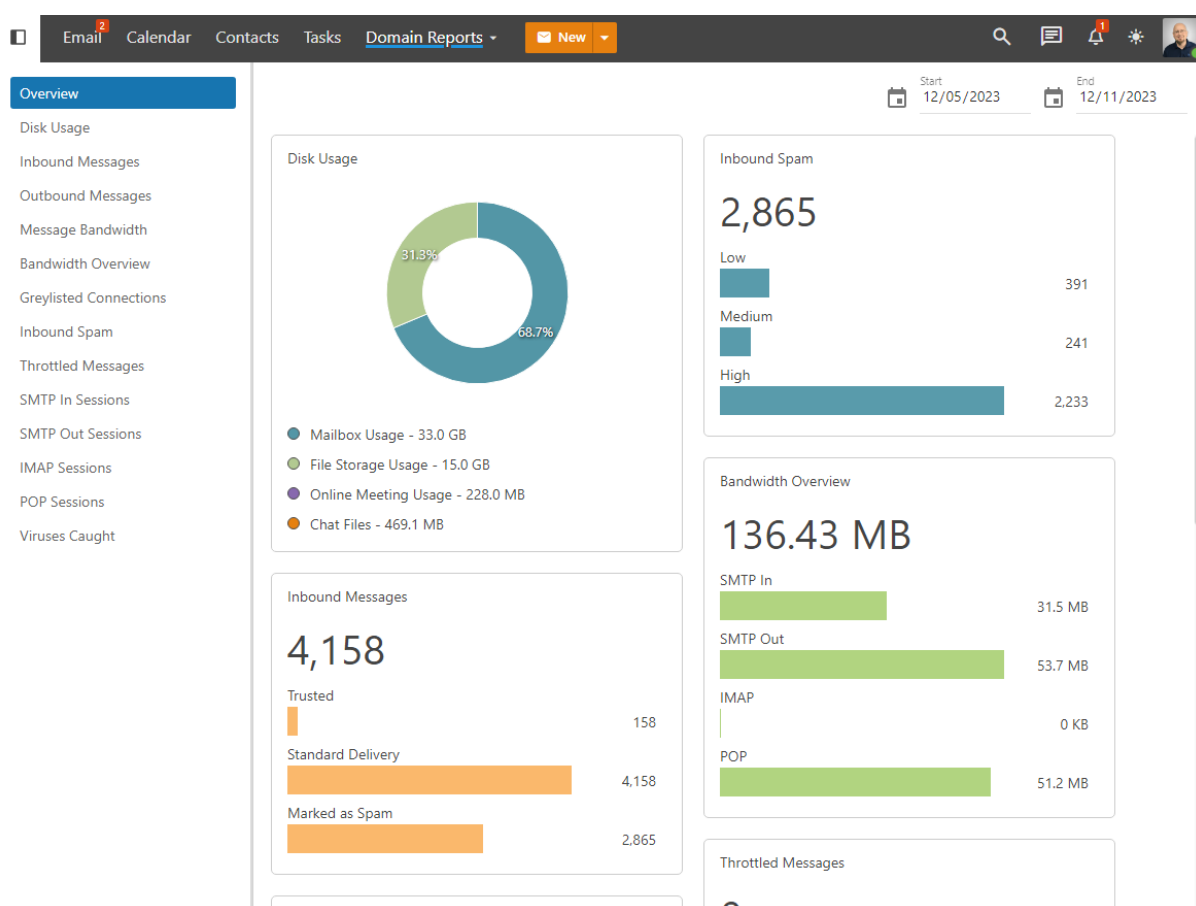
System Administrators

Finally, system administrators have access to a number of system-wide reports that give a detailed overview, as well as minute detail, about how the server itself is performing. For example, drive usage and average read/write statistics, memory usage, drive statistics and other server health items. In addition, system administrators can drill down into trend reports to view domain usage reports, then drill down further and view statistics down to the individual user level. System administrators also have access to detailed security reports such as abuse detection reports and information on blacklisted/whitelisted domains.

There is also a dashboard available to system administrators that gives a quick overview of how the server is running as a whole. This includes the uptime for the mail service, CPU and memory usage, drive statistics and much more.
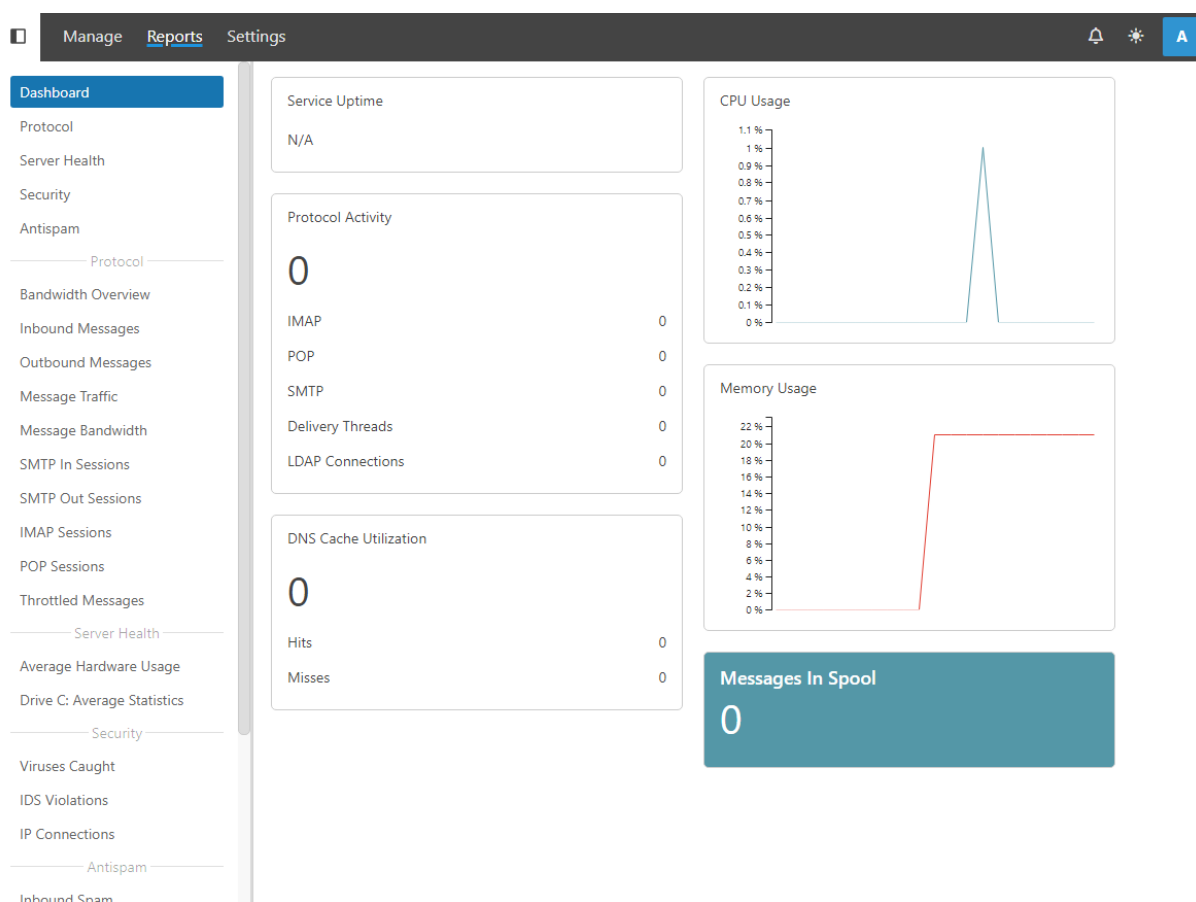
User Reports

Overview

In the Reports area, the Overview report is essentially a dashboard that gives users a quick update of certain aspects of their account. This includes point-in-time updates on their incoming and outgoing messages, a breakdown of overall disk usage, and spam counts and viruses caught.
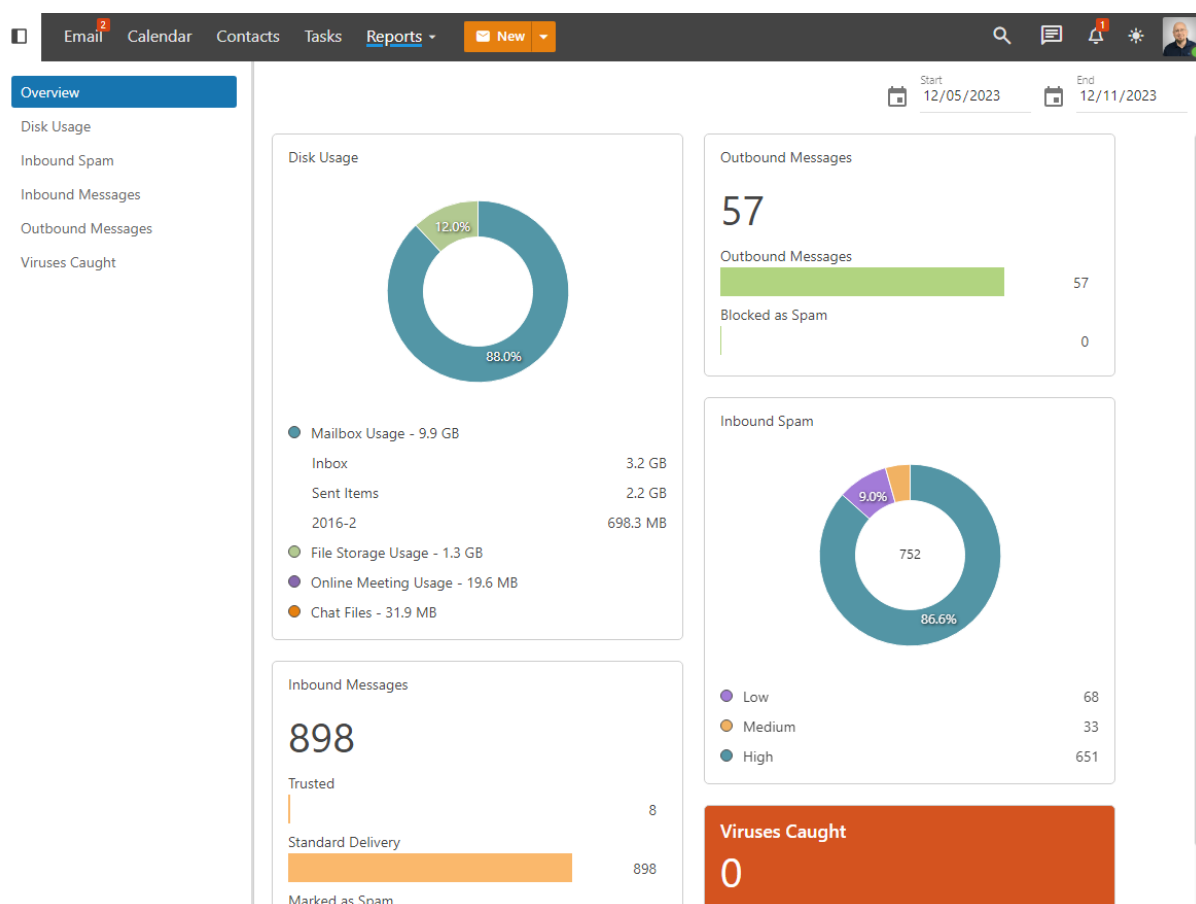
The cards on the dashboard include:

• Disk Usage - The overall disk space being used, which includes message data as well as file storage and online meeting storage. The "top" folders are listed as well. If a user is set to "unlimited" disk space, the circle chart displays how the disk space is being used. For users with a disk space limit, the chart will also show how much "free" disk space is available. The graph shows the percentage of the total spaced used by each category. (If the spaced used percentage is less than 1, it will display in the graph as 0%.)

• Inbound Messages - The total number of messages received by the user in the given period. This includes messages received from trusted senders, messages delivered via standard delivery and messages marked as spam.

• Outbound Messages - The total number of messages sent by the user in the given period, including a separate item for outgoing messages that were blocked as spam.

• Inbound Spam - The total number of messages marked as spam, with a breakdown of the 3 spam levels: High, Medium and Low. The graph shows the percentage of the total for each spam level. (If the spam % is less than 1, it will display in the graph as 0%.)

• Viruses Caught - The total number of viruses caught and quarantined by SmarterMail for the given period.

User Disk Usage Report

This report provides a user with an understanding of their overall disk space usage. Each folder the user has is listed along with file storage, showing a user their usage based on the type of item being looked at. A chart is also provided for a visual understanding of overall usage. As this is an overview of their usage, it's not possible to view any trend over time.

The following report items are available, and each column is sortable — ascending or descending — simply by clicking on the report item's header:

> • Folder - The name of the "folder" being returned. This includes default folders and custom folders, as well as folders created in File Storage and online meetings. As an aside, embedded folders are listed as Parent/Child. So, if you have a parent folder called "Sales" that has a "Bids" sub-folder, it would show up as Sales/Bids.
> • Type - The type of folder: either Mail or File Storage.
> • Percent of Total - The percentage of the overall total that is being used by that folder.
> • Disk Usage - The total disk space being used for that folder, in either KB or MB.

Inbound Spam

This report tells you the number of spam messages which you received, by tolerance level, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period, for each spam level identified.

A user can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Users can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

> • Day - The date the messages were received.
> • Spam Low - The total number of messages received with a low spam tolerance level.
> • Spam Medium - The total number of messages received with a medium spam tolerance level.
> • Spam High - The total number of messages received with a high spam tolerance level.
> • Spam Total - The total number of messages received will any spam tolerance level assigned to it.

Inbound Messages

This report tells you the number of messages which you received, by message type, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period, for each message type that's identified.

A user can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Users can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The date the messages were received.
- Inbound Messages - The total number of messages received that are NOT spam or NOT from a Trusted Sender.
- Inbound Spam Messages - The total number of messages received that were marked as spam.
- Inbound from Trusted - The total number of messages received that were sent from a Trusted Sender.

Outbound Messages

This report tells you the number of messages which you sent for whatever time period you specify. There is also a handy chart that displays the trend line for the time period, for each message type that's identified.

A user can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Users can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The date the messages were sent.
- Outbound Messages - The total number of messages sent that are NOT spam.
- Outbound Spam Messages - The total number of messages you sent that were marked as spam.

Viruses Caught

This report tells you the number of viruses that were received, per message, through email and caught by the virus protection set up by your system administrator for whatever time period you specify. There is also a handy chart that displays the trend line for the time period.

A user can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Users can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The day of the week covered by the report.
- Viruses Caught - The total number of viruses detected from incoming mail.

Domain Admin Reports

Overview

In the Reports area, the Overview report is essentially a dashboard that gives domain administrators a quick update of certain aspects of their domain. This includes point-in-time updates on their incoming and outgoing messages, a breakdown of overall disk usage, and spam counts and viruses caught.
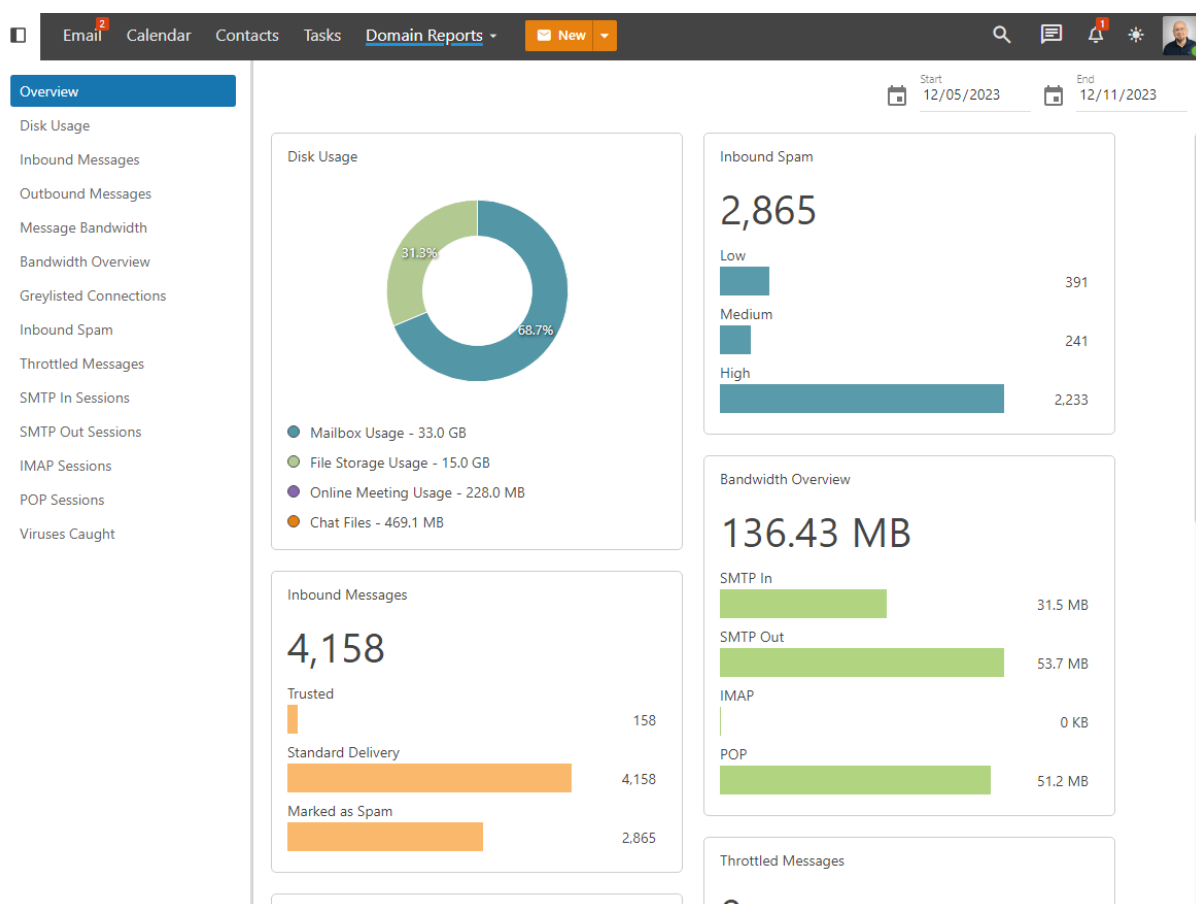
The cards on the dashboard include:

• Disk Usage - The overall disk space being used, which includes message data as well as file storage and online meeting storage.

• Inbound Messages - The total number of messages received by domain users in the given period. This includes messages received from trusted senders, messages delivered via standard delivery and messages marked as spam.

• Outbound Messages - The total number of messages sent by domain users in the given period, including a separate item for outgoing messages that were blocked as spam.

• Message Bandwidth - The total bandwidth used for incoming and outgoing messages.

• Greylisted Connections - The total number of connections that were greylisted, and thereby delayed, as well as the total number messages that bypassed greylisting.

• Inbound Spam - The total number of messages marked as spam, with a breakdown of the 3 spam levels: High, Medium and Low.

• Bandwidth Overview - The total bandwidth used, by protocol, for the time period selected.

• Throttled Messages - The total number of messages throttled and delayed.

• SMTP Out Sessions - The total number of outgoing messages for the time period selected.

• SMTP In Sessions - The total number of incoming messages for the time period selected.

• IMAP Sessions - The total number of IMAP sessions for the time period selected. These

would be messages received via an email client or outside service using the IMAP protocol.

• POP Sessions - The total number of POP sessions for the time period selected. These would be messages received via an email client or outside service using the POP protocol.

• Viruses Caught - The total number of viruses caught and quarantined by SmarterMail for the given period.

Domain Disk Usage Report

This report provides a domain administrator with an understanding of the overall disk space usage for the domain as a whole, broken down by each individual user. Each folder the user has is included in their total along with file storage and online meetings. A chart is also provided for a visual understanding of overall usage. As this is an overview of their account usage, it's not possible to view any trend over time. To see the list of folders for a particular user, and the usage details for each, simply click on their name.

The following report items are available, and each column is sortable — ascending or descending — simply by clicking on the report item's header:

• User - The name of the owner of the mailbox. Clicking on the username will open a new report that will display a breakdown of the disk usage for that particular user.

• Last Login - The date of the user's last login to the webmail interface.

• Percent of Total - The percentage of the overall total that is being used by that user.

• Disk Usage - The total disk space being used for that user, in either KB or MB.

• Disk Space Limit - The total amount of disk space allocated for the particular user. If the disk space is unlimited, an infinity sign is displayed. (∞)

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Inbound Messages

This report tells you the number of messages which all users of the domain received, by message type, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period, for each message type that's identified.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the

report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The date the messages were received.
- Inbound Messages - The total number of messages received that are NOT spam or NOT from a Trusted Sender.
- Inbound Spam Messages - The total number of messages received that were marked as spam.
- Inbound from Trusted - The total number of messages received that were sent from a Trusted Sender.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Outbound Messages

This report tells you the number of messages which were sent by all users of the domain for whatever time period you specify. There is also a handy chart that displays the trend line for the time period, for each message type that's identified.

A domain admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The date the messages were sent.
- Outbound Messages - The total number of messages sent that are NOT spam.
- Outbound Spam Messages - The total number of messages you sent that were marked as spam.

• Total Outbound Messages - The total number of outbound messages, including outbound spam messages.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Message Bandwidth

This report tells you the total bandwidth used by all users of the domain for whatever time period you specify. There is also a handy chart that displays the trend line for the time period for both incoming and outgoing bandwidth.

A domain admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

• Day - The date the messages were sent.
• Data Sent - The total bandwidth used for outgoing messages.
• Data Received - The total bandwidth used for incoming messages.

The primary benefit of this report is when tracking down email abuses. If a particular day shows a significant amount of bandwidth used for sending messages, there's a good possibility that either a user is spamming the server or that a user was compromised. If a day shows a significant amount of bandwidth used, the domain admin can change the report's Mode and pull up the list of mailboxes to further troubleshoot which user is causing the increased load.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Bandwidth Overview

This report tells you the total bandwidth used by all users of the domain, per protocol, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period for both incoming and outgoing bandwidth.

A domain admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The date the messages were sent.
- SMTP In - The total bandwidth used for incoming messages.
- SMTP Out - The total bandwidth used for outgoing messages.
- IMAP - The total bandwidth used for IMAP traffic. This is generally bandwidth used by email clients connected to the mailbox using IMAP as the connection method.
- POP - The total bandwidth used for POP traffic. This is generally bandwidth used by email clients connected to the mailbox using POP as the connection method.

The primary benefit of this report is when tracking down email abuses. If a particular day shows a significant amount of bandwidth used for sending or receiving messages, there's a good possibility that either a user is spamming the server or that a user was compromised. If a day shows a significant amount of bandwidth used, the domain admin can change the report's Mode and pull up the list of mailboxes to further troubleshoot which user is causing the increased load. Understanding "how" the bandwidth is being used — for example, if IMAP shows a significant increase for a particular user — makes it easier for an admin to track down what exactly is happening and where.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Greylisted Connections

This report tells you the number of allowed connections and delayed connections for all messages sent to the domain, for whatever time period you specify. Blocked connections would be those that were greylisted, meaning there was a slight delay between when the message was sent and when it was actually delivered. There is also a handy chart that displays the trend line for the time period.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The day of the week covered by the report.
- Passed - The total number of messages that passed greylisting and were delivered to the mailbox without delay.
- Blocked - The total number of messages that were delayed due to greylisting.
- Total - The total number of connections made to the domain. (I.e., SMTP, POP, IMAP, etc.)

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Inbound Spam

This report tells you the number of spam messages which were received at different tolerance levels for your specific domain. There is also a handy chart that displays the trend line for the time period.There is also a handy chart that displays the trend line for the time period.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the

report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The day of the week covered by the report.
- Spam Low - The total number of messages received with a low spam tolerance level.
- Spam Medium - The total number of messages received with a medium spam tolerance level.
- Spam High - The total number of messages received with a high spam tolerance level.
- Spam Total - The total number of messages received will any spam tolerance level assigned to it.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Throttled Messages

This report shows the number of messages that have been throttled for the domain, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

Domain administrators may use this report to identify issues with high usage customers. For example, if a user is sending a high number of messages, and is, therefore, hitting a throttling threshold, that is an unnecessary use of system resources that can be easily corrected.

The following report items are available:

- Day - The day of the week covered by the report.
- Throttled - The total number of messages throttled by the server.

• Delayed - The total number of messages that were delayed — or not sent out immediately — due to a throttling violation.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

SMTP In Sessions

This report tells you the number of connections plus the different types of issues reported from SMTP incoming mail for your specific domain. Domain administrators may use this report to identify high usage accounts, or accounts that have seen particular types of issues. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

• Day - The day of the week covered by the report.
• New Connections - The total number of overall, inbound connections to the mail server on that day.
• Blocked Connections - The number of inbound connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.
• Bad Commands - The total number of connections that had invalid SMTP commands, poor syntax, etc.
• Terminations - The total number of permanent errors for incoming messages due to spam weight, too many recipients, bad commands, etc.
• Bandwidth - The total amount of bandwidth used for all connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right

hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

SMTP Out Sessions

This report tells you the number of connections plus the different types of issues reported from SMTP outgoing mail for your specific domain. Domain administrators may use this report to identify high usage accounts, or accounts that have seen particular types of issues. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. This report can also be used to find potentially compromised accounts because the administrator would see a jump in outgoing SMTP connections over time, and possible a jump in errors.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The day of the week covered by the report.
- New Connections - The total number of overall outgoing connections from the mail server on that day.
- Blocked Connections - The number of outgoing connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.
- Bad Commands - The total number of connections that had invalid SMTP commands, poor syntax, etc.
- Terminations - The total number of permanent errors for outgoing messages due to spam weight, too many recipients, bad commands, etc.
- Bandwidth - The total amount of bandwidth used for all connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

IMAP Sessions

This report tells you the number of connections plus the different types of issues reported for clients or other services connected to user accounts using the IMAP protocol. Domain administrators may use this report to identify high usage accounts, or accounts that have seen particular types of issues. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. This report can also be used to find potentially compromised accounts because the administrator would see a jump in outgoing IMAP connections over time, and possible a jump in errors.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The day of the week covered by the report.
- New Connections - The total number of IMAP connections from the mail server on that day.
- Blocked Connections - The number of IMAP connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.
- Bad Commands - The total number of IMAP connections that had invalid SMTP commands, poor syntax, etc.
- Terminations - The total number of permanent errors for IMAP messages due to spam weight, too many recipients, bad commands, etc.
- Bandwidth - The total amount of bandwidth used for all IMAP connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

POP Sessions

This report tells you the number of connections plus the different types of issues reported for clients or other services connected to user accounts using the POP3 protocol. Domain administrators may use this report to identify high usage accounts, or accounts that have seen particular types of issues. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. This report can also be used to find potentially compromised accounts because the administrator would see a jump in outgoing POP connections over time, and possible a jump in errors.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The day of the week covered by the report.
- New Connections - The total number of POP connections from the mail server on that day.
- Blocked Connections - The number of POP connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.
- Bad Commands - The total number of POP connections that had invalid SMTP commands, poor syntax, etc.
- Terminations - The total number of permanent errors for POP messages due to spam weight, too many recipients, bad commands, etc.
- Bandwidth - The total amount of bandwidth used for all POP connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Viruses Caught

This report tells you the number of viruses that were received through email, per message, for all users of the domain and caught by the virus protection set up by the system administrator, for whatever time

period you specify. This includes numbers for Windows Defender and ClamAV. There is also a handy chart that displays the trend line for the time period.

Regarding the counts, this report is a per-message report. That means that the numbers seen may not appear to match up, when looking at the domain as a whole versus looking at individual users of the domain.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

Domain admins can also switch the report from a "Trend" report, which shows the data for the domain as a whole, to display information by User. This is called the report's "Mode".

The following report items are available:

- Day - The day of the week covered by the report.
- Viruses Caught - The total number of viruses detected, either incoming, outgoing or both.

To dig down into a report, it's possible to change the report's Mode from Trend to Users. Selecting Users allows a domain administrator to see which users received viruses during the time period. This can help note if a generic address, such as sales@@ or administrator@@ addresses, are being targeted so that appropriate action can take place.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Settings

User Settings

Account

The Account Settings section contains basic configuration options for a user's account, including their forwarding and reply-to addresses, webmail preferences and more.

When accessing your account settings, the following cards will be available, each with its own options:

- Changing your Password
- User
- Notifications
- Folder Auto-Clean
- Default Folders
- WebDAV
- Webmail
- Email
- Forwarding
- Two-Step Authentication

Changing your Password

To change the password used to log into your SmarterMail account, click on the Change Password button at the top of the Account page. In order to protect your security, you will be required to enter the current password before entering the new one.

Your new password must meet the following requirements:

- At least 12 characters long
- Includes at least one uppercase letter
- Includes at least one lowercase letter
- Contains at least one number (0–9)
- Includes at least one special character (e.g., #, @@, &, etc.)
- Does not match your username
- Is not a commonly used password

If your SmarterMail credentials are handled in Active Directory or if you do not have permission to change your password, you will need to contact your domain or system administrator for assistance. Depending on who manages your SmarterMail email services, this could be the IT department of your company or a third-party hosting company / ISP.

User

- Language - The language a user selects/sets for use in SmarterMail is EXTREMELY important. That's because it's much more than simply what is seen in the webmail client. SmarterMail's language selection is the basis for everything: the things you see in the webmail interface as well as what's returned to an email client when you connect using Outlook, eM

Client, iOS Mail and more. That includes things like settings labels, folder names, calendars and calendar appointments, contact groups, email message content, log files and essentially everything within SmarterMail. Therefore, it is extremely critical that whatever language is set in SmarterMail is the language you actually want to use. Note: The options displayed here are dependent upon the translation files the SmarterMail administrator has added to the mail server. Furthermore, SmarterMail translation files are provided by product users, and SmarterTools makes no warranty on the correctness of the translation.

• Changing Language Settings : When a user tries to update their language, SmarterMail checks for potential conflicts prior to changing the language. For example, if a user is set to English and they have a folder named "Bandeja de entrada", if they try to change their language to Spanish, the change will not be saved and they will see a warning letting them know that the language wasn't updated to prevent an email folder name conflict. This is because "Bandeja de entrada" is the Spanish name for Inbox used in the default Spanish language translation file. If the change was saved, there would be 2 folders with the same name, which would cause issues.

• Time Zone - The time zone of your location. This field determines the timestamp for items within the interface, including the date and time messages were received or a Note was updated.

• Reply-To Email Address - The email address used in the reply-to header of messages sent through webmail. This address will be used by receiving email clients when replying to a message. While it's possible to set the Reply-to address for a user, that user can change the Reply-to when composing a message or reply in an email client, such as Microsoft Outlook. Should they do this, that address will take precedence over what's set in the user's settings.

• Recovery Email Address - The email address to which password reset instructions will be sent if you forget your password. This is also the address used for Two-Step Authentication, if it's enabled for your user. (Or Forced by the system or domain administrator.) This address should be separate from the SmarterMail account, such as a Gmail or Yahoo! address, or even the default email address of a domain administrator. Note: The backup email address can only be used if two-factor authentication is in use, or if the system administrator has enabled password retrieval for the login page.

• Plus Addressing - Plus addressing allows users to automatically sort incoming email without creating content filtering rules first. One of its major benefits is that it allows users to generate special email addresses if they do not want to give out their real address. For example, if user@@example.com needs to provide a valid email address to sign up for a newsletter, he can sign up for the newsletter using the following address: user+technewsletter@@example.com. When the newsletter is delivered, it can automatically be routed to the Technewsletter folder. If the folder does not already exist, it can be created automatically. In addition, sub-folders and/or folders with spaces can be created as part of a Plus Address. If you include the "/" character in

your plus address, you can automatically create subfolders. For example, the plus address myname+Newsletters/ACME@@example.com will create a folder called Newsletters, then create an ACME folder under it, and drop the newsletter into the ACME folder. Using an underscore (_) in the folder name will create it with a space. For example, myname+acme_newsletters will create a folder called Acme Newsletters. As an added bonus, you can connect to folders in your email using POP3 by using plus addressed emails. The example above, when input into your POP email client as your login name, will return the contents of that folder. Note: For plus addressing to work, the plus (+) sign is required AFTER the username but BEFORE the domain name. For example, username+foldername@@domain.com.

• Disabled - Select this option to turn off plus addressing for your account.
• Move to Folder - If the target folder already exists, the incoming message will be placed into it. If the folder does not exist, it will be created automatically. Note: To prevent abuse, no more than 10 folders can be auto-created in this method during a six-hour period.
• Move to Folder (If Exists) - If the target folder already exists, the incoming message will be placed into it. If the folder does not exist, the email will be placed in the Inbox.
• Leave in Inbox - The incoming message will be placed in the Inbox.
• Show in Global Address List Enables or disables the user from being displayed in the GAL. Some users, especially generic ones (hr@@, billing@@, etc.) may not need to be displayed in the GAL. Note: MAPI requires use of the Global Address List (GAL) in order to work properly. Therefore, regardless of whether the domain's Global Address List feature is disabled, or a user/alias has Show in GAL disabled, Outlook MAPI will always show the GAL directory and be available via autocomplete when typing in a recipient's email address.

Notifications

Browser notifications allow your browser to alert you about common activity within SmarterMail, even if your browser window is minimized or hidden behind other screens. Note: In order for browser notifications to work, your browser must be running and logged into a SmarterMail site.

A request to enable browser notifications will appear upon your first login to SmarterMail, when using a new browser or after clearing your standard browser's cookies. If your Account Settings page shows the message: "Browser notifications have been disabled in this browser," it means that you have denied the request to push these alerts. Instructions on how to enable notifications for a site vary with each browser, so we encourage reviewing your browser documentation for the exact steps.

The following alerts can be enabled or disabled for browser notifications.

• Calendar reminders - Enable or disable notifications for calendar appointments that have a reminder enabled.

• Chat messages - Enable or disable notifications when a chat message is received from SmarterMail's standard Chat section or an online meeting.

• New emails - Enable or disable notifications when an email is received in your Inbox.

Folder Auto-Clean

Setting up auto-clean rules for email folders is a simple, yet effective, way to limit how much of your disk space is taken up by messages in default folders like Junk Email, Sent Items, and Deleted Items as well as any custom folders a user creates. Unlike domain administrators, who can only create auto-clean rules on the default folders created by SmarterMail, users can set up rules for any folder, including custom folders.

Setting up auto-clean rules helps users ensure that their disk space does not fill up unnecessarily. In some cases, particularly when SmarterMail is being provided by a hosting company or ISP, users may have disk space limits set for their accounts. Keeping unnecessary or unwanted email cleaned up, and freeing up space that could be used by unnecessary messages, is one way to help these users stay within the limits placed by their hosting company.

• Override auto-clean settings - Enable this setting to override the settings established by the domain administrator, allowing you to create your own rules. Any changes you make will not be affected if the system administrator changes their policy, unless they disable domain overrides.

If the "Override auto-clean settings" setting is missing, the auto-clean rules created by the Domain or system administrator will be displayed at the bottom of this card. If no rules were created by an administrator, a note saying such will be displayed.

However, if "Override auto-clean settings" is turned on, you're presented with a New rule button that will allow you to create your own rule(s). Auto-clean rules can be created for any default mail folder, and can be created based on a message's age, the length of time a message has been in a folder, or a particular folder's size.

Size of Folder vs. Age Rules

It's possible to set an auto-clean rule either based on the size of a folder, or the age of a message (or messages) within a folder. Size-based auto-clean rules are run whenever an action is performed on a particular folder. For example, moving a message into the folder. Once that action occurs, the auto-clean rule is run, and it runs each time an action is performed. Age-based rules, however, run once per day, on the FIRST folder action for that day. For example, deleting an email first thing in the morning. When you delete an email, it's moved to the Deleted Items folder, which is a folder action. At that

point, if there's an age-based auto-clean rule for the Deleted Items folder, the rule is run, and then is silent until an action is performed on the next day. If no action is performed on a folder with an age-based rule, the rule still runs automatically shortly after midnight, server time.

When using a folder's size, it's possible to set upper and lower limits for the space used for the folder. For example, you can create an auto-clean rule so that when a folder gets larger than 50MB in size, the rule automatically deletes messages to reduce the folder's size to 5MB. When freeing up space, the total size of each message is used, which includes any message attachments.

When using Age as a guideline, there are two types of age: Message Age and Age in the Folder.

- Message Date: This is based on the initial receipt date of the message. So if you received a message on January 1st, and the number of days is set to 14, on January 15 the message is automatically deleted.
- Time in Folder: This is based on when a message is actually moved to the folder that has the auto-clean rule configured. The age of the message itself is not used. That means, if the Age in Folder is set to 14 days, it doesn't matter when the message was received. Instead, the message is deleted 14 days after it's been moved into the folder.

Default Folders

When creating a new user in SmarterMail, default folders are created for holding certain types of information. Calendar appointments/events, contacts, notes, tasks, etc. are initially stored in these folders: My Calendar, My Contacts, My Notes, My Tasks. However, users may want to change where this information is held when, for example, a new contact is added. Users may want contacts stored, by default, in their own "Business Contacts" folder as opposed to My Contacts. This is where specifying default folders comes in handy.

It is worth mentioning that only existing folders can be selected as a new default. Therefore, users will need to go to specific areas and create new folders before they can be selected as the new default folder.

Changing the default folder for a specific item is simply a matter of selecting it from the relevant dropdown. Once a default folder is changed, any new item created will be stored in that folder. (Existing items remain in their original folder. Only new items will use the new default.) note: If a particular user has any Delegation rules, default folders can not be changed.

WebDAV

WebDAV is an open standard that extends standard HTTP and allows users to attach to, and interact with, collaborative items such as calendars, contacts, etc. using email clients, mobile clients,

scheduling services, and more. This link, then, is what would be used when attempting to attach, for example, a user's calendar to a scheduling services such as Harmonizely.com.

Webmail

This card covers how to access the SmarterMail web interface using your preferred browser. To adjust these settings, log in to your SmarterMail account, click the More button, scroll down to Settings , and you'll find the Webmail card in your Account . For a list of supported browsers, see Browser Requirements .

- Compose Font - Specify the default font for emails by selecting an option from the list.
- Font Size - Specify the default font size for emails by selecting an option from the list.
- Default From Address - Select the email address that you reply from by default for messages sent through webmail. Your SmarterMail email address and any domain aliases or SMTP accounts configured will be shown in this list. (This setting does not prevent you from manually changing the Send From address when composing a message.)
- Preview Pane - To specify where the preview pane displays in the webmail interface, select the appropriate option from the list: Right or None. By default, the preview pane appears to the right of the messages list. Disabling the Preview Pane means only a list of messages appears in the content pane and each message will need to be opened separately in order to view their contents.
- Search Language Indexer - The language that the Lucene indexer will index against. In most cases, Generic Indexer is the best selection as it incorporates English and common umlauts. However, if the interface is viewed in certain languages, such as Chinese, Japanese, or Korean, this setting should specify the language for better indexing results.
- Use received address as from address for replies - When enabled, replying to a message via webmail will use that email's To: field as the From: address for your reply. This means messages sent to your main SmarterMail email address, to a domain alias, to an email alias, to an SMTP account, to a disposable address or even to a Plus address will have replies sent from those same addresses. For example, if an email is sent an alias you are part of (e.g., office@your_domain.com), when you reply to that email via webmail, the reply will be sent from office@your_domain.com. The same holds true for domain aliases. If you have your_domain.com as the primary domain, and a domain alias of your_other_domain.net, and an email is sent you your_name@your_other_domain.net, when you reply to that email using webmail, the reply is sent FROM your_name@your_other_domain.net. (This setting does not prevent you from manually changing the From address when composing the reply in webmail.)
- Request read receipts by default - Select this option to automatically request read receipts for all outgoing messages sent via webmail. When this setting is enabled, all outgoing messages that are sent via webmail will request that the recipient(s) send a read receipt when the message

has been read. If the read receipt is sent by the recipient(s), you will receive a message from the system administrator confirming that the message has been read. Note: Users should be careful when enabling this feature and should only do so if required for business or compliance or regulatory requirements.

• Request delivery receipts by default - Select this option to automatically receive delivery receipts for all outgoing messages sent via webmail and email clients. When this setting is enabled, you will receive a message from the system administrator verifying the delivery status of your outgoing message. Note: Users should be careful when enabling this feature and should only do so if required for business or compliance or regulatory requirements.

• Draft auto-save - Enable this option to have drafts of messages created within the webmail client to be saved every 2 minutes.

• Hide email avatars in the message list - Enable this option to hide any avatars — images, monograms, Gravatar pictures, etc. — from your list of messages. This disables avatars for all folders, including custom folders. It does not have any effect on messages, or messages that display in the content pane.

• Show images from external websites - Enable this option to automatically display all in-line remote content when an email is viewed. (Remote content is considered to be any image, video, animated gif, etc. that has an external source and is contained in the message.) When this is enabled, you will not have to manually display the remote content on emails you receive; it will be visible automatically. Note: Emails from trusted domains and senders will always display remote content automatically.

• Allow Inline Images From - Here you can enter the email addresses or domains (one entry per line) whose in-line remote content should be displayed automatically, even if the previous setting is turned off. If an email address is entered, emails received from that address will automatically display all remote content. If a domain is entered, remote content that comes from a source containing that domain will be automatically displayed. For example, if "smartertools.com" was entered in this field, remote content from a source of "https://images.smartertools.com" would be automatically displayed, even if that email was sent from user@@example.com. (If an exception for an email address is added from an email directly, that email address will be listed here.) Note: Emails from trusted domains and senders will always display remote content automatically.

• Allow Email Tracking From - Here you can enter the names of mail tracking providers (one entry per line) that you will allow. In addition, when enabling an email tracking provider from the tracker modal on individual messages, they appear here.

Email

This card applies to configuration in email clients such as Outlook, eM Client, Apple Mail, Windows Mail, Spark, Thunderbird, Mailbird, and others. To adjust these settings, log in to your SmarterMail account using the web interface, click the More button, scroll down to Settings , and you'll find the Email card in your Account . For details on supported email clients, please refer to Synchronizing with SmarterMail .

• Delete Email Action - To specify the action performed on deleted email messages (not folders — deleted folders and their contents will always go to the Deleted Items folder), select the appropriate action from the list. Note: Messages deleted from the Junk Email folder are always permanently deleted and do not follow the Delete Email Action that is set.

• Move to Deleted Items folder - Deleted items will appear in the deleted items folder, which will need to be regularly emptied.

• Permanently Delete - Permanently deletes and purges the message. Note: When deleted messages are purged, the action is final. You will not be able to retrieve these messages later.

• Mark as Deleted - Flags the message for deletion, but it does not move messages to the Deleted Items folder and messages remain until the folder is purged.

• Move to Junk Action - Using Move to Junk moves the email to your Junk Email folder, and also helps the system recognize the sender and message contents as possible spam. This information is used to help train new HAM/SPAM settings that are available to system administrators.

• Move to Junk Only - Emails will be sent to the Junk Email folder, so you'll want to check this folder and clear it out every now and then. note: When enabled, all email headers will be checked using the From address in the header, which may differ from the From address displayed in the message.

• Move to Junk and Block Sender - Emails from this sender will go straight to your Junk Email folder, and the sender's email address will be added to your Blocked Senders list. Be sure to check and clear your Junk Email folder periodically.

• Move to Junk and Block Domain - Emails from this domain will go straight to your Junk Email folder, and the email domain will be added to your Blocked Domain list. Be sure to check and clear your Junk Email folder periodically. note: When you move an item to Junk, it won't appear in the Blocked Senders or Blocked Domains list right away, it may take 5 to 10 minutes to update.

• Remove from Junk Action - Removing an email from Junk moves it to any folder you choose, whether your inbox or a custom folder you've created.

• Remove from Junk Only - Removing an email out of Junk will place it into any folder you choose, whether it's your inbox or a custom folder you've created (this is the default action).

• Add to Trusted Senders - Enabling this setting will will move the email from your Junk Email folder to a folder of your choice, such as your Inbox or any custom folder you've created. The sender will also be added to your Trusted Senders list.

• Remove from Junk and Remove from Block - Enabling this setting will will move the email from your Junk Email folder to a folder of your choice, such as your Inbox or any custom folder you've created. The sender or their domain will also be removed from any blocks added, based on your Move to Junk action. note: When you move an item to Junk, it won't appear in the Blocked Senders or Blocked Domains list right away, it may take 5 to 10 minutes to update.

• Mark messages downloaded by POP as read - Enable this option to mark all messages that are downloaded via a POP3 connection as read.

Forwarding

If this card is not displayed, you are not permitted to utilize automated forwarding. This feature must be enabled for the domain and for your user. Contact a SmarterMail administrator for assistance enabling this feature.

• Forwarding Address - The email address to which messages sent to your mailbox will be automatically forwarded. Note: Messages routed to other email folders via content filters or plus addressing will also be forwarded to this address. Messages routed to the Junk Email folder will not be forwarded by default. However, these can be included if the domain's "Forwarding Exclusion" is set to "No exclusion - Forward all mail."

• Keep original sender and recipients when forwarded - When enabled (which is the default), an email is essentially re-routed to the new recipient and keeps its original "To" and "From" addresses. When disabled, the forward behaves as if the email was manually forwarded, so the "From" address is replaced with the address of the mailbox forwarding the message, and the "To" address is the mailbox listed in the Forwarding Address.

• Delete messages when forwarded - Enable this option to delete messages from your SmarterMail mailbox after they are forwarded.

Two-Step Authentication

When enabled for a domain by the system administrator, Two-Step Authentication adds an extra layer of protection to your SmarterMail account. It ensures that only YOU can access your account, even if someone knows your password.

When you are protected with Two-Step Authentication, logging into webmail requires two methods of authentication: your SmarterMail password and a verification code that's only available to you. This

code can be generated from an app, like the Google or Microsoft Authenticator apps available for iOS and Android, or delivered via a recovery address that's set up for your account. In addition, if you access email using a mobile or desktop email client, such as Microsoft Outlook or Apple Mail, you will need to use "application passwords" when setting up those accounts. (If you have already set up an email client, you'll need to re-log in using an application password after Two-Step Authentication is set up.)

Once you click the Enable button, you'll walk through the process of setting up Two-Step Authentication. The steps you walk through depend on which type of authentication you select: Authentication App or Recovery Address. Regardless, the fields you'll see are as follows:

Two-Step Authentication   ?

When logging in, your account will be secured with a password and verification code. Retrieve the code through an authenticator app, such as Google Authenticator.

Email clients or applications that use your account will be disconnected until you reconnect those accounts using the new Application Passwords.

Verification Methods
Authenticator App   ▼

Recovery Email Address *
jsmith@gmail.com

Confirm Recovery Email Address *
jsmith@gmail.com

Cancel   Next

- Verification Methods - This is where you select the type of additional verification you want to use: Authenticator App (e.g, Google or Microsoft Authenticator) or Recovery Address. Regardless of which method you choose, you'll have to supply a Recovery Email Address. This is necessary even when using an Authenticator App for instances where issues occur with the

app, such as the inability to scan a QR code, that may require an authentication code to be emailed to you.

• Recovery Email Address - This is an alternative email address, different than the one you're using, that can receive authentication codes. If you already have one set for your account, it will be displayed here. However, you can change it to a separate address if you so desire. You will have to re-enter this address to confirm it on the next line.

• Verification Code - If using the Authenticator App method, you'll be asked to scan a QR code with the app you want to use for authentication, then enter the code displayed by the app. If you're using Recovery Email Address, you'll need to enter the verification code that was emailed to that address.

Setting Up Two-Step Using a Recovery Email Address

Using a Recovery Email Address means that each time you log in to webmail, a verification code will be sent to the Recovery Email Address you specify. You then enter that code on the SmarterMail login screen for your account, prior to being able to access webmail. To get started with using Two-Step with a recovery address, do the following:.

• Select Recovery Email Address from the Verification Methods dropdown.

• Enter and confirm the Recovery Email Address that will be used to retrieve the verification code. (This email address will automatically be used as the Recovery Email Address used for resetting your password as well.)

• Click Next.

• Wait a moment for the verification code to be sent to that address, then enter the 6-digit code once it's received.

• Click Check to confirm the verification code and complete the Two-Step Authentication setup.

Setting Up Two-Step Using an Authenticator App

Using an Authenticator App, such as Microsoft Authenticator, means that each time you log in to webmail, you'll retrieve the verification code from your authenticator app of choice. You then enter that code on the SmarterMail login screen for your account, prior to being able to access webmail. To get started using an Authenticator for Two-Step, do the following:

Two-Step Authentication   ?

Using an authenticator app, such as Google Authenticator, scan the QR code below, and provide the 6-digit verification code.

Can't scan the QR code?

Verification Code *

Cancel   Back   Check

• Install an authenticator app, such as Google or Microsoft Authenticator , on your phone or computer. (In this article, we'll demonstrate how to set up Two-Step Authentication using Google Authenticator on your mobile device.)

• Select Authenticator App from the Verification Methods dropdown.

• Enter and confirm a Recovery Email Address that will be used as an alternative method to retrieve the verification code. If your authenticator app is not accessible, the verification code will be sent to this address instead. (This email address will automatically be used as the Recovery Email Address used for resetting your password as well.)

• Click Next. A QR code will appear on the next page.

• Open the Google Authenticator app. Click "BEGIN SETUP" if you aren't already using it for other accounts, or use the plus (+) icon to add a new token.

• Select Scan QR Code to use your phone's camera to scan the code that's displayed in

SmarterMail. A new token will be added to Google Authenticator.

• Enter the token's 6-digit code into SmarterMail.

• (If you can't scan the QR code, click on "Can't scan the QR code?" in SmarterMail. In the Authenticator app, choose to create a new token by Manual entry. In the Account field, enter a token descriptor, such as the username of your account. In the Key field, type in the secret key that's displayed in SmarterMail. Then enter the token's 6-digit code into SmarterMail.)

• Click Check to confirm the verification code and complete the Two-Step Authentication setup.

Logging in with 2-Step

To log in to SmarterMail, enter your email address and password. Then enter the 6-digit verification code that's sent to your recovery email address or the token that's displayed in the authenticator app.

Configure Third-party Applications with App Passwords

Note that once 2-Step Authentication is set up for your account, you will also need to re-configure any third-party applications or email clients using the "application passwords" that are automatically generated and displayed on the Two-Step Authentication card in your Account settings. Several passwords are provided based on the protocol-type being used. For example, an EAS password would be used for any mobile email client. Passwords can be used multiple times, in multiple clients. They can also be reset/refreshed. Be sure to use the correct password for the corresponding protocol.

Two-Step Authentication

Congratulations! Your account is protected with two-step authentication!

Strong passwords have been created for third-party applications. In place of your normal account password, use the Application Password for the account you're setting up.

Disable

Webmail
Use normal account password

IMAP/POP/SMTP (Most email clients)
●●●●●●

EAS (Mobile clients, Microsoft Outlook, Windows Mail)
●●●●●●

MAPI & EWS (Outlook, Apple Mail, eM Client)
●●●●●●

WebDAV (Microsoft Outlook, etc.)
●●●●●●

LDAP (SmarterMail LDAP server)
●●●●●●

Regardless of which method you use, using Two-Step Authentication is a great way to keep your email communication protected.

Profile

The Account Profile section contains details for a user, including their name, birthday, email address(es), work information and more. If a system administrator has enabled the Global Address List (GAL), the information contained in a user's profile will be publicly available to all other users on the domain if that setting is enabled when the User is created by the domain administrator. Users can access that public contact information only by accessing the GAL through webmail or LDAP. Note: LDAP is a feature available to SmarterMail Enterprise users only.

The information contained in a user's Profile will also be available in email clients, such as Microsoft Outlook. This is especially true when syncing to that client using a protocol such as MAPI. In addition, much of the information configured in a user's Account Profile is also available as a variable that can be used when domain administrators create domain level signatures. Regardless, you can fill out as much or as little of this information as you want.

When accessing your profile, you'll be presented with a number of different cards:

Personal Info

- Display Name - Your name as you want it to appear. For example, "Dan Henderson".
- Title - Whatever Title you want to be used, such as Mr., Mrs., Dr., etc.
- First Name - Your first name.
- Middle Name - Your middle name.
- Last Name - Your last name.
- Suffix - If you have a suffix, such as "Jr.", "III", "Esq.", etc., put it here.
- Home Page - If you have a personal website, you can enter the URL here.
- Instant Messenger - If you have an IM handle, or a Skype address, you can enter it here.
- Birthday - Your birthdate goes here.
- Additional Information - You can pretty much add anything else you want in here: favorite color, pet's name, whatever.

Profile Pictures

To upload a profile picture, click on the avatar or current image next to your Display Name, which will open your File Explorer/Finder. From here, select the image you want to use for your profile.

Note: Photos/images must not be over 5mb in size; square images work best. Uploading a profile picture will automatically update your avatar in the webmail interface. However, profile pictures are not updated in any third-party chat clients, like Adium or Pidgin, until you log into the chat client and force a status change.

Phone Numbers

• Phone Number - Specify your home, work or mobile phone numbers, pager number and personal or company fax numbers. Once you add one number, another box appears below this one where you can add others.

Email Addresses

• Email Address - Add any secondary email addresses you have, like a Gmail address, a personal email address, etc. If you want to remove an address, simply click the X button next to it.

Addresses

• Home Address - Specify your home address, including your street address, city, state/province, postal code and country.
• Work Address - Specify your work address, including its street address, city, state/province, postal code and country.
• Work Info - Specify your work information, including your company name, job title, department, office, and the URL of your company's website.

Other

This area allows you to add any additional information you want associated to your profile. This includes your Anniversary (work or marriage), your nickname, the name of your spouse or assistant, etc. To prohibit the display of business hours, like for the weekends or other days off, simply put the same beginning and end time for that day of the week. (E.g., 11:00 PM - 11:00 PM)

Autoresponder

An autoresponder is a pre-written reply that is automatically sent when an email message is processed by SmarterMail. These are commonly used to notify senders of a change in contact information or that the recipient is out of the office or on vacation. For example, a standard autoresponder message could be: "I will be out of the office from June 1 to June 15. I will respond to your message upon my return to the office on June 16. If you need immediate assistance, please contact Jane Doe at jdoe@example.com."

SmarterMail offers two (2) types of autoresponder: one for domain users and one for "everyone else". This is helpful as you may want to let your co-workers know that, say, you're out of the office but you'll be available for calls if anything comes up, but let everyone outside of your organziation know that you're out of the office but will be back by a certain date. In addition, SmarterMail gives you some flexibility on who gets your "Out of Office" message and who doesn't. Autoresponders are sent

out once per day, per sender. That means that if you receive multiple emails from the same individual in a 24-hour period, they will only get 1 automated reply. This prevents inbox spamming as well as prevents the potential for "email loops" — such as if the person sending you a message has their own autoresponder set up, there is no chance for the 2 mailboxes to continually sending each other automated replies.

It's worth mentioning that if Autoresponder is not displayed in the navigation pane for a user, the system administrator of the installation may have it disabled for the domain. Therefore, the system administrator must enable Autoresponders on the Options tab in Antispam settings Note: As mentioned, autoresponders only work on messages processed by SmarterMail. Therefore, messages pulled into SmarterMail using Email Retrieval will not trigger an autoresponder for that message.

When accessing your autoresponders, the following items will be available:

Autoresponder

- Subject - The words or phrase that will appear in the subject of the autoresponder message (e.g. Out of Office).
- Response to Send to Domain Users - The message that will be automatically sent to the other accounts that have been set up for your domain. SmarterMail allows users to create HTML formatted autoresponders that can include stylized text, links, images and more.
- Response to Send to Everyone Else - This message will be sent to anyone outside of your domain. (Depending on the what's been set on the Options card.)

Options

System administrators can enforce a domain-wide autoresponder exclusion in order to prevent SmarterMail from sending autoresponder replies to spam messages. Otherwise, if no settings are passed down to you, you'll have the following options:

- Enable Autoresponder - Turn on the autoresponder. Once enabled, the below will display:
- Disable responses to indirect mail - By enabling this setting, the autoresponder will only be triggered by email sent directly to you. Any email you receive through a mailing list, forward, or an alias will not trigger the autoresponder.
- Only send between certain dates - Enable this setting to specify the date range that your autoresponder will be active. Then set the specified start and end dates and times. This option is particularly helpful for planned absences, like a vacation or extended holiday.
- Send To - This dropdown allows you to set up who received your autoresponder messages. You may not want to send one to just anyone who emails you, but only send them to a specific subset of people. This dropdown allows you to do just that.

• Domain Users Only - This will only send an autoresponder to others on your domain. In this instance, you'll only need to fill out the "Response to Send to Domain Users" message.

• Domain Users and Contacts Only - This will send an autoresponder JUST to others on your domain as well as anyone listed in "My Contacts". In this case, you'll want to fill out both messages.

• Everyone - This will send an autoresponder to anyone who emails you. In this case, you'll want to fill out both messages.

Calendar Settings

SmarterMail gives users several customized settings for how they want calendars to appear. This includes the default timeframe to display, calendar auto clean rules and more.

When accessing your calendar settings, the following options will be available:

Options

• Display weekends - Select this option to include weekends in your calendar. Because some people only use their calendars for the "business week," disabling weekends can help to keep a calendar clean and organized.

• Display task start times in the calendar view - Select this option to view the date and time a task is scheduled to start on the calendar.

• Display task due times in the calendar view - Select this option to view the date and time a task is scheduled to be completed on the calendar.

• Hide completed tasks - Select this option to remove completed tasks from the calendar view.

• Default Duration - The default amount of time to reserve for a new appointment or event. This is 1 hour by default.

• Default Reminder - The default amount of time prior the beginning of an appointment or event that will trigger a reminder notification for participants. This is 5 minutes by default.

• First Day of Week - The default day that a user's week begins. By default, this is Sunday.

Note: Even though tasks may be displayed in your calendar, if you are syncing your calendar with a desktop and/or mobile email client, the task will not show up on your calendar. Instead, they will generally be considered notifications and will display in mobile and/or desktop clients accordingly.

Calendar Auto-Clean

SmarterMail allows users to keep past calendar events from cluttering up their calendar views. Generally system and/or domain administrators will set this option for all users of the domain, but domain administrators may allow users to manage their own calendar auto-clean settings. Therefore, if you have the ability to "Override auto-clean settings", you can do so with this setting. Simply toggle

the setting, then select the "Auto-Clean Months" you want to use. Note: Recurring calendar appointments that are ongoing (i.e., have not ended) are not impacted by calendar auto-clean timings or settings.

Business Hours

SmarterMail allows users to customize new calendar appointments to display their typical hours. For example, if you typically schedule appointments from 8 a.m. to 5 p.m., you can configure the business hours to correspond with those times, allowing SmarterMail to automatically scroll your calendar view to those hours. You can configure the visible hours for each day of the week to allow for flexibility in your schedule.

Connectivity

SmarterMail provides a variety of options that allow users to manage and access third-party, external accounts directly within SmarterMail. When accessing your connectivity settings, the following options will be available:

Jump To:

- Email Retrieval - Download emails from third-party accounts directly into SmarterMail
- SMTP Accounts - Send emails from third-party accounts directly within SmarterMail
- Synchronized Devices - Review the syncing connections for your user
- Authenticated IPs - The IP addresses being used by any device connecting to your SmarterMail account. These can be clients on mobile or desktop clients, etc.
- Mailbox Migration - Importing email, contacts, calendars, tasks, and notes from third-party accounts

Regarding GMail and Microsoft and Email Retrieval / SMTP Accounts

Google transitioned to their "Sign in with Google" authentication method as a part of their roll-out of 2-Step Verification and as a way to ensure that any product or service you're connecting to your Google account is "secure" enough to do so. However, not every application or service can, much less wants to, integrate with Google using "Sign in with Google". As such, when using Mailbox Migration to migrate a Gmail account to SmarterMail, or when adding a Gmail account to the Email Retrieval card, you will be required to use an "app password." App passwords are 16-digit passcodes that can be used in place of your existing Gmail password that allow applications and/or devices to access your Gmail account. For the time being , Google allows the use of app passwords for connecting accounts to third-party services. However, Google's policies around integration with third parties is likely to change, becoming more rigid and restrictive.

In the case of connecting Google Drive as a Cloud Storage Connection, SmarterMail uses "Google Picker" as a way to validate your connection. You log into Google with your account, then when adding links to files, a separate Google modal opens. Here, you can select the various files you want to link to right from Google Drive itself.

For its part, Microsoft moved to OAuth 2.0 for services such as Microsoft 365, Outlook.com, and Hotmail. This is essentially the same as the authentication methods Google has introduced. It simply means that, when setting up additional accounts within SmarterMail, or migrating accounts from these services into SmarterMail, you will first need to authenticate your account by logging in to the Microsoft account being used. You will no longer have to enter your account and account password within SmarterMail (the password field is, in fact, removed), just your username. From there, you're directed to Microsoft where you're required to log in.

Email Retrieval

These days it's rare for someone to have, and use, a single email address. That's why SmarterMail's Email Retrieval feature is so great: it allows users to pull email from another account directly into the SmarterMail web interface. This means users can add their Gmail, Hotmail, Yahoo! or any other mail account to SmarterMail so that they can have all of their emails, from a number of different accounts, within a single web-based email client

In addition, a nice complement to Email Retrieval is SMTP Accounts. When used together, users can send and receive email from external accounts directly within the SmarterMail webmail client. Note: Email Retrieval simply pulls messages from the retrieval account into SmarterMail. SmarterMail does not process those emails like those sent directly to a SmarterMail mailbox. Therefore, things like spam filtering, autoresponders, virus checking, etc. are not performed by SmarterMail as it does not actually process the messages, it simply pulls them into the webmail client.

Using Email Retrieval

To establish a connection with an external email account, click New Retrieval Task on the Connectivity page of your account settings. You'll see a list of email services and providers, much like you see during a mailbox migration. Regardless of the type of account you are setting up — POP or IMAP — or which service you're connecting to, several pieces of information are required in order for SmarterMail to connect to the account and start retrieving messages. If these settings are unknown, it's a good idea to contact your IT or email administrator with the list below that corresponds to the type of connection you want. (I.e., POP or IMAP.) Note: When setting up Email Retrieval and connecting to another SmarterMail account (as opposed to any other email provider), that SmarterMail account needs to have MAPI/EWS enabled in order to pull over all relevant folders. This includes Calendars, Contacts, Tasks, and Notes, in addition to email.

Microsoft Exchange and Exchange Services Retrieval

Most email servers, and email services like Yahoo! and Gmail, allow users to use either POP or IMAP for connecting accounts. Microsoft, however, is different. They've deprecated "basic authentication" methods for connecting to Microsoft Exchange and/or Microsoft Exchange services such as Microsoft 365 (Office) and Outlook.com/Live.com. Instead, they're utilizing OAuth 2.0 for authentication to these systems. As a result, the information required for connecting Microsoft 365, Outlook.com, or Exchange accounts for email retrieval is a bit different than what's required for POP and IMAP.

In addition, there's an extra step required when using an actual Microsoft Exchange account or an account that is powered by Microsoft Exchange like Outlook.com. Microsoft requires you to actually sign in to their services using the Microsoft account you're retrieving because that's part of the OAuth 2.0 process. Therefore, once you have your retrieval set up, you'll see a new pop-up from Microsoft asking you to sign in to your account or use whatever secondary authentication method created for that Microsoft account. (E.g., Receive a code to your backup email address.)

- • Server Address - The address for the email server you want to connect to. When using Microsoft 365 or Outlook.com/Live.com, SmarterMail automatically fills in the server to be used. It's important to note that when using these services, the server address added by SmarterMail should not change — it will work for Microsoft 365, Outlook.com and Live.com addresses. However, when connecting to an on-premises (or remotely hosted) Exchange server you manage yourself, you will need to fill in this information.
- • Email Address - The full email address of the account you'll be adding. For example, my_name@outlook.com.
- • Retrieval Method - The method by which SmarterMail checks for new messages on the server, either Manual or Automatic. If you choose to manually retrieve messages, you will have to navigate to the Connectivity page, click on the retrieval task, then click Retrieve Messages Now in order to check for new messages. If you choose to automatically retrieve messages, you will not need to return to the Connectivity page, as messages would be automatically retrieved every 10 minutes.
- • Folder Transfer Method - This is how you want the folders within your account to be transferred into SmarterMail. You can have them transfer as Root Level Folders , meaning they will appear intermingled with any existing folders in your primary account, or as Subfolders . When transferring as subfolders, you will be asked to select a folder you want to import into. Therefore, it's recommended that you create a folder specifically for the folders from the account you're retrieving. For example, create a "M365" folder and then use that.
- • Require SSL - Select this option if the connection to the server must be SSL.
- • Enable content filtering - Select this option to apply your SmarterMail content filtering settings to any messages downloaded from this server.

POP Retrieval

SmarterMail's POP retrieval service will download email messages from the Inbox of another server via POP3 and deliver them to your SmarterMail mailbox. One primary difference between POP and IMAP is that a POP account will generally retrieve the messages then delete them from the originating server. While SmarterMail's POP Retrieval DOES allow you to leave messages on the server, users need to make sure they enable it. Otherwise, POP retrieval will delete the messages from the server after they are downloaded to your mailbox. The other primary difference is that IMAP allows the retrieval of ALL messages in the external mailbox, while POP will only download the contents from the Inbox.

In addition, some services (e.g., outlook.com) do not offer POP as a retrieval method. Instead, they default to IMAP or they use a different protocol.

When creating a new account for POP message retrieval, the following options are available:

• Type - Select POP.
• Server Address - The address for the email server for which you want to connect. This will most likely be the URL to the mail server. (E.g., mail.example.com).
• Port - The port used to connect to the email server. By default, the port is 110. However, some mail providers may require a separate port be used for POP retrieval.
• Username - The identifier used to authenticate with the email server. This will most likely be the full email address you want to bring into SmarterMail.
• Password - The password used to log into the mail account.
• Retrieval Method - The method by which SmarterMail checks for new messages on the server, either Manual or Automatic. If you choose to manually retrieve messages, you will have to navigate to the Connectivity page, click on the retrieval task, then click Retrieve Messages Now in order to check for new messages. If you choose to automatically retrieve messages, you will not need to return to the Connectivity page, as messages would be automatically retrieved every 10 minutes. Note: Administrators can adjust the interval used by automatic retrieval by temporarily stopping the SmarterMail service and modifying the value in the mailboxConfig.xml file. -->
• Destination Folder - The folder where messages from the external account should be downloaded.
• Enable APOP authentication - Select this option if the server requires additional login security.

• Leave messages on server - Select this option to keep your messages on the server after they are downloaded to your SmarterMail mailbox.
• Require SSL - Select this option if the connection to the server must be SSL.
• Enable spam and content filtering - Select this option to apply your SmarterMail spam and

content filtering settings to any messages downloaded from this server. If the antispam solution being used for the account you're retrieving is good, this may not be necessary. Note: After you've added your information, when you click the Save button, the connection is tested prior to actually being saved by SmarterMail. If an error occurs during the test, you will receive a notification that an error occurred and will need to correct it prior to being able to save the connection.

IMAP Retrieval

SmarterMail's IMAP retrieval service will download email messages from another server via IMAP and deliver them to your SmarterMail mailbox. One primary difference between IMAP and POP is that an IMAP account will leave the original messages on the original mail server by default. The other primary difference is that IMAP allows the retrieval of ALL messages in all folders of the external mailbox, while POP will only download the contents from the Inbox.

When creating a new account for IMAP message retrieval, the following options are available:

- Type - Select IMAP.
- Server Address - The address for the email server you want to connect to. This will most likely be the URL to the mail server. (E.g., mail.example.com).
- Port - The port used to connect to the email server. By default, the port is 143. However, some mail providers may require a separate port be used for IMAP retrieval.
- Username - The identifier used to authenticate with the email server. This will most likely be the full email address you want to bring into SmarterMail.
- Password - The password used to log into the mail account.
- Retrieval Method - The method by which SmarterMail checks for new messages on the server, either Manual or Automatic. If you choose to manually retrieve messages, you will have to navigate to the Connectivity page, click on the retrieval task, then click Retrieve Messages Now in order to check for new messages. If you choose to automatically retrieve messages, you will not need to return to the Connectivity page, as messages would be automatically retrieved every 10 minutes. Note: Administrators can adjust the interval used by automatic retrieval by temporarily stopping the SmarterMail service and modifying the value in the mailboxConfig.xml file. -->
- Folder Transfer Method - The method by which SmarterMail imports emails from the server. The advantage of creating an IMAP connection, rather than POP, is that IMAP allows existing folders to be brought into SmarterMail. Users can choose to add their external account folders as root folders or append them as subfolders on an existing SmarterMail folder.
- Requires SSL - Select this option if the connection to the server must be SSL.
- Enable spam and content filtering (Inbox only) - Select this option to apply your SmarterMail

spam and content filtering settings to any messages downloaded from this server. If the antispam solution being used for the account you're retrieving is good, this may not be necessary. Note: After you've added your information, when you click the Save button, the connection is tested prior to actually being saved by SmarterMail. If an error occurs during the test, you will receive a notification that an error occurred and will need to correct it prior to being able to save the connection.

Removing a Retrieval Task

To remove a retrieval task, click on the account from the list of retrieval tasks. Then click Delete .

SMTP Accounts

These days it's rare for someone to have, and use, a single email address. That's why SmarterMail's SMTP Accounts feature is so great: it allows users to send email from another account directly within the SmarterMail Web interface. This means users can add their Gmail, Hotmail, Yahoo! or any other mail account to SmarterMail so that they can send all of their emails, from a number of different accounts, from within a single interface.

A nice complement to SMTP Accounts is Email Retrieval. When used together, users can send and receive email from external accounts directly within SmarterMail.

Connecting an SMTP Account

To establish a connection with an external email account, click New SMTP Account . Several pieces of information are required in order for SmarterMail to connect to the account. If these settings are unknown, it's a good idea to contact your IT or email administrator with the list below.

When creating a new SMTP account, the following options are available:

    • Display Name - The name that should appear in the From field of emails sent using this account.
    • Server Address - The address for the external email server for which you want to connect. This usually takes the form of mail.example.com.
    • Server Port - The port used to connect to the email server. By default, the port is 25. However, some ISPs block port 25 by default. Therefore, it's a good idea to check with your email provider or email administrator to ensure that you're using the proper port for this account.
    • Encryption - The type of encryption required by the external email server. Many ISPs and service providers require you use SSL to send emails.
    • Email Address - The full email address that corresponds to the external email server. For example, jdoe@@example.com.
    • Enable Authentication - Select this option if SMTP authentication is required to send mail

from this email address. What that means is that, once you attempt to send a message using this account, SmarterMail will pass your credentials back to the sending server to authenticate your address and let the sending mail server know that you're authorized to send mail from that account.

• Username - The identifier used to authenticate with the external email server. In many cases, this and the Email Address will need to be identical.

• Password - The password used to authenticate with the external email server. Note: After you've added your information, when you click the Save button, the connection is tested prior to actually being saved by SmarterMail. If an error occurs during the test, you will receive a notification that an error occurred and will need to correct it prior to being able to save the connection.

Removing an SMTP Account

To remove an SMTP account, or to simply reset the connection, click on the account from the list of SMTP Accounts. Then click Delete .

Synchronized Devices

In the Synchronized Devices section, a user can review the syncing connections that are configured for their user. SmarterMail will show the type of connection being made (generally, the protocol being used) and, in most cases, the device/client and protocol, except for IMAP or POP connections as these are not listed. For example, "Outlook (MAPI)" or "WindowsMail (EAS)". SmarterMail Enterprise uses multiple data synchronization technologies to sync user data with email clients and mobile devices, including:

• MAPI is an optional add-on that syncs SmarterMail mailboxes with Microsoft Outlook for Windows and that allows Outlook users the same features and functionality that's available within Outlook when using Microsoft Exchange.

• EAS is an optional add-on that is the standard for syncing with most smartphones and tablets.

• EWS is an optional add-on that seamlessly syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients that support the protocol, including Microsoft Outlook for Mac, Apple Mail, the Outlook client for iPad and eM Client.

• CalDAV is an extension of the WebDAV protocol that syncs SmarterMail calendars with Macs, iPads, iPhones, and other devices/applications that use the technology.

• CardDAV is an extension of the WebDAV protocol that syncs SmarterMail contacts with Macs, iPads, iPhones, Thunderbird and other devices/applications that use the technology.

(For more information regarding the different synchronization methods available for SmarterMail and/or your device, please refer to Synchronizing with SmarterMail .)

Deleting a Connection

In general, users should not delete a sync connection as this may cause the device/application to stop functioning with SmarterMail. Deleting a connection is only recommended if you are no longer utilizing that device or if you are experiencing issues and want to completely resync the device's connection to SmarterMail.

When reconfiguring a device's connection, you should:

> • Remove your SmarterMail account from the device.
> • Delete the connection from the Synchronized Devices section.
> • Then add the account configuration back to the device.

Resync all Devices

There may be instances where a user who has multiple different clients set up will want to manually force all of those clients to resync. This should generally be done at the request of the domain administrator, but it can be done any time there is at least one device listed. Forcing a resync of one or more clients can help resolve issues, such as emails appearing in one client and not another.

That said, resyncing all clients can take some time to complete, especially for particularly busy/active users. Therefore, it should only be done during off hours, when possible.

When pressing the Resync all Devices button, the user is presented with a confirmation dialog warning them of the time that may be necessary to complete the action. Once acknowledged, a toast notification appears letting them know the process has begun. From there, notifications are used to let the user know when the process completes, and if there are any issues. Resyncing of clients is logged, so if an issue presents itself, the user should contact their domain administrator, who can then help further troubleshoot the issue.

Authenticated IPs

This section displays all of the authenticated logins, by public IP addresses, over the previous 3 days for your user. These IPs may be associated with email clients, webmail clients, mobile devices or any other type of connection that accesses your SmarterMail user. note: Private IPs, or ones generally reserved for internal use on a network, are excluded from this list.

Where possible, the associated protocol is listed as well, which can be used to help identify what is connecting and from where. For example, EAS connections are most likely mobile devices. The same IP address may show up multiple times if, for example, you're logged in via webmail as well as Outlook on the same computer.

Mailbox Migration

The mailbox migration tool makes moving a user from an email provider like Microsoft 365 or Yahoo!, or from another email server like MailEnable or Open X-change, to SmarterMail incredibly easy. Depending on whether the provider allows it, Mailbox Migration can import email, contacts, calendars, tasks and notes into a SmarterMail Account. Note: When migrating from another SmarterMail server, the account(s) on the source SmarterMail server need(s) to have MAPI/EWS enabled in order to pull over all relevant folders. This includes Calendars, Contacts, Tasks, and Notes, in addition to email. Otherwise, IMAP can be used to migrate just email.

Migrating a Mailbox

To import data from a third-party mail server, do the following:

- Log into SmarterMail as a user.
- Click the Settings icon.
- Click on Connectivity in the navigation pane. The Connectivity page allows you to add cloud file storage providers that you can use to link files from in your messages, you can add SMTP accounts, you can view your connected devices...AND you can migrate messages from third party services or other mail servers into SmarterMail.
- On the Mailbox Migration card, click the Migrate button.
- The Mailbox Migration modal appears. Here, you will select which service or mail server you want to migrate data from. Find your appropriate starting point and click on its icon.
- The information required will vary based on the service or server you're migrating from, and in some cases SmarterMail will know information, such as the Server Address you're migrating from. For example, when migrating from Office.com, you'll simply need your email address and password: SmarterMail fills in the Server Address for you. However, if migrating from another email server, such as MailEnable, you'll need more detailed information. The most information you'll need is:

- Items to Import - You'll be able to select what you want to migrate over to SmarterMail: Email, Contacts, Calendars, Tasks or Notes — or all of them. That said, in some cases you will not be able to choose — the choice is made for you by the provider. Therefore, this may not always be available, especially if migrating from another mail server like Zimbra or MailEnable.
- Server Address - This will be the URL you use to log in to the mail server, or the mail server address you use when connecting to an email client. For example, mail.your-domain.com. Whenever possible, SmarterMail pre-fills in the server address to make it easier for you to start the migration.
- Type - This will either be POP or IMAP. The difference is that POP will pull ONLY messages

from the Inbox whereas IMAP may be able to pull additional items such as calendars.

• Port - The port that's associated with the Type you've selected.

• Email Address - This is the full email address you're migrating over. For example, jdoe@@office.com

• Password - This is the password you use to log into the account you're migrating over. Note: Some services require an extra layer of authentication. For these services, the Password field is hidden. Instead, users will need to log in to their accounts at these services directly, thereby offering a more robust and secure form of account authentication.

• Require SSL - This is enabled by default, requiring a secured login.

• Delete existing SmarterMail mailbox items - Enabling this will overwrite any existing SmarterMail data with the data that's being migrated over. That includes all contacts, calendar entries, etc. If this is NOT enabled, the migrated data will be "merged" into any existing data and nothing is overwritten.

• Once you've filled out the necessary information, and selected the items you want to migrate over, the mailbox migration will start. You can track its progress as the data is imported. So now, it's a waiting game. The total time necessary to migrate your data depends on how much data there is, your internet connection and other factors. Note: It may take some time for your mailbox data to import. You can continue using SmarterMail during this time as the migration process happens in the background. In addition, the type of items available for migration are purely dependent upon the service you're migrating from. SmarterMail cannot migrate any item that is not allowed by the service provider.

Our knowledge base offers a couple of different articles that walk through the migration process. Please see:

• Migrate an Account From Another Service into SmarterMail
• Migrate a Mailbox From Microsoft 365 (Office) to SmarterMail

A few quick notes regarding Mailbox Migration:

• The mailbox migration tool will only transfer email, contacts, calendars, tasks, and notes (if supported) from a single third-party mailbox to your SmarterMail mailbox. System administrators can use mail server conversion tools to migrate multiple mailboxes or entire domains from mail server applications like MailEnable, Merak, MailMax, or Imail quickly and easily. System administrators can also use Web services to run migrations for multiple accounts.

• SmarterMail is typically able to keep date and time stamps when importing from other email servers as long as they follow the standard time and date format in the email header. In addition, it may be necessary to make changes to your account, especially if you're importing data from

services like Microsoft 365 (Office) or Yahoo! to allow for mis-named "insecure applications". So, be sure to make any necessary security changes to your account BEFORE you start the migration process.

• There may be a discrepancy in the number of items in the Deleted Items folder after a migration. This is because some email providers, notably those made by Microsoft, don't restrict the type of item that gets stored in Deleted Items. For example, in your Office.com account there may be contacts, calendar appointments, notes, and tasks in Deleted Items. SmarterMail only allows mail messages in Deleted Items, we do not import other item types during a migration.

• Finally, if there are issues with a migration, SmarterMail logs all migration activity. Therefore, a system administrator can check the Mailbox Importing logs for a user to see what happened, and find a resolution.

Content Filtering

Content filtering is a great way for system administrators, domain administrators and/or users to perform actions on incoming emails that meet specific criteria. For example, it's possible to use content filters to delete messages with certain attachments (e.g., attachments with a .exe extension), forward messages from a specific email address to another account, move messages to a certain folder or even alter the subject of a message by appending something to it prior to delivery. While content filters are most commonly used to organize email by moving messages to specific folders, they're extremely flexible and allow you to filter messages the way you want to.

Content Filtering is available to users and domain administrators in the Settings and/or Domain Settings areas. System administrators have a Content Filtering tab available to them for each domain that's managed on the SmarterMail server. In both the Settings and Domain Settings areas, there is a Content Filtering option in the navigation menu that's used to see any existing filters as well as to manage filters. That being said, the filters created are only viewable/editable by the role that created them. That means the domain content filters are only available to domain administrators and users see their own filters. However, any filter created for a domain by a system administrator is available to both the system administrator and the domain administrator.

Once the Content Filtering section is accessed, any existing filters will be listed. Content filters run in order, from top to bottom. In addition, content filters run from top-down: that means that content filters created by system and/or domain administrators run first, then filters created by users. That means that if a message could be managed by more than one, it will be handled by the FIRST content filter encountered. So, if you're seeing weird or unexpected behavior for messages, you may want to re-organize the order of your filters. You do this by moving them by clicking the Up and Down arrows next to the content filter names, moving them up and down in the "order of operations." You may also

want to contact your domain administrator to see if they have any content filters created that could be impacting message delivery. Note: Some content filtering actions, such as a Forward action, do not work in conjunction with Plus Addressing as content filters are run BEFORE any plus addressing commands. Using both could lead to duplicate messages or other unwanted/unnecessary behavior. In addition, automatic forwarding is incompatible with certain message types, such as autoresponders and Delivery Status Notifications (DSN). This is to avoid the potential for feedback loops that can cause issues such as the spool filling up.

To delete a content filter, simply select it from the list and click the Delete button.

Create/Edit Content Filters

When adding a content filter, the following cards will be available, each with options pertaining to the conditions you want to use for the rules, and the actions that are taken based on the conditions you set:

General

- Name - The friendly name chosen to describe the rule.
- Match Type - Because multiple conditions can be configured per content filter, SmarterMail provides the option to require ALL conditions to be met or ANY of the conditions to be met in order for the rule's action to be triggered. Select the appropriate option from this list.
- Enable wildcards in search strings (* and ?) - Wildcards can be used to replace a specific word, phrase or character, where a question mark (?) represents a single character and an asterisk (*) represents any text. For example, if you wanted to block sales01@@domain.com, sales02@@domain.com and sales03@@domain.com, you could enter sales??@@domain.com . If you wanted to block all sales addresses, you could enter sales* instead.

Conditions

Click on New Condition to specify the criteria that triggers the rule's action(s). For each condition selected, you will be able to add specifications and enter any necessary details, as required. For example, if you choose to filter on 'From Address', you can enter one or multiple email addresses. If you choose to filter on 'Contains specific words or phrases', you can enter the specific text and choose to look for that text in an email's subject, message body, header, etc.

On many conditions, you also have the ability to reverse the logic of the criteria item by changing the Comparison selection. For example, imagine you only want to accept email from specific domains. You would choose the 'From specific domains' condition and set the Comparison field to 'Does Not Match". Any messages sent from domains that do not match what you've entered in the text box can be deleted. Note: If you select a condition that requires a value to be entered, and the field is left blank, SmarterMail will ignore this rule.

The following conditions are available, separated by Condition Type:

From Address

This condition allows you to select whether you want to run the filter against specific addresses or domains, or trusted senders. Then, you set the comparison type: whether the field matches or doesn't match the condition type. Then, you enter in the addresses or domains you want to use for the filter. The fields to use include:

- From specific addresses
- From specific domains
- From trusted senders

Contains Specific Words or Phrases

This condition allows you to look in various areas for words or phrases, then take action when those words or phrases are found. You can set the comparison type, whether the words/phrases are found or not, and then the words or phrases you want to use for the filter. You can further refine a phrase search by enclosing the phrase in quotation marks. (The same can be done to individual words.) The fields to use include:

- Subject
- Body
- Subject or Body
- From Address
- To Address
- Email header
- Anywhere in message

To Address

This condition allows you to look in the To: or Cc: fields for specific addresses or domains. You can set the comparison type, whether the address or domain are included in the selected field, then the addresses or domains you want to use for the filter. The fields to use include:

- To specific addresses
- To specific domains
- Only to me
- My address in to field
- My address not in to field
- My address in to or cc field

Attachments

This condition allows you to filter emails based on whether or not messages have attachments, or even by specific filename, extension type, or file size. The fields to use include:

- Has any attachment
- Specific filenames
- Specific extensions
- Over specific size

Other

This condition allows you to filter based on a number of different criteria, including flag type, message size, spam probability, etc. The fields to use include:

- Flagged as high priority
- Flagged as normal priority
- Flagged as low priority
- Message automated (no return address)
- Sender authenticated
- Message over size
- Message under size
- Received in date range
- Sent through a specific server (by IP address)
- Spam probability

Actions

Click on New Action to specify what should occur when an email triggers the content filter condition(s). note: If you select an action that requires a value to be entered, and the field is left blank, SmarterMail will ignore this rule.

The following actions are available:

- Delete message - Deletes the message so that it will never arrive at your Inbox. Note: Messages deleted through content filtering cannot be recovered.
- Bounce message - Sends a message back to the sender of the email saying that the message was bounced, and not delivered. Note: If the system administrator has disabled bouncing, the sender is never notified and the message is simply deleted.
- Move message - Delivers the incoming message to the folder you choose from the dropdown list. note: If you later delete that folder and leave the content filter active, the filter will automatically create the folder when the action is triggered.

• Add Header - Adds an email header within the incoming message, which can be useful when performing additional filtering through Outlook or other email clients. Headers should be formatted like "X-someheadername: value"

• Add Text to Subject - Appends a prefix to the subject line of the email. This is useful for categorizing emails as the subject line will be altered to include the text you specify in the text box.

• Forward message - Forwards a copy of the message to another email address and leaves you a copy of the message as well.

• Mark as read - Automatically marks the messages as read, which means it will not show up in your inbox, or any other folder, as unread.

• Set Priority - Automatically elevates the priority of a message. For example, if you create a content filter that flags a message from a VIP, you may want to set the priority of the message to High as well to denote its importance.

• Flag message - Automatically flags the message for follow-up. This makes it easy to find messages that have been acted upon by your content filter.

Manually Running Filters

Users can manually trigger one or more of their content filters to run against a specified email folder. The ability to run content filters on-demand is a convenient way to clean up the mailbox, as actions can be performed on EXISTING emails rather than incoming email only.

It's possible to run a content filter on a specific folder simply by selecting the folder name and the selecting Run Content Filter from the Actions menu icon that appears at the bottom of the SmarterMail interface. (It's to the right of the folders icon.) Once selected, a modal opens and you are able to select the content filter to run from the dropdown, then clicking OK . The filtering process may take some time to complete, but you may continue to work while the process runs in the background. When the filtering process has completed, an Action Succeeded toast notification will appear within the Email section.

<u>Important notes regarding on-demand filters:</u>

• The 'Sent through specific server (by IP address)' and 'Sender Authenticated' conditions as well as the 'Bounce message' action cannot be used when manually running a content filter. If a filter contains one of the restricted actions or conditions as its only action or condition, the filter should be triggered manually. If a filter contains one of the restricted actions or conditions along with other actions or conditions, please note that the restricted action or condition will be omitted from the filter process.

• The 'Delete message' action will immediately purge the email from the system. Without Message Archiving enabled, these messages may not be recoverable.

• The 'Prefix Subject' action must re-write the message. It will attempt to timestamp the new message with the date from the message header. However, if the date cannot be parsed from the message header, the re-written message will show the current time.

• The 'Trusted Senders' condition will look for Current trusted senders. It cannot look for messages from trusted senders that were configured at the time the message was delivered.

• Running content filters on-demand executes the filters in the order they appear. However, the on-demand process does not loop through messages multiple times to perform the filter actions. Instead, it will gather all of the actions it could run on the message first and then runs them in the order they would have been found.

• When there are multiple actions for one filter, the actions that don't require a re-write of the message will be done first. For example, a message will be marked as read before it is moved to another folder.

Events

The Event system in SmarterMail is an incredibly powerful and flexible tool that allows users to automatically perform actions based on specific criteria and remain up-to-date with what is going on with the SmarterMail server. SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to users that need the information. For example, users can automatically add an additional recipient on messages they send or receive notifications when a task is due or their user disk space has met a certain threshold.

Access your events page will display a full list of the events created for a user. If no events have been created, this page may be blank. Any existing events can be edited as needed, simply by clicking on them. Events can also be deleted from this page.

When creating events, the following cards will be available and each card will contain options that pertain to its purpose:

General

• Event Name - The friendly name of the event.

• Event Status - New events default to a status of Enabled. However, to temporarily stop an event from triggering, you can change the status to Disabled.

• Event Category - The feature to which the event pertains: Email, User or Collaboration.

• Event Type - The occurence that triggers the event. Each category has several specific event types that can trigger the action.

• User - The user that the event applies to.

Event Categories and Types

Below is a list of the Event Categories, and the Event Types that are available for each, for User Events:

Email

- Message Received
- Message Sent

User

- User Disk Space Used

Collaboration

- Calendar Reminder Occurred
- Task Reminder Occurred

Conditions

Each event type has its own corresponding conditions. The global conditions that are seen across all event types are listed below. Multiple Conditions can be used when creating a given Event. Conditions are checked in order, from top to bottom, before the Action(s) is/are performed.

- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.

Below are the Event Conditions that are available and their respective Conditions:

Email

- From Address - The email address from which the email message was sent.
- From Domain - The domain from which the email message was sent.
- To Address - The email address the email message is being sent to.
- To Domain - The domain to which the email message is being sent.
- Subject - The words that will trigger the event if found within the subject of the message.
- Size (KB) - The message size in KB that will trigger the event.
- Intra Domain - Select this option to trigger the event when an email is sent/received from within the domain.
- Spam Level - The spam level of the message -- usually Low, Medium or High.
- Messages an Hour - The total number of email sent in an hour.

User

- Domain - The domain on which the event occurs.
- Full Name - The full name of the person that will trigger the event.
- Mailbox Usage (%) - The percentage of mailbox space utilization that will trigger the event.
- Mailbox Usage (MB) - The mailbox space utilization in MB that will trigger the event.
- Username - The username that wil trigger the event.

Collaboration

- Subject - The words that will trigger the event if found within the appointment or task subject.
- Location - The appointment location that will trigger the event.
- Description - The words that will trigger the event if found within the appointment or task description.
- Email Address - The email address that will trigger the event.
- Priority - The Priority level assigned to a Task.
- Percent Complete - The percentage complete the Task is.
- Status - The Task's status.

Actions

Each event type has its own corresponding actions. The global actions that are seen across all event types are listed below. Multiple Actions can be assigned to a given Event. Actions are performed in order, from top to bottom.

- Show a notification - This option will display a notification to the Notifications window. It can also send a popup browser notification.
- Send an email - This option will send an email to the specified address.
- Add Recipient - Adds a recipient to the message. (For Email Event Category Only)

Mailing Lists

As a SmarterMail User you may be tasked with becoming a "List Moderator". What that means is that you're the person who manages a mailing list for your organization. Therefore, it's your job to get the setup the mailing list, manage subscribers, manage who can post to the list and much more. If you do become a List Moderator, the Mailing Lists tab in your Settings is where you go to work on those lists.

When you access your mailing lists page, if you are the moderator of a list it will be displayed on this page with following:

- List Name - The name of the mailing list.
- List Moderator - The List Moderator's Display Name. As you're managing the lists, this should

be you.

- Subscribers - The total number of subscribers for the mailing list.
- Digest Subscribers - The total number of digest subscribers for the mailing list.

If a mailing list is ever corrupted or otherwise broken, it will appear in the list with a red warning icon next to its name. Clicking on the list will spawn a modal window notifying the list administrator of the issue, and give them the ability to remove the mailing list from the page. Removing the list allows the list administrator to re-use the List Name and, therefore, recreate the list or use the same list name for a different subscriber base.

If the List Administrator does not want to remove the list, it IS possible it can be recovered: A system administrator would need to get a copy of mailinglist_data.json from the domain's Archived Data and either replace the existing file, or manually merge it with the existing file.

Managing Mailing Lists

As a List Moderator you have full control over the various settings for the list, or lists, you manage. To see these settings, simply click on the list you want to manager and it's options will open.

For information on the tabs listed and the options available, see the information below:

- Options - Configure the mailing list options and permissions
- Subscribers and Digest Subscribers - Add subscribers who will receive the standard mailing list postings or digest emails.
- Allowed Posters - Whitelist email addresses or domains who can post to the mailing list
- Banned Posters - Prevent specific email addresses or domains from posting to the mailing list
- Messages - Configure the header and footer for postings as well as the replies sent to listserv commands
- Custom Fields - Customize list postings with subscriber custom fields

Scheduling

This feature is only available in SmarterMail Enterprise.

Sending calendar invitations to individuals, or groups of people, is a perfectly fine way of connecting with others. However, in some cases it can be a bit too time-consuming. For example, if you run a consulting business and want to provide some type of free evaluation or initial consultation to attract new business. Sending out invites to each person who contacts you may work, but wouldn't it be better if these people could simply schedule a time on their own — a time that fits their schedule as well as your own?

Well, that's where SmarterMail Scheduling comes in. Using Scheduling gives you the ability to set up different meeting types, set your availability, check various calendars to ensure there's no conflicts, and much more. You can even provide an external URL that people can use to schedule appointment times, or even embed scheduling details into a custom page to ensure branding guidelines are followed.

Regardless of how the Scheduling page is used, once someone actually sets up an appointment, meeting invitations are automatically sent to BOTH the page visitor and the SmarterMail user. For the SmarterMail user, the appointment will be automatically accepted and added to their calendar, with the complete appointment details.

When accessing Scheduling , the following cards will be available:

Settings

The Settings card allows you to set up basic guidelines for using the Scheduling feature. These guidelines include:

- Enable Scheduling - This toggle actually enables the scheduling feature. When toggled off, all cards are hidden from view. When enabled, all of the cards associated with the various parts of the scheduling feature are displayed.
- Mark appointments as private - Enabling this will block out time on a calendar, but not display the details of the blocked time. This works similarly to marking appointments as private when sending out meeting/appointment invitations for a calendar.
- Calendar to use for appointments - This will be the calendar to use for the appointment types that are scheduled. The dropdown will display any default, custom, or shared calendars for the user.
- Minutes between appointments - This is the default time between scheduled appointments. For example, when set to 30 minutes (the default), if a person schedules a 1-hour appointment at 9:00 a.m., the next available time displayed for an appointment would be 10:30 a.m. (1 hour for the appointment, plus the 30 minutes between appointments.)
- Lead time for new appointments - This is the default between the current time and when an appointment can be scheduled. For example, if it's 9:00 a.m. and the lead time is set to 30 minutes, the potential first available time for a new appointment to be scheduled would be 9:30 a.m. The idea behind this setting is that it's impractical for someone to schedule an appointment that occurs immediately as it doesn't offer the user any lead time to prepare, etc.
- Enable Schedule password - When enabled, this password protects the public Scheduling page for the user. Therefore, only people with the password will be able to schedule an appointment with the user.

Appointment Types

Appointment Types allow a user to set the type of appointment someone will schedule with them. For example, an interview, a demonstration, and initial consultation, a training session, etc. These types, then, appear on the actual scheduling page a visitor sees when they set up their appointment. Each type will appear in a dropdown, and the visitor selects the type of appointment they want to set up.

To add an Appointment Type, do the following:

- In SmarterMail, click the More button and then choose Settings from the dropdown. Once you're in Settings, click on Scheduling .
- In Scheduling , find the Appointment Types card, then click the New Appointment Type button and a new modal opens.
- In that modal, set the Name for the appointment type. For example, "Product Training".
- Next, set the Duration of the appointment. The duration can be in 15 minute increments up to an hour, then hourly up to 12 hours.
- Then, it's possible to set how far in advance someone can schedule an appointment with you, called the Booking Horizon Limit . For example, if you don't want anyone to be able to schedule an appointment further than 2 weeks from the current day, set the Booking Horizon Limit to 2 weeks.
- If the appointment will be via a SmarterMail Online Meeting, toggle Online Meeting . When an appointment is made by a visitor, a SmarterMail Online Meeting is automatically created for that specific appointment, and the URL is included in the meeting invites sent to both the organizer and visitor.
- If any Location OTHER than a SmarterMail Online Meeting is going to be used, enter it. Generally, this will be a phone call, a meeting room, etc. However, should a user want to use the same Online Meeting URL from SmarterMail, or any other online meeting URL (e.g., Microsoft Teams), it can be entered.
- Next, you can set a Description for the meeting that's displayed on the Scheduling page. This can be any text you want to use to detail the meeting, such as its purpose or any expectations you have for participants.
- Lastly, you can set the Calendar Description . This is the information that appears in the calendar appointment that is sent to the person making the appointment, and will appear as the description of the appointment for the SmarterMail user as well.

Once all of the information has been entered, be sure to save the settings. Then, be sure to save the page.

Calendars to Check for Conflicts

People use many calendars for many different things. As such, when offering the public the ability to schedule an appointment type it's important to know when a SmarterMail user is available so as to not double book appointments. Therefore, having the ability to check more than one calendar to ensure there aren't any conflicts is important.

By default, the Calendar to use for appointments that's selected on the Settings card will always be used when checking for conflicts. However, there may be other calendars a SmarterMail user will want checked, like a Training or Meetings calendar. Any calendar that the SmarterMail user has available to them will be displayed, including shared calendars, domain calendars, or even web calendars.

If another calendar needs to be added, repeat the steps above until all have been added. When finished, be sure to save the page.

Availability

Availability is just that: when a SmarterMail user wants to make themselves available for public scheduling. For example, if they only want people to be able to set appointments in the afternoon, they can set their Availability to just those afternoon hours. If they want to be available for a few hours a day, or a few hours every coouple of days, they can do that as well.

The days and times set in Availability are what will appear on their public page when a visitor starts the scheduling process. To set Availability, do the following:

- • First, toggle the days to be available.
- • Next, set the times to be available on those particular days.
- • Once all of the changes have been made, be sure to save the page.

Custom Fields

There may be some types of data a SmarterMail user wants to set prior to an appointment being made. For example, a part number, a product name, a ticket number, etc. In these cases, Custom Fields can be created. These fields can then be filled out and included in the meeting invitation that's created once a visitor schedules something. By default, a visitor's email address and their full name will always be required when scheduling an appointment. This is why they're displayed and uneditable. A total of 5 additional custom fields can be added, not counting Email Address and Full Name.

To add a Custom Field, do the following:

- • Type the name of the Custom Filed on the line.
- • If the Custom Field is required, toggle that on the same line.

• Once a custom field is added, a new line appears automatically. If more fields are desired, they can be added.

• Once all of the changes have been made, be sure to save the page.

Page Details

Page details consist of the following:

Page URL

This is the URL of the SmarterMail user's public-facing scheduling page. It can be used in a signature, as an added line at the bottom of emails, as a link on a person's contact page, etc. It's the page visitors will go to in order to schedule an Appointment Type.

Embed Code

The Embed Code allows a SmarterMail user to embed their scheduling page into a custom template. Creating a custom page allows users to offer corporate branding in terms of colors, logos, etc. so that a visitor feels more comfortable setting up an Appointment Type.

Sharing

The Sharing page in a user's settings provides the user with information about any and all shares attached to, or provided by, the user. The page is separated into individual tabs:

• Shared With Me

• Shared With Others

• Delegation

Another way to share items is using the Sharing area. You access this are by going to Settings > Sharing. You'll notice this area separated into 2 different tabs: Shared with Me and Shared with Others.

Shared With Me

This tab displays all the items that have been shared with your user. This includes email folders and sub-folders, contact lists, tasks and notes. This tab displays the following:

• Shared By - The user sharing the item with you. This can be an individual user, or, in the case of shared resources such as Conference Rooms or Equipment, the domain itself.

• Folder - The name of the folder that's been shared. This is, essentially, the name of the shared item. (E.g., Conference Room A)

• Type - The type of shared item: calendar, email folder, notes, etc.

• Attached - This indicates whether the item is actually attached to your user. If it's not attached,

it can't be accessed.

• Subfolders - This indicates whether the subfolders within the parent are also shared with you.

• Permissions - The permission level you have for the shared item. (E.g., Read-Only)

Clicking on an item in the Shared with Me list opens the details of the item. You can see the name, who shared it and the permission for the item. In some cases, there are also customization options and additional information that may be available. For example, on calendars you can adjust the color of the calendar items to customize how they appear. Finally, you can attach or detach the share from within the modal window. You can also attach or detach items simply by checking the box next to the item, then clicking the appropriate button at the top of the content window.

You'll also notice "Attach" and "Detach" buttons. While shares are automatic, you may have need to remove, or Detach, a shared item, for one reason or another. For example, if your CEO's calendar was shared with you, but you need to show your calendar to someone — a client, possibly — you may want to temporarily detach the CEO's calendar from yours so no sensitive information is displayed. In this case, you'd select the CEO's calendar and click the Detach button. Then, once the prospective client leaves, you'll want to select that calendar and click the Attach button. The key here is that you've removed the share, but the CEO hasn't. Therefore, the calendar is still shared with you, it's just been temporarily detached.

Shared With Others

This tab displays the items you have shared with others within your organization. It offers similar information as the Shared with Me tab, including:

• Folder - The name of the "folder" that's been shared. This is, essentially, the name of the shared item. (E.g., Conference Room A)

• Type - The type of shared item: calendar, email folder, notes, etc.

• Subfolders - This indicates whether the subfolders within the parent are also being shared.

• Permissions - The number of permission levels associated to the share. This is an indication of how many users and/or user groups the item has been shared with. For example, if an email folder is shared with 3 individual users, 3 would be displayed for the item as there are 3 separate shares of it.

Clicking on an item opens its options. This allows you to modify the share by adding in additional users, changing permissions for existing users and/or user groups, etc.

Creating a New Share

It's also possible to create a new shared item from the Shared With Others tab. Simply click the New button at the top of the content pane. This opens a new modal and offers the following options:

- Folder - The type of share you want to create, based on the "folder", or item, you want to share. All of the items you have available to be shared are listed in this dropdown: all calendars, all email folders, all address books, all notes and all tasks.
- Users - This area allows you to share the item with one or more user, and each user you add to the share can have their own permission level. These are:

- None - This permission acts as a "negater" and is, therefore, only available for users. For example, let's say you have a user group set up for your Marketing Department. However, you don't want to share Notes with Henry because he ate your piece of cherry pie last week. You add Full Control access to the Marketing Department user group, you'd add Henry's username under Users and set his access to "None". That way, you're sharing Notes with everyone in Marketing EXCEPT Henry as you've negated his permission.
- Availability - Used exclusively for calendars, this permission means that the user with this permission can see whether a person is available for scheduling purposes, but it doesn't allow for the viewing of a calendar or its appointments/events.
- Read-only - This means that the user can only view the items in the share (calendar entries, contact lists, etc.), they have no control over editing entries, adding entries, etc. A read-only share would be good, say, for a colleague who needs access to a contact list, but who doesn't need to manage those contacts in any way.
- Manage - This access allows others to add, edit and/or delete any items within the share. (But, importantly, NOT the share itself.)
- Owner - This access allows others to rename and/or delete the specific folder that's being shared. Basically, they use whatever is being shared just as if it were their own.
- User Groups - This area allows you to share the item with groups of users that have been set up previously. When sharing with a User Group, the same permission levels are available EXCEPT for None as that is a user-only permission.

As you can see, the process for sharing contacts, calendars, tasks and even email folders is essentially the same and relatively simple: you select the item you want to share, add the users and/or user groups you want to share to, and set the permissions for each. Once you've saved your settings, the people you've shared with will have those items automatically mapped to their users.

Delegation

One of the features of Microsoft Outlook (and a few other clients, such as eM Client) is the ability to set up "Delegation". Delegation is the process of allowing another user on your domain to access your user and its associated items (i.e., Calendar, Notes, etc.) and act "on behalf of" you, based on the permission level you set for them.

The benefit of this is that someone — an associate, an executive assistant, etc. — can help manage your schedule, reply to inquiries for you, manage tasks for you, etc. For especially busy individuals, having another person help manage your workload can be extremely beneficial. Delegation allows this. In addition, when actions are taken "on behalf of" someone — for example, sending a meeting invitation — that is noted on the item, even when viewed in the webmail client.

The process of delegation is handled within the client itself, outside of SmarterMail. The Delegation tab simply shows you whom you've delegated access to and the permission level granted to each user. This tab also allows you to remove a delegate.

Signatures

An email signature is a block of text automatically appended at the bottom of an email message. Signatures may contain the sender's name, address, phone number, disclaimer, or other contact information. In addition, SmarterMail allows users to create HTML formatted signatures that can include stylized text, links, images, etc. For example, a signature can contain a company logo and tagline, an image that links to a personal or business social media account, or even links to other properties, like a company's help desk or management interface.

There are a couple of different pieces to using custom signatures:

- • Creating the actual signature, and
- • "Mapping" that signature to the account, or accounts, that should use it.

When accessing Signatures , the following settings will be available:

Signatures

To create a new signature, click the New Signature button. Then enter a friendly name and the content that should be appended to each message. Using the Custom Variables button, you can add variables that will pull in details such as the current date, your display name, website, etc.

Mapped Field

Use this card to assign a signature to your mailbox and any SMTP accounts, email aliases or domain aliases that have been configured for your account. Note: Domain administrators can enforce signatures on a domain-wide basis for user accounts, domain aliases and email aliases. In such cases, you may not be able to map a signature to these addresses.

If multiple signatures are available, you can manually change the signature used by selecting a new one from the Signature dropdown in the webmail compose window.

A Practical Example: Adding an Image

How to add an image to a signature is, believe it or not, one of the most common questions we get from users. It's actually a pretty easy thing to do, and there are a few different ways to do it:

- Use the Add Image button in the toolbar — By far the simplest way is to use the Insert Image button in the editor's toolbar. Simply create your signature, put the cursor where you want the image, then use the button. You can then format the image to whatever size you need.

- Add an image to your Profile — Do this by going into your Profile, and clicking on the image box next to your display name. You can upload an image — a logo, a headshot, etc. — and then use that image as part of your signature using the #ContactPicture# variable.

- Edit the HTML to insert an image — The HTML editor gives you the ability to edit the HTML code that's generated when you create a signature. You do this by first clicking the + sign to expand all of the HTML editor tools, then clicking on the "View Code" button, which is a sheet of paper with these symbols on it: <>. Once you see the HTML for your image, you simply edit it to add an <img src=""> that points to the location of the image (e.g., https://www.smartertools.com/images/email/temp_2010/twitter_icon.png). The image can be hosted on your website or via a third-party image hosting service such as Imgur.

- Use a third-party service — This is a bit of a different approach, but there are services out there that allow you to create very intricate and dynamic email signatures. These signatures, then, can be added using the HTML editor or even added as signatures in email clients. There is some debate about the efficiency, much less the necessity, of doing this, but the services are out there and they are an option for you.

Regardless of how you choose to do it, adding an image to your signature is not only easy, it adds a bit more personalization to your messages.

Spam Filtering

SmarterMail includes a variety of antispam measures that will help keep a user's inbox free of unwanted mail. In the Spam Filtering section, users can review/configure the spam filtering options and trusted senders for their account.

In most cases, a system or domain administrator has already configured the filtering options for spam messages on your domain. However, if they allow it, you can override those settings to select your own options for filtering out potentially unwanted email. Note: Wildcards are not supported for Blocked or Trusted senders.

Options

> • Override spam settings for this account - Enable this setting to customize the way spam is handled and to override the settings created by the domain administrator. If this option is disabled, the domain's default spam filtering policy will be displayed and cannot be edited.

When you override the spam options set by your administrator, you can choose the actions that are taken when email comes in that has a low, medium, or high probability of being spam. For each spam level, choose the action you wish to have taken. If you choose to add text to the subject line of messages, type the text in the box below the action drop down.

Trusted Senders

Users can add specific email addresses (such as jsmith@@example.com) or domains (such as example.com) that will be exempted from general spam filtering. This lets the system know that these messages come from a trusted source and can prevent mail from friends, business associates, and/or mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's Contacts list is considered a trusted sender and bypasses spam filtering. Adding domains and/or email addresses also impacts the "Verification Score" of a sender — the shield that is displayed alongside a sender's address when viewing messages in webmail.

However, if the system administrator has enabled SPF, DKIM, and/or DMARC, (all of which are strongly recommended), SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses, and IP bypasses. This "trust but verify" approach is important because anyone can write any return path that they want when sending a message. Therefore, this extra layer of protection helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender. If an SPF, DKIM, or DMARC check fails on an incoming message, the "trusted sender" is no longer trusted by SmarterMail, and the weights of all enabled spam checks will be applied to that message.

If the trusted sender status of an email was bypassed due to a failed SPF, DKIM, or DMARC check, the TotalSpamWeight line in the email header will specify the check(s) that failed, and why. Additional information about SPF, DKIM, and DMARC status can also be found in the header.

The Trusted Senders area has three editable areas. Users simply click the pencil icon to add the following:

• Trusted Domains - Full domain names (e.g., example.com) to add as "Trusted".

• Trusted Email Addresses - Full email addresses (e.g., jsmith@@example.com) to as as "Trusted".

• Bypass Spam Filtering for Unverfied Senders - This will only be displayed if the domain administrator has enabled the setting. Full email addresses the user wants to exempt from ALL spam checks, included SPF, DKIM, and DMARC checks.

When entering trusted senders or domains, enter only one item per line break.

Blocked Senders

Users can add specific accounts to their Blocked Senders list. For example, if you receive a message from dan@@im-a-spammer.com, you can left-click on the email address in the message view and select "Block Sender" from the context menu. When you do this, that message, and any future message from that specific sender, will have whatever Action is set on the Blocked Senders card applied. This allows users to have a bit more granular control over senders that escape whatever spam filtering the system administrator has set up. Note: Any Action set on the Blocked Senders card are applied just for the user who sets them — these Actions are not domain-wide or system-wide, they are only applied for the specific user who creates them.

As for the Blocked Sender Actions themselves, they include:

• None - Nothing happens to the messages from Blocked Senders.

• Move To Junk Email Folder - Messages are moved to the Junk folder, then handled however items in that folder are handled (e.g., auto-clean rules).

• Move To Deleted Items Folder - Messages are moved to the Deleted Items folder, then handled by whatever rules apply for that folder (e.g., auto-clean rules).

• Delete - The messages are flat out deleted and, therefore, unrecoverable.

Any address that has been marked for blocking will appear in the Blocked Senders list. Clicking the pencil icon allows users to review and possibly edit the list of senders they have blocked. Users can also manually enter addresses rather than simply using the context menu from their message view.

Domain Settings

Accounts

Adding New Users

Whether starting with a brand new domain, or managing a domain that's been around for a while, one of the duties of a domain administrator is adding in new users.

Just a few pieces of information are needed in order to add a User. Once this information is provided, domain administrators can then adjust any configuration settings for the User or they can simply rely on the User Defaults that have been set up.

Adding Users

When adding a new user, the following initial options will be available:

• Username - The identifier the user uses to login to SmarterMail. This is the portion of the email address that comes before the domain name. For example, the "jdoe" part of jdoe@@example.com.

• Authentication Mode - The authentication method used to login to SmarterMail. By default, SmarterMail will use its included username/password authentication. However, SmarterMail can also be integrated with customers using Microsoft Windows Active Directory for their corporate logins. For information on Active Directory integration, visit the SmarterTools Knowledge Base .

• Active Directory Username - If Active Directory is selected for the Authentication Mode, this field will appear. Enter the Active Directory username to authenticate against for Active Directory authentication.

• Domain - If Active Directory is selected for the Authentication Mode, this field will appear. Enter the Domain to authenticate against for Active Directory authentication.

• Password - If SmarterMail is selected for the Authentication mode, this field will appear. Enter the password this user will use to log into their account.

• Confirm Password - If SmarterMail is selected for the Authentication mode, this field will appear. Confirm the password this user will use to log into their account.

• Force password change at next login - Enable this setting to require the user to set a new password the first time they log in to the SmarterMail web interface.

After the initial creation of a new user, additional options can be edited. For those, see Managing Users .

Users

This settings page is only available to domain administrators.

The Users section is where a domain administrator can manage the user accounts on their domain. This document explains the actions that can be taken on user accounts, including the ability to import users, improve the search functionality for a user by reindexing their account, enabling or disabling the MAPI/EWS and/or EAS synchronization add-ons, and more.

More information is available for adding new users as well as Managing Users .

When initially going to the accounts are of a domain, the Users tab will load by default. Here, you'll see a list of users already set up for the domain. You can also edit users, add new users, delete users, and much more on this tab.

When viewing the Users tab, the following information is listed:

• Account - The username, or name that appears to the left of the "@@" symbol in the email address.
• Name - The Display Name set for the User.
• Type - The "Role" of the User: User, Domain Admin or Primary Admin.
• Enabled - Whether the User is allowed to send/receive email (Enabled) or not.
• Last Login - The last date and time the User logged in to SmarterMail and the protocol used to log in. Note: It is possible that when an Account uses webmail exclusively and SmarterMail's Chat is enabled for the account, that their Last Login shows (XMPP) as the protocol. This is becuase XMPP is the last protocol to connect once a user logs in to webmail. If Chat is disabled, the protocol listed will be (Webmail) as XMPP is not used.
• Disk Usage - The total amount of disk space being used versus their limit. Mousing over this indicator displays a pop up showing the total disk usage, then a split by Primary and Secondary storage.

The Actions (□) menu provides you with a number of different ways to interact with the domain users. This includes:

• Impersonate User - As the system administrator, or if domain administrators have permission to impersonate users, when a user is selected and this action is taken, the administrator will log in to SmarterMail as that user and be able to see their entire account.
• Enable - Enables the account, allowing the user to access their mailbox and send/receive email.
• Disable - Disables the account. This, essentially, locks the user out of their account. However, when disabling a user, the domain administrator does have the ability to "allow incoming messages", so mail is still received even though the user is unable to log in.
• Expire Password - Force a user to change their password on their next webmail login.
• Reindex - Reindexes users/accounts to improve the search functionality for a user by reindexing their account.
• Recalculate Disk Usage - Recalculate the disk usage for one or more user accounts.
• Resync Devices - This forces a resync of all clients and all protocols for the selected user(s).
• Import from CSV - Import new user accounts from a CSV file.
• Import from Authentication Provider - When enabled, this allows a domain administrator to import new user accounts from Microsoft's Active Directory or via LDAP.

• Export All to CSV - Export a CSV file of all users on the domain.

• Attach User (System admin only) - Select this option to attach a user that is on disk but not in the domain. In other words, to restore the entire account. note: The user's folder needs to be correctly placed in the domain folder on the server prior to performing this action.

• Attach Folder (System admin only) - Select this option to attach a folder that is on disk but not in the user's folders list. In other words, to restore a user's email folder.

• Rebuild Folder (System admin only) - Select this option to copy .grp files or .eml files into an existing user's folder and have SmarterMail re-build that folder to include the new .grp and .eml files. In other words, to restore a user's emails. note: When rebuilding folders, there could be a UID conflict issue if you restore .grp files into an existing folder with existing .grp files. If you are only restoring email messages, it is recommended that you create a new folder within the SmarterMail interface and copy the .grp and/or .eml files to that new folder. Then use the Rebuild Folder function. This issue would not occur when restoring .eml files into an existing folder with existing email.

• Detach User (System admin only) - This allows you to essentially remove the user from the domain without affecting any of the user's data. Their data remains on disk, but it's not part of the domain. For example, if a user leaves but the domain admin (or the business) wants to retain the user's data for legal or regulatory reasons. When needed, the user can be re-attached to the domain and the information access.

Expire Password

This option can be used to expire the password of one or more users, forcing the user(s) to change their password the next time they log into the webmail interface. To expire the password of one or multiple users, checkmark the desired user accounts, click on the Actions (□) button, then click on Expire Password . Note: If password changes were disabled for a user, expiring the user's password will automatically enable password changes and expire their password. They will be required to set a new password next time they log in. In addition, accounts set to Active Directory authentication cannot be expired.

Reindex

If a user reports errors or a lack of results when performing a search, it may be necessary to reindex their user account, which will regenerate the mailbox index file. To reindex one or multiple users, checkmark the desired user accounts, click on the Actions (□) button, then click on Reindex .

Recalculate Disk Usage

This option can be used to recalculate the disk usage for the selected user(s). If you find discrepancies in the user's disk usage display throughout the various areas of the interface (in the email section,

reports, or Users grid), use this option to recalculate and correct that display. Please note that there may be no visual effect if the disk usage numbers shown were already correct. To refresh the disk usage for one or multiple users, checkmark the desired user accounts, click on the Actions (▢) button, then click on Recalculate Disk Usage .

Resync Devices

This option can be used by either a domain administrator or a system administrator to help potentially resolve an issue that's seen by a user who is using a particular client. (I.e., Microsoft Outlook, eM Client, etc.) For example, a user can see an issue receiving new emails in Outlook for Windows, which uses the MAPI protocol. The issue they're seeing may be the result of something hung in a different client: iOS Mail that uses EAS, eM Client that uses EWS, Gmail that is using IMAP. To help resolve this issue, an administrator can force a resynchronization of all clients across all protocols, thereby clearing up any issue regardless of which protocol is affected.

An administrator (domain or system) can use this tool on up to 25 individual accounts, on a single domain, at a time. Once started, a toast notification appears for the administrator(s) running the resync that lets them know the resync has started. They also see a notification. Once the resync has completed another notification appears with the results. If one or more users are unable to be resynced, that information appears in the notification, but the resync will continue until all users have been synced. note: The notification will appear for all domain or system administrators, not just the one running the resync.

All resyncs are captured in the Administrative logs. Important Note: Resyncing user protocols can cause an increase in server resources, so it is restricted to 25 users at a time to mitigate impact on a server. When resyncing ALL users (in batches of 25) administrators will want to closely monitor CPU and memory usage to ensure the server can handle the additional load.

Import from CSV

To add new SmarterMail users via a CSV spreadsheet, click on the Actions (▢) button then click on Import from CSV . Upload the CSV file that contains the user information and click Next . The first page of the import modal will allow you to map the CSV column headers to the appropriate configuration option within SmarterMail. For example, if your CSV contained a column header for "user name", you can select the "Username" mapping.

At minimum, the CSV file must contain a "Username" column header. All remaining configuration options will mimic the domain's User Defaults template. If no "Password" column header is provided in the CSV, the import modal will prompt you to create a temporary password for the user(s) being imported. Those users will be prompted to change their password the next time they log into the webmail interface.

Import Users From Authentication Provider

This feature is only available to domain administrators using SmarterMail Enterprise.

By default, SmarterMail uses a standard username/password authentication method. However, some organizations rely on Windows-based authentication methods like Active Directory or LDAP. SmarterMail can certainly interact with either of these authentication methods.

Active Directory (AD) is just what the name implies: a directory of users that are part of an organziational unit. AD stores the users and their information, including login information and passwords. SmarterMail can integrate with AD rather easily, but it can only read AD information, it cannot write or otherwise change AD credentials or user information.

The Lightweight Directory Access Protocol (LDAP) is, as its name implies, a lightweight client-server protocol that email servers, software and network appliances can use to connect to, and look up information from, a directory service. For example, LDAP can be used to look up information from Microsoft Active Directory.

Just as with Active Directory, SmarterMail acts as an LDAP client. That means LDAP can be used to integrate SmarterMail with Microsoft Active Directory as a lookup service for users, finding the accounts within aliases, and finding mailing list subscribers, as well as an authentication method for users. The LDAP integration between SmarterMail and AD via LDAP is, therefore, one-way: SmarterMail can look up information within Active Directory, but it can't send information TO Active Directory.

Therefore, when either LDAP or Active Directory are used as an authentication method for users, if the user changes their password, display name or other information in SmarterMail, that change is NOT synced back to Active Directory, either directly or via LDAP. However, if that same information is changed in AD, it will sync back to SmarterMail.

It's also worth noting that LDAP integration will only function if SmarterMail is on the same domain as the LDAP server you are trying to connect to.

Export All to CSV

To export a list of all user accounts on the domain, click on the Actions (□) button then click on Export All CSV . The CSV file will continue a variety of details about the user accounts, including their username, display name, authentication method, home and work address, disk usage, and more.

Managing Users

This settings page is only available to system administrators and domain administrators.

The Users section is where system and domain administrators can add, view and modify users on a domain, where each user represents a person's actual mailbox and email address (ex: jdoe@@example.com). Administrators can modify basic configuration options for a user, including their password method, features they can access, reply-to addresses, webmail preferences and more.

For a better understanding of the actions that can be performed in the Users section, see the Users Overview page.

When viewing or editing a user, the following cards are available:

- Account
- User
- Service Access
- Folder Auto-Clean
- Default Folders
- Temporary Password
- Webmail
- Forwarding
- User Groups
- Throttling

User Actions (□)

When viewing a specific user from the Users page, several actions can be performed by clicking the Actions (□) button. These include:

- Impersonate User - If domain administrators have permission to impersonate users, when a user is selected and this action is taken, the domain administrator will log into the user's account and be able to see their entire account.
- Rename - Allows a domain administrator to change the username.
- Change Password - This allows the domain administrator to change the password for the user (or on the user's account). This option is not available when using Active Directory authentication.
- Expire Password - This removes the user's SmarterMail password, forcing them to change it on their next login to webmail. This option is not available when using Active Directory authentication.
- Reindex - Improves the search functionality for a user by reindexing their account.
- Recalculate Disk Usage - Recalculates the disk usage for the user.
- Resync Devices - This option can be used to help potentially resolve an issue that's seen by the user when using a particular client. (I.e., Microsoft Outlook, eM Client, etc.) For example, the

user may see an issue receiving new emails in Outlook for Windows, which uses the MAPI protocol. The issue they're seeing may be the result of something hung in a different client: iOS Mail that uses EAS, eM Client that uses EWS, Gmail that is using IMAP. To help resolve this issue, a resynchronization of all clients across all protocols may clear up any issue regardless of which protocol is affected.

Account

• User - The identifier the user uses to log in to SmarterMail. To change an account's username, click on the Actions (□) button and then Rename .

• Status - Domain administrators can change the status of a user to limit their access as needed. For example, if a user leaves the company, either voluntarily or not, a domain administrator can suspend the user pending further review by company management. Options include:

• Enabled - The mailbox is in use by the user.

• Disabled and allow mail - The mailbox continues to receive email but the user is unable to access their mailbox.

• Disabled and don't allow mail - The mailbox no longer accepts incoming messages and the user is unable to access their mailbox.

• Display Name - The friendly name that is displayed on outgoing messages.

• Mailbox Size Limit - The maximum size of the mailbox. By default, the maximum mailbox size is 100 MBs. However, domain administrators can change this to whatever they like to correspond to company limits. For unlimited disk space, type in 0.

• Domain Administrator - Enable this setting to make this user one of the domain administrators for the domain, which allows the user to create new users and edit domain-wide settings.

User

• Language - The language selected for Users in SmarterMail is EXTREMELY important. That's because it's much more than simply what is seen in the webmail client when that User logs in. SmarterMail's language selection is the basis for everything: the things seen in the webmail interface as well as what's returned to an email client when connecting using Outlook, eM Client, iOS Mail and more. That includes things like settings labels, folder names, calendars and calendar appointment, contact groups, email message content, log files and essentially everything within SmarterMail. Therefore, it is extremely critical select the proper language for a User. For more information, see Languages, Protocols and Clients

• Changing Language Settings : When a user tries to update their language, SmarterMail checks for potential conflicts prior to changing the language. For example, if a user is set to English and they have a folder named "Bandeja de entrada", if they try to change their language to Spanish,

the change will not be saved and they will see a warning letting them know that the language wasn't updated to prevent an email folder name conflict. This is because "Bandeja de entrada" is the Spanish name for Inbox used in the default Spanish language translation file. If the change was saved, there would be 2 folders with the same name, which would cause issues.

• Time Zone - The time zone to use for marking the sending and receiving date and time.

• Reply-to Email Address - The email address used in the reply-to header of messages sent through webmail. This address will be used by receiving email clients when replying to a message. While it's possible to set the Reply-to address or a user, that user can change the Reply-to when composing a message or reply in an email client, such as Microsoft Outlook. Should they do this, that address will take precedence over what's set in the user's settings.

• Recovery Email Address - The email address to which password reset instructions will be sent if the user forgets their password. This address should be separate from their SmarterMail address, such as a Gmail or Yahoo! address, or even the default email address of a domain administrator. If the user is protected by 2-Step Authentication, this address may also be used to retrieve the 2-Step verification code. Note: The backup email address can only be used if the system administrator has enabled password retrieval for the login page.

• Plus Addressing - Plus addressing allows users to automatically sort incoming email without creating content filtering rules first. A major benefit of plus addressing is that it allows users to generate special email addresses if they do not want to give out their real address. For example, if user@@example.com needs to provide a valid email address to sign up for a newsletter, he can sign up for the newsletter using the following address: user+technewsletter@@example.com. When the newsletter is delivered, it can automatically be routed to the Technewsletter folder. If the folder does not already exist, it can be created automatically. Note: For plus addressing to work, the plus (+) sign is required AFTER the username but BEFORE the domain name. For example, username+foldername@@domain.com.

• Disabled - Select this option to turn off plus addressing for the account.

• Move to Folder - If the target folder already exists, the incoming message will be placed into it. If the folder does not exist, it will be created automatically. note: To prevent abuse, no more than 10 folders can be auto-created in this method during a six hour period.

• Move to Folder (If Exists) - If the target folder already exists, the incoming message will be placed into it. If the folder does not exist, the email will be placed in the Inbox.

• Leave in Inbox - The incoming message will be placed in the Inbox.

• Disable password changes - Select this option to prevent the user from changing the login password. This setting overrides the password expiration found in Security settings. A user's password will not expire or be required to be changed if this setting is enabled.

• Show in Global Address List - This setting is enabled by default and allows users to be displayed in the Global Address List, which is found in the Contact section. This option is

useful for only displaying addresses that are tied to real people as opposed to addresses used by departments, such as support@@example.com. Note: This option is only available when using SmarterMail Enterprise.

Service Access

This card can be used to adjust a user's access to the standard protocols that SmarterMail utilizes. For example, you can limit services like POP, IMAP and SMTP so that specific users are not able to connect their email accounts to external email clients. The following services can be managed for each user:

- Webmail - Enable this option to allow users to log into SmarterMail from the webmail interface.
- POP - Enable this option to allow users to download mail to an email client using POP3.
- IMAP - Enable this option to allow users to create a two-way email sync between SmarterMail and an email client using IMAP.
- Inbound SMTP - Enable this option to allow users to receive email from external senders. That is, any user outside their own domain. (So, from Gmail, etc.)
- Outbound SMTP - Enable this option to allow users to send email to external recipients. That is, any user outside their own domain. (So, to Gmail addresses, etc.)
- Chat (XMPP) (Enterprise Only) - Enable this option to activate SmarterMail's included Chat feature for users.
- WebDAV - This will give users the ability to set up accounts to sync calendars (calDAV) and/or contacts (cardDAV) to various mobile and desktop clients that support this protocol.
- EAS (Enterprise Only) - This will give users the ability to set up Exchange accounts on mobile email clients, contacts and calendar apps, etc.
- MAPI/EWS (Enterprise Only) - This will give users the ability to set up Exchange accounts in Microsoft Outlook for Windows, Outlook for Mac, Apple Mail and eM Client.

Temporary Password Note: This setting is reserved for system administrators who are managing and/or impersonating a user.

This option allows system administrators to create an additional, temporary password in order to troubleshoot issues. A user's actual password will rarely be shown to system administrators, and creating and using a temporary password does not disable the user's standard account password or impact their ability to log in or access webmail. Creating a temporary password, rather than impersonating the account, may be required when it's necessary to log into a user's email or IM client where impersonation is not available. In addition, administrators will find that some behavior in webmail may be slightly different when an account is impersonated versus when they're logged in directly.

When using Temporary Password, the following options are available:

> • Generate - Clicking this button will automatically generate a temporary password for the account. Only one temporary password may be created at a time, and on creation, will be available for 24 hours.
>
> • Revoke - Revoking a temporary password invalidates it immediately. Therefore, a new temporary password will need to be generated as needed.
>
> • Extend - Choosing to extend the password will add 24 more hours to the remaining time.

Folder Auto-Clean

Setting up auto-clean rules for email folders is a simple, yet effective, way to limit how much of your disk space is taken up by messages in default folders like Junk Email, Sent Items, and Deleted Items as well as any custom folders a user creates. Unlike domain administrators, who can only create auto-clean rules on the default folders created by SmarterMail, users can set up rules for any folder, including custom folders.

Setting up auto-clean rules helps users ensure that their disk space does not fill up unnecessarily. In some cases, particularly when SmarterMail is being provided by a hosting company or ISP, users may have disk space limits set for their accounts. Keeping unnecessary or unwanted email cleaned up, and freeing up space that could be used by unnecessary messages, is one way to help these users stay within the limits placed by their hosting company.

> • Override auto-clean settings - Enable this setting to override the settings established by the domain administrator, allowing you to create your own rules. Any changes you make will not be affected if the system administrator changes their policy, unless they disable domain overrides.

If the "Override auto-clean settings" setting is missing, the auto-clean rules created by the Domain or system administrator will be displayed at the bottom of this card. If no rules were created by an administrator, a note saying such will be displayed.

However, if "Override auto-clean settings" is turned on, you're presented with a New rule button that will allow you to create your own rule(s). Auto-clean rules can be created for any default mail folder, and can be created based on a message's age, the length of time a message has been in a folder, or a particular folder's size.

Size of Folder vs. Age Rules

It's possible to either set an auto-clean rule based on the size of a folder, or the age of a message (or messages) within a folder. Size-based auto-clean rules are run whenever an action is performed on a particular folder. For example, moving a message into the folder. Once that action occurs, the auto-clean rule is run, and it runs each time an action is performed. Age-based rules, however, run once per

day on the FIRST folder action for that day. For example, deleting an email first thing in the morning. When you delete an email, it's moved to the Deleted Items folder, which is a folder action. At that point, if there's an age-based auto-clean rule for the Deleted Items folder, the rule is run, and then is silent until an action is performed on the next day.

When using a folder's size, it's possible to set upper and lower limits for the space used for the folder. For example, you can create an auto-clean rule so that when a folder gets larger than 50MB in size, the rule automatically deletes messages to reduce the folder's size to 5MB. When freeing up space, the total size of each message is used, which includes any message attachments.

When using Age as a guideline, there are two types of age: Message Age and Age in the Folder.

> • Message Date: This is based on the initial receipt date of the message. So if you received a message on January 1st, and the number of days is set to 14, on January 15 the message is automatically deleted.
> • Time in Folder: This is based on when a message is actually moved to the folder that has the auto-clean rule configured. The age of the message itself is not used. That means, if the Age in Folder is set to 14 days, it doesn't matter when the message was received. Instead, the message is deleted 14 days after it's been moved into the folder.

Default Folders

When creating a new user in SmarterMail, default folders are created for holding certain types of information. Calendar appointments/events, contacts, notes, tasks, etc. are initially stored in these folders: My Calendar, My Contacts, My Notes, My Tasks. However, users may want to change where this information is held when, for example, a new contact is added. Users may want contacts stored, by default, in their own "Business Contacts" folder as opposed to My Contacts. This is where specifying default folders comes in handy.

It is worth mentioning that only existing folders can be selected as a new default. Therefore, users will need to go to specific areas and create new folders before they can be selected as the new default folder.

Changing the default folder for a specific item is simply a matter of selecting it from the relevant dropdown. Once a default folder is changed, any new item created will be stored in that folder. (Existing items remain in their original folder. Only new items will use the new default.) Note: If a particular user has any Delegation rules, default folders can not be changed.

Webmail

> • Delete Email Action - To specify the action performed on deleted messages, select the

appropriate action from the list. note: This action only affects messages. If folders are deleted, the folder and its contents will always go to the Deleted Items folder.

• Move to Deleted Items folder - Deleted items will appear in the deleted items folder, which will need to be regularly emptied.

• Permanently Delete - Permanently deletes the message. note: When deleted messages are purged, the action is final. You will not be able to retrieve these messages later.

• Mark as Deleted - Flags the message for deletion, but it does not move messages to the Deleted Items folder and messages remain until the folder is purged.

• Compose Font - Specify the default font for emails by selecting an option from the list.

• Font Size - Specify the default font size for emails by selecting an option from the list.

• Default From Address - Select the email address that you reply from by default for messages sent through webmail. Your SmarterMail email address and any domain aliases or SMTP accounts configured will be shown in this list. (This setting does not prevent you from manually changing the Send From address when composing a message.)

• Preview Pane - To specify where the preview pane displays in the webmail interface, select the appropriate option from the list: Right or None. By default, the preview pane appears to the right of the messages list. Disabling the Preview Pane means only a list of messages appears in the content pane and each message will need to be opened separately in order to view their contents.

• Search Language Indexer - The language that the Apache Lucene indexer will index against. In most cases, Generic Indexer is the best selection as it incorporates English and common umlauts. However, if the user views the interface in certain languages, such as Chinese, Japanese, or Korean, this setting should specify the language for better indexing results.

• Use To: address for replies - When enabled, replying to a message via webmail will use that email's To: field as the Send From address of a reply, regardless of whether the message was sent to a specific SmarterMail email address or a domain alias, email alias, SMTP account, disposable address or plus address. For example, if an email is sent an alias, replies to that email via webmail will automatically use the email alias address of the Alias member as the Send From address. (This setting does not prevent a user from manually changing the Send From address when composing a message.)

• Request read receipts by default - Select this option to automatically request read receipts for all outgoing messages sent via webmail. When this setting is enabled, all outgoing messages that are sent via webmail will request that the recipient(s) send a read receipt when the message has been read. If the read receipt is sent by the recipient(s), the user will receive a message from the system administrator confirming that the message has been read. Note: Users should be careful when enabling this feature and should only do so if required for business or compliance or regulatory requirements.

• Request delivery receipts by default - Select this option to automatically receive delivery receipts for all outgoing messages sent via webmail and email clients. When this setting is enabled, the user will receive a message from the system administrator stating the status of their outgoing message. Note: Users should be careful when enabling this feature and should only do so if required for business or compliance or regulatory requirements.

• Mark messages downloaded by POP as read - Select this option to mark all messages that are downloaded via a POP3 connection as read.

• Draft auto-save - Enable this option to have drafts of messages created within the webmail client to be saved every 2 minutes.

• Hide email avatars in the message list - Enable this option to hide any avatars — images, monograms, Gravatar pictures, etc. — from your list of messages. This disables avatars for all folders, including custom folders. It does not have any effect on messages, or messages that display in the content pane.

• Show images from external websites - Enable this option to automatically display all in-line remote content when an email is viewed. (Remote content is considered to be any image, video, animated gif, etc. that has an external source and is contained in the message.) When this is enabled, the user will not have to manually display the remote content on emails they receive; it will be visible automatically. Note: Emails from trusted domains and senders will always display remote content automatically.

• Allow Inline Images From - Here you can enter the email addresses or domains (one entry per line) whose in-line remote content should be displayed automatically, even if the previous setting is turned off. If an email address is entered, emails received from that address will automatically display all remote content. If a domain is entered, remote content that comes from a source containing that domain will be automatically displayed. For example, if "smartertools.com" was entered in this field, remote content from a source of "https://images.smartertools.com" would be automatically displayed, even if that email was sent from user@@example.com. (If an exception for an email address is added from an email directly, that email address will be listed here.) note: Emails from trusted domains and senders will always display remote content automatically.

• Allow Email Tracking From - Here you can enter the names of mail tracking providers (one entry per line) that you will allow. In addition, when enabling an email tracking provider from the tracker modal on individual messages, they appear here.

Forwarding

If this card is not displayed, your domain has not been permitted to utilize automated forwarding. To display these options, a system administrator must enable the Automated Forwarding feature for your

domain. Note: These settings only affect webmail. If it's been disabled for your domain, forwarding may still occur when using Events and/or content filters, or when using an email client.

- Allow automated forwarding - Select this option to allow the user to utilize the automated forwarding feature and to display the forwarding settings. If this setting is disabled, the Forwarding card will not be displayed in the user's Account settings.
- Forwarding Address - The email address to which messages sent to the mailbox will be automatically forwarded. note: Messages routed to other email folders via content filters or plus addressing will also be forwarded to this address.
- Keep original sender and recipients when forwarded - When enabled (which is the default), an email is essentially re-routed to the new recipient and keeps its original "To" and "From" addresses. When disabled, the forward behaves as if the email was manually forwarded, so the "From" address is replaced with the address of the mailbox forwarding the message, and the "To" address is the mailbox listed in the Forwarding Address.
- Delete messages when forwarded - Select this option to delete messages from the SmarterMail mailbox after they are forwarded.

User Groups

User Groups are used to give a specific subset of users on the domain permission to access shared resources. For example, if a business wanted to make it easy for members of its sales department to share their calendars with other team members, the domain administrator would create a user group for all the sales department employees.

If any User Groups have been created, they'll be listed here and can be set to On or Off for specific users.

Throttling

Throttling limits the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. Domain administrators can use this feature on a per-user basis to either delay or reject messages that exceed their desired limits, thereby ensuring users don't send out massive amounts of email throughout the day that can possibly get the domain blacklisted. Note: For each threshold and action, you'll see "(Default = X)" which indicates the throttling policy that's put in place by the system administrator for the ENTIRE domain. It's important to consider the domain's throttling limits when modifying a specific user's limits. For example, if you set the user's throttling limit to the domain max, and that user sends that many messages in an hour, the WHOLE domain would be throttled. This means that outgoing messages from all users on the domain would either be delayed or rejected, depending on the domain's throttling action. (If messages are already in the spool, from a user or a

domain, when a throttling limit is reached, these messages are essentially delayed even if the throttling action is set to "reject" — only new messages sent would be rejected.)

- Outbound Messages per Hour (0 = Unlimited) (Default = 5000) - The number of messages sent by the user per hour.
- Message Throttling Action (Default = None) - Select an action for SmarterMail to take once the particular throttling level is reached. Of course, administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of mail being sent falls beneath the throttling limit that is set.
- Outbound Bandwidth per Hour (0 = Unlimited) (Default = 100) - The total number of MBs sent by the user per hour.
- Bandwidth Throttling Action (Default = None) - Select an action for SmarterMail to take once the particular throttling level is reached. Of course, administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of bandwidth being used falls beneath the throttling limit that is set.

Aliases

This settings page is only available to domain administrators.

An email alias is essentially a forwarding email address that can be used to forward messages to a single address or multiple email addresses. Aliases are most commonly used for departments or groups of individuals, like a small team of people working on a project or task. For example, in a working environment with multiple email addresses, the office may want to make a central email address that distributes messages to all personnel. The alias, workplace@@example.com, can be made for messages to be sent and then distributed to all the employees. Note: Even though an alias acts as an email address, users cannot log in to an alias like they do a standard email address; there is not a mailbox associated with the alias and no email is ever actually stored for the alias itself. Instead, emails are simply sent to the list of addresses provided for the alias and are stored in the mailboxes of the individual users.

When viewing the Users tab, the following information is listed:

- Account - The "username" of the alias, which is used when sending an email to the alias, chatting the alias (if available), etc.
- Display Name - The friendly name given to the alias.
- Description - A brief description/explanation of the alias.
- Email Addresses - The total number of actual users associated to the alias. E.g., 6 would mean 6 email addresses are used for the alias.
- Show in GAL - Denotes whether the alias will be displayed in the Global Address List (GAL).

• All Users - Denotes whether the alias incorporates all users of the domain as opposed to individual email addresses. E.g. an "Office" alias would probably include all users.

• Send From - Denotes whether users are able to send from the alias.

• Show in GAL - Denotes whether the alias will be displayed as part of the Global Address List.

• Show in Chat - Denotes whether the alias will appear when using Live Chat.

Adding Aliases

Whether creating a new alias or editing an existing one, the following options will be available:

• Name - The name of the alias. This name will be used to create the email alias address. For example, if you want to use the email alias address "info@@example.com", you'd simply use "info" for the Name. (You do NOT need to add the domain to the end of the name — that's supplied automatically.)

• Display Name — This is the friendly name used for the Alias. When used in conjunction with "Allow alias users to send from this alias", this is the display name that appears as the sender in the recipient's inbox.

• Email Addresses (one per line) - Type the full email address(es) of the user(s) who should receive emails sent to this alias.

• Internal use only - Enable this option to only allow emails to be delivered to accounts that are hosted within the same SmarterMail server.

• Include all domain users - Enable this option to include all domain users automatically in the alias. note: This option does not override the email addresses listed in the Email Address box. If selected, all domain users will be included in addition to the users entered in the Email Addresses text box.

• Alias can be used as from address in webmail - Enable this option to allow alias users (those users/accounts that are part of the alias) to manually change their From address to the alias email address on new emails and replies. When a user sends mail as an alias, the recipient will see the alias's Display Name as the email friendly from address. If the Display Name for the alias is blank, the user's Display Name shows.

• Show in Global Address List - Enable this option to display the alias in the Global Address List. Note: This feature is only available when using SmarterMail Enterprise.

• Show as a room in chat (Enterprise Only) - Enable this option to allow the alias to appear as a room in Chat. Enabling aliases for chat means that chats can be sent to the alias, and everyone in that alias, from within webmail as well as when using third-party chat clients.

• Use as domain catch-all - Enable this option to use the alias address as a catch-all for the domain. A catch-all alias is an email address that will catch any incoming email sent to an

invalid address on a domain. Instead of bouncing the message back to the sender, the message will be stored in the mailbox that is assigned as the catch-all. Note: This option will only be visible if the system administrator has enabled catch-all as a feature for the domain. In addition, only one email alias can be assigned as the domain catch-all at a time. Enabling a different alias as the catch-all will override any assignment already in place.

A Note About Catch-All Aliases

A catch-all alias is simply that: an alias that catches all email sent to a domain that doesn't correspond to an actual user. Catch-all aliases can be useful as long as they are monitored and kept clear of unwanted email. However, due to the nature of email and the amount of spam that is sent every day, a catch-all can become a burden to email systems and to domain administrators. Therefore, it is suggested that they be used sparingly, or not at all if it can be avoided. Furthermore, it is important to never set an autoresponder for a user that the catch-all forwards to as it may result in backscatter, causing additional bandwidth usage and potentially causing your domain to be blacklisted.

Mailing Lists

Mailing Lists Overview

This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For example, many companies use mailing lists to email newsletters, promotional offers, or information about product updates to subscribers. Unlike an Alias , a mailing list allows people to subscribe to, or unsubscribe from, email communications. In addition, mailing lists can be public or private, be replied to by all users or managed by a single list moderator and more. Note: SmarterMail can accommodate mailing lists of up to 75,000 subscribers. Anything greater than that should be managed by a third-party mailing list service provider such as Constant Contact or MailChimp.

Using a mailing list is as simple as sending a standard email: the allowed posters simply send an email to the list address, which takes the form of the list name appended to the domain name. For example, if you create a mailing list called "newsletter" you send a message to newsletter@@example.com. If there are other requirements, such as a password, etc. those need to be taken into account as well.

By default, when a subscriber reads a mailing list message, the From field in the subscriber's inbox will display the email address of the individual that sent the mailing list message; the To field will display the list name or mailing list email address; and the Reply To field will display the mailing list

email address or the email address of the individual that sent the message, depending on the list settings.

Mailing Lists can be managed by system administrators with Manage Domains permissions, domain administrators and the list moderators themselves. Accessing Mailing Lists is dependent on the role you possess:

List Moderators

If you are a list moderator, when you navigate to your Settings, you'll have Mailing Lists display in the navigation pane. The lists you manage will be displayed here.

Domain Administrators

As a domain administrator, lists are displayed on the Mailing Lists tab on the domain's Accounts page. All lists set up for various administrators are displayed here.

System Administrators

As a system administrator, select a domain and go to the Accounts tab for the domain. All lists set up for various list moderators for the domain can be found on the Mailing Lists tab.

Regardless of your role, whether creating a new mailing list or modifying an existing one, the following options will be available:

- Options - Configure the mailing list options and permissions
- Subscribers and Digest Subscribers - Add subscribers who will receive the standard mailing list postings or digest emails.
- Allowed Posters - Whitelist email addresses or domains who can post to the mailing list
- Banned Posters - Prevent specific email addresses or domains from posting to the mailing list
- Messages - Configure the header and footer for postings as well as the replies sent to listserv commands
- Custom Fields - Customize list postings with subscriber custom fields

Variables

Emails that are posted to a mailing list support the use of the following variables. These variables can be used in the body or subject line of emails that are sent to the mailing list subscribers and also in the footer, header and subscriber Messages . Though similar to Custom Fields in format, these variables need no additional configuration. Simply enter the variable below to display its associated information. Variables will always follow this format: #Variable#

- Unsubscribe Link (#UnsubscribeLink#) - An unsubscribe variable is included to allow users to unsubscribe from the mailing list with a URL. Note: This URL can also be given friendly

hyperlink text (rather than linking the URL) by modifying the Friendly Unsubscribe setting when configuring or modifying a mailing list. For more information, see Mailing List | Options .

• Recipient (#Recipient#) - The email address of the subscriber who was sent the message.

• Sender (#Sender#) - The email address of the user sending the message.

• Domain Date Now (#DomainDateNow#) - The current date (in shorthand) according to the domain's new user time zone defaults found in User Defaults. Ex: 07/13/2015.

• Domain Time Now (#DomainTimeNow#) - The current time according to the domain's new user time zone defaults found in User Defaults. Displayed in 24-hour format.

• Domain Date Time Now (#DomainDateTimeNow#) - The current date and time according to the domain's new user time zone defaults found in User Defaults. Displayed in shorthand and 24-hour format.

• Domain Day Now (#DomainDayNow#) - The current date (date alone, without month and year) according to the domain's new user time zone defaults found in User Defaults. Ex: 13.

• Domain Month Now (#DomainMonthNow#) - The current month (in numeric value) according to the domain's new user time zone defaults found in User Defaults. Ex: 07.

• Domain Year Now (#DomainYearNow#) - The current year according to the domain's new user time zone defaults found in User Defaults. Ex: 2015.

• Domain Day Name Now (#DomainDayNameNow#) - The current day of the week according to the domain's new user time zone defaults found in User Defaults. Ex: Monday.

• Domain Month Name Now (#DomainMonthNameNow#) - The current month (by its name) according to the domain's new user time zone defaults found in User Defaults. Ex: July.

• Moderator Date Now (#ModeratorDateNow#) - The current date (in shorthand) according to the Moderator's time zone. Ex: 07/13/2015.

• Moderator Time Now (#ModeratorTimeNow#) - The current time according to the Moderator's time zone. Displayed in 24-hour format.

• Moderator Date Time Now (#ModeratorDateTimeNow#) - The current date and time according to the Moderator's time zone. Displayed in shorthand and 24-hour format.

• Moderator Day Now (#ModeratorDayNow#) - The current date (date alone, without month and year) according to the Moderator's time zone. Ex: 13.

• Moderator Month Now (#ModeratorMonthNow#) - The current month (in numeric value) according to the Moderator's time zone. Ex: 07.

• Moderator Year Now (#ModeratorYearNow#) - The current year according to the Moderator's time zone. Ex: 2015.

• Moderator Day Name Now (#ModeratorDayNameNow#) - The current day of the week according to the Moderator's time zone. Ex: Monday.

• Moderator Month Name Now (#ModeratorMonthNameNow#) - The current month (by its

name) according to the Moderator's time zone. Ex: July.

• Server Date Now (#ServerDateNow#) - The current date (in shorthand) according to the server's system time zone. Ex: 07/13/2015.

• Server Time Now (#ServerTimeNow#) - The current time according to the server's system time zone. Displayed in 24-hour format.

• Server Date Time Now (#ServerDateTimeNow#) - The current date and time according to the server's system time zone. Displayed in shorthand and 24-hour format.

• Server Day Now (#ServerDayNow#) - The current date (date alone, without month and year) according to the server's system time zone. Ex: 13.

• Server Month Now (#ServerMonthNow#) - The current month (in numeric value) according to the server's system time zone. Ex: 07.

• Server Year Now (#ServerYearNow#) - The current year according to the server's system time zone. Ex: 2015.

• Server Day Name Now (#ServerDayNameNow#) - The current day of the week according to the server's system time zone. Ex: Monday.

• Server Month Name Now (#ServerMonthNameNow#) - The current month (by its name) according to the server's system time zone. Ex: July.

Options

> This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

Mailing lists has a number of moving parts. As a result, we've separated each tab for creating/managing a mailing list into its own page:

• Options - The configuration options for an individual mailing list.

• Subscribers and Digest Subscribers - Add subscribers who will receive the standard mailing list postings or digest emails.

• Allowed Posters - Whitelist email addresses or domains who can post to the mailing list

• Banned Posters - Prevent specific email addresses or domains from posting to the mailing list

• Messages - Configure the header and footer for postings as well as the replies sent to listserv commands

• Custom Fields - Customize list postings with subscriber custom fields

Creating a New Mailing List

When creating or managing a mailing list, a modal window opens with the following fields:

• Name - This is the name that will be used when sending to the list. A list name is similar to an email address: it simply needs to be whatever will be appended to the left of the domain name.

For example, "MarketingNewsletter". Posters, then, send messages to "MarketingNewsletter@@domain.com". Therefore, just as with accounts, list names should not include spaces, special characters, etc.

• List Moderator - This is the existing Account that will act as the administrator of the list. Select a user from the dropdown. Note: It is possible for the List Moderator to be a domain alias.

Once the new list is created, or if a list is being edited, the first tab you see is the Options tab.

Options

• Name - This is the name that will be used when sending to the list. A list name is similar to an email address: it simply needs to be whatever will be appended to the left of the domain name. For example, "MarketingNewsletter". Posters, then, send messages to "MarketingNewsletter@@domain.com". Therefore, just as with accounts, list names should not include spaces, special characters, etc.

• Status - New mailing lists default to a status of Enabled. To temporarily prevent postings to this list, change the status to Disabled.

• List Moderator - The "owner" of the mailing list. This person will actively manage the mailing list, posts to the list and any replies. The administrator must be an active email user for the domain.

• Show in Global Address List - There are times when you may want a mailing list to show up in the Global Address List so that all of your subscribers can send to it. If that's the case, enable this setting.

• Description - A brief summary of the mailing list.

Message Options

• List To Address - The email address that will display in the To field when a subscriber receives a mailing list message. Setting this to List Address means that the email address associated with the list will display as the To: address when recipients receive the message. The other option is to use the Subscriber Address, which means each subscriber will see their own email address in the To: field.

• List From Address - The email address that will display in the From field when a subscriber receives a mailing list message. By default, this is set to List Address. However, the email address of the person who poststo the list can be used, or each message to list subscribers can come from a specific user. Note: When setting this to "Poster Address", the poster's email address will be used. However, in order to bypass potential conflicts when performing DKIM and ARC signing (as the poster can be someone outside of the domain the list belongs to), SmarterMail will send messages "on behalf of" the List Moderator. That means that the "on

behalf of" text may appear under the From address in some mail clients. In these cases, the Sender will be the actual person sending a message to the list but it will appear "on behalf of" the list moderator.

• List Reply To Address - The email address that will display in the Reply To field when a subscriber receives a mailing list message. When a subscriber hits 'Reply' to the message, this address will receive the reply. If a subscriber hits 'Reply All' all list recipients will receive the reply. By default, this is set to List Address, but just as with the From address, the poster's address can be used or replies can be sent to a specific user.

• Text to show in unsubscribe link - The text entered here will be hyperlinked when using the Unsubscribe variable . If this field is left blank, the unsubscribe link will hyperlink the full URL.

• Webmail URL - The URL for the SmarterMail login page. This setting can be used to override the server's configured hostname for mailing list communications. Note: URLs should include the https:// prefix. For example: https://mail.example.com/

• Send Subscribe Email - Select this option to automatically send an email to new subscribers confirming their subscription to the list. This email is only sent when subscribe is initiated by the listserv command. If an administrator manually adds a subscriber to a list via the web interface, via the API or by importing via CSV, this email is not sent to the subscriber(s). Note: This is not an opt-in message, only a confirmation email.

• Send Unsubscribe Email - Select this option to automatically send an email response to unsubscribe requests. This email is only sent when unsubscribe is initiated by the listserv command. If an administrator manually removes a subscriber from a list via the web interface, via the API or by importing via CSV, this email is not sent to the subscriber(s).

• Enable double opt-In - Select this option to automatically send an email to new subscribers that requires them to confirm that they are subscribing to the list by clicking on an activation link. Using double opt-in is a good way to confirm subscriptions to the list and to help reduce abuse complaints. This email is only sent when double opt-in is initiated by the listserv command. If an administrator manually adds or removes a subscriber from a list via the web interface, via the API or by importing via CSV, this email is not sent to the subscriber(s). Note: If Double Opt-in is disabled for a list, any unverified subscribers will be removed from the list. A warning appears noting this for list moderator prior to making this change.

• Disable list error replies - Select this option to prevent the system from automatically replying to incorrect listserv commands.

Posting

• Password - To restrict people from sending emails to a mailing list, type a password in this field. Note: To send emails to a mailing list that is password protected, you must add the

password to the beginning of the subject line of the email, enclosed by brackets and colons. For example, if "password" is entered into this field, the subject line of the email would need to begin with [:password:].

• Subject Prefix - The optional text that will appear in the subject line. SmarterTools recommends using a subject prefix for discussion lists to help subscribers easily filter through posts. For example, add a "List- " or "Discussion -" prefix so that users know that the message is posted to an email list. Recipients can then create filters to move those messages to a specific folder or manage them in some other way.

• Allow anyone to post - When enabled, anyone can email the list, regardless of whether they are subscribed to the list or not. In turn, this sends an email to all members. Note: This setting can cause abuse if it is not closely monitored. Therefore, it is recommended to restrict the allowed posters to just subscribers, at the very least.

• Allow subscribers to post - When enabled, allows the list subscribers, and only the list subscribers, to send and receive posts. This can cause abuse issues as well if you have an active list, so this should only be used for smaller lists or for digest mode only.

Regardless of which option is enabled, List Moderators will always have the ability to post to the list. For particularly large lists, or for very active lists, it is recommended that both options, above, be disabled so only the List Moderator can post to the list as this ensures only relevant information is passed along and there is less chance of abuse.

Commands

• Mailing List Command Address This is the email address that is used when sending a list command.

• Enable SUBSCRIBE Command - Select this option to allow people to subscribe to the mailing list by emailing a listserv command to the command address. For more information, refer to Listserv Commands . Note: If this option is disabled, only list moderators can add new subscribers to the mailing list.

• Enable LIST Command - Select this option to allow people to receive a list of the mailing list subscribers by emailing a listserv command to the command address. For more information, refer to Listserv Commands . Note: It is recommended that you leave this option disabled, as people or automated systems could use the user list for malicious purposes.

Throttling

Throttling limits the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. Domain administrators can use this feature to ensure a mailing list does not send out massive amounts of email throughout the day, thereby possibly getting the domain blacklisted.

• Outbound Messages per Hour - The number of messages sent by the mailing list per hour. By default, the number of outgoing messages is 500.

• Message Throttling Action - When using either message or bandwidth throttling, administrators can select an action for SmarterMail to take once the particular throttling level is reached. Domain administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of mail being sent falls beneath the throttling limit that is set. By default, mailing lists are set to Delay messages once the threshold has been reached.

• Outbound Bandwidth MB per Hour - The total number of MBs sent by the mailing list per hour. By default, the outgoing bandwidth is 50MB.

• Bandwidth Throttling Action - This is the action to take if the throttling limit is reached. Administrators can elect to do nothing, delay the messages, or reject them outright.

Digest Settings

To reduce the number of emails mailing list subscribers receive, domain administrators can allow subscribers to sign up for digest mode or normal mode. Essentially, digest mode condenses all the messages sent to the list into a single email that is sent to subscribers on a monthly, biweekly, weekly, daily, or other defined basis. This is especially useful for very active lists or lists with a larger number of subscribers.

• Enable digest mode - Enable this setting to view and modify the remaining Digest settings.

• Subject - The subject line for the digest email.

• Trigger Type - The frequency of the digest emails: Daily, Weekly, Biweekly, Monthly or Manual. If Manual is selected, digest emails will only be sent when using the Send Digest button.

• Digest Format - The format (HTML, text, etc.) in which digest emails are sent.

• Disable non-text attachments in digest - Select this option to remove non-text attachments from the digest email.

• Send Digest - Allows an administrator the ability to send the Digest manually.

Subscribers and Digest Subscribers

This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

Individuals that sign up to receive messages from the mailing lists are called subscribers. Subscribers are categorized into two ways: the Subscribers tab stores the subscribers for standard mailing list postings and the Digest Subscribers tab stores subscribers for condensed digest emails.

Manually Adding Subscribers

There are two primary methods for manually adding subscribers — either regular list subscribers or digest subscribers — to a mailing list:

• If there are only a few emails to add to the mailing list, list moderators, domain administrators or system administrators with the proper domain management permissions can manually add subscribers.

• If there are a large number of emails to add to a mailing list, domain administrators or system administrators with the proper domain management permissions can upload a .CSV file containing all of the subscriber emails.

Adding individual subscribers to a mailing list:

• Select the desired mailing list. The mailing list settings will load in the content pane.

• On the Subscribers tab, the list of subscribers to this mailing list will load in the content pane.

• Using the New button, add the subscriber(s) email address(es), one per line.

• Once all addresses have been added, be sure to Save you changes.

Adding multiple subscribers to a mailing list at once:

It's also possible to add multiple users to a list at one time by uploading a list of users using a .CSV file. At a bare minimum, the .csv file must contain a column named "EmailAddress". Any additional columns in the .csv file will be added as Custom Fields for the corresponding subscriber/email address.

The Import from CSV option can be used to:

• Add new Subscribers, with our without Custom Field data.

• Update/overwrite the Custom Field values for existing Subscribers.

• Add new Custom Fields to existing Subscribers. note: If you import a CSV that contains existing Subscribers, their Custom Field data will be overwritten with the contents of the CSV.

• Select the desired mailing list and go to the Subscribers tab.

• Using the Actions (□) button, select Import CSV File . The Upload Subscribers modal window opens.

• You can either drag-and-drop a CSV file into the modal window, or click inside the window to open File Explorer to find and "open" the file. Click Upload in the content pane toolbar.

Managing Subscribers

Once a subscriber has been added to the list, you can modify their custom field values, review the

other mailing lists to which they are subscribed, see the history of bounce messages they've received and reviewed the history of messages they've received.

To download the list of subscribers as a text file, click on the Actions (☐) , then Export CSV File .

Allowed Posters

This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

List moderators, domain administrators and system administrators (with the proper Manage Domains permissions) can restrict the posting privileges for a mailing list to Anyone, Subscribers Only or Moderators Only. In addition, they can use the Posters section to specify additional list subscribers who can post messages to the list — these special subscribers are considered "Whitelisted" as they've been given special permission to post messages, in addition to, say, Moderators Only.

To add additional posters to a mailing list, use the Allowed Posters tab.

Using the New button, enter the email address(es) of the people who can post messages to the mailing list. Be sure to save your changes.

Uploading/Downloading Subscribers

In addition to manually adding new subscribers, it's possible to upload a text file that contains subscriber emails and any Custom Fields assigned to your subscribers. Text files should be in Comma Separated Value (.CSV) format.

Of course, since you can upload a subscriber list, you can also download one. This is especially convenient if the subscribers for one list — or a subset of those subscribers — is interested in another list you start up. Downloading your list subscribers, then editing it if needed, makes it simple to add subscribers to a new list.

Banned Posters

It's also possible to keep a list of users who are banned from posting to your mailing list. You can manually add email addresses to this list, as well as import subscribers. You can also download a banned posters list to use in other mailing lists you administer.

Banned Posters

This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

Administrators (list, domain or system) can restrict the posting privileges for a mailing list to Anyone,

Subscribers Only or Moderators Only. In addition, they can use the Banned Users section to specify additional blacklisted posters.

To prevent users from posting to a mailing list, use the Banned Posters tab.

To add a new banned user, use the New button and enter the email address(es) of the people who cannot post messages to the mailing list. Be sure to save your changes.

Messages

This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

Administrators can customize the system messages used for mailing lists. Some system messages, such as headers and footers, are viewable by list subscribers. Other messages are only viewable when emailing listserv commands to the mailing list username. For more information, please see Listserv Commands . Note: Variables can be used in the footer, header and subscribe system messages. For more information on variables, see Mailing Lists Overview .

To edit a particular message, simply select it from the list. When you do, a modal opens that will allow you to fully customize the message, as well as how that message is presented using a complete HTML editor. Once you've made your changes, be sure to save them.

- Command help email — LISTSERV COMMAND ONLY. This is the default message that is returned when a listserv command is sent to the mailing list username but the command is not recognized. By default, it returns information on how to properly format commands.
- Digest footer - This is the footer that is displayed when digest emails are sent to digest list subscribers.
- Digest header - This is the header that is displayed when digest emails are sent to digest list subscribers.
- Digest separator - This is the character set (e.g., dashes) that will be used to separate messages within digest emails.
- Double op-in successful email - This message is sent to subscribers notifying them that they were successfully subscribed to the list when the double opt-in subscription model is used.
- HELP response - LISTSERV COMMAND ONLY. This can be used to return information about the list, such as its creation date, last updated date, etc. or any other information the domain or list owner wants returned.
- LIST members response - disabled - LISTSERV COMMAND ONLY. This is returned when a particular list is set to not allow a list of subscribers to be returned. That is, the LIST command is not enabled for that list.
- LIST members response - enabled - LISTSERV COMMAND ONLY. This returns a list of

subscribers for a particular list. This requires the LIST command to be set.

• LIST response - LISTSERV COMMAND ONLY. This returns a list of the mailing lists for a particular domain. This requires the LIST command to be set.

• Post failure - insufficient permissions - This email is sent to posters that do not have the proper permission to post to the list. For example, this is returned to list subscribers who reply to the list but only moderators are allowed to post.

• Post failure - invalid list password - When a list is password-protected, this message is returned when a person posting to the list provides the incorrect information.

• Post failure - list disabled - This message is returned when a user attempts to post to a list that is no longer active.

• Post failure - message too big - This is returned when a message posted to a list is larger than the maximum size set for messages.

• Posted message footer - This is the footer (information at the very bottom of the message) that is displayed on messages that are sent to list subscribers.

• Posted message header - This is the header (information at the very top of the message) that is displayed on messages that are sent to list subscribers.

• SET MODE DIGEST response - failed - LISTSERV COMMAND ONLY. This is returned when the list command that sets the digest mode for a subscriber fails.

• SET MODE DIGEST response - ok - LISTSERV COMMAND ONLY. This is returned when the list command sets the digest mode for a subscriber.

• SET MODE STANDARD response - failed - LISTSERV COMMAND ONLY. This message is returned when the list command tries to set the mode for a subscriber that is not actually subscribed to the list.

• SET MODE STANDARD response - ok - LISTSERV COMMAND ONLY. This is returned when the list command sets the standard mode (one email per list post) for a subscriber.

• SUBSCRIBE response - double opt-in required - This message is sent to subscribers to verify their subscription request when your mailing list utilized a double opt-in subscription model (recommended).

• SUBSCRIBE response - list is private - This is returned when anyone tries to subscribe to the list but the list doesn't allow for automatic subscriptions. Instead, the list owner will need to add the subscriber manually.

• SUBSCRIBE response - subscribed - This is sent to a list subscriber when they subscribe to a specific list.

• UNSUBSCRIBE response - This is sent to a user when they unsubscribe from a specific list.

Mailing Lists | Custom Fields

This settings page is only available to domain administrators, mailing list moderators and system administrators with the proper permissions.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For a complete understanding of how mailing lists work, please see Mailing Lists Overview .

Mailing lists can utilize Custom Fields in order manage information about subscribers. When a custom field has been created, a value can be applied to a specific subscriber. Then, the custom field is used as a variable in a mailing list message in order to display that custom information about the subscriber. For example, if you'd like your messages to be sent out with the subscriber's first name in the message greeting (ex. "Hello John,"), you'd first create the Custom Field then add a value for each subscriber.

To create or manage Custom Fields, log into SmarterMail as an administrator (list, domain or system) and go to the Settings area based on your role. Then click on Mailing Lists in the navigation pane. Open a mailing list's configuration options and click on the Custom Fields tab.

Adding a New Custom Field

use the New button to add a new subscriber field. A modal window will display the following options:

- Name - The name of the Field. note: The text entered here is used as the variable when using custom fields in mailing list messages. For example, if you enter "First Name" in this field, you will need to enter #First Name# as the variable in the mailing list message.
- Default Value - Enter the text that should be automatically entered for current and new subscribers. Once the field is created, subscribers can be individually modified to change the value. Note: If a default value is not included, and the subscriber does not have their field configured, the variable will be removed from the message, leaving a blank space in its location.

Using Custom Fields in Messages

A Custom Field can be used in mailing list messages as a type of custom variable. To enter Custom Fields as variables, the name of the field must be enclosed with a #. For example, if a Custom Field was created for "Customer Name", you would enter #Customer Name# in your message.

Listserv commands

Listserv commands allow you to control the list through commands sent in email messages to the listserv command address. By default, the command address for a domain is "listserv@@example.com", where example is the name of your domain. However, your system administrator may change this command address.

To send a command, compose an email to the command address with the command in the body of the message. The subject of the message is ignored.

Available Commands Note: Any references to listname should be replaced with the list you are trying to use.

Help listname - Replies to the email with the contents of the Help system message for that list.

Subscribe listname - Adds your email address to the subscribers list of the mailing list. Note: This command can be disabled by the domain administrator.

Unsubscribe listname - Removes your email address from the subscribers list for the mailing list referenced by listname.

Set mode digest listname - Sets your email address to receive emails in digest mode, which will send all messages for the list combined into one email at regular intervals.

Set mode standard listname - Sets your email address to receive emails in standard mode (the default), which will send messages one at a time to your email account.

User Connections

SmarterMail will monitor users and display the number of connections to the different syncing protocols, including SMTP, IMAP, POP, XMPP, EAS, MAPI/EWS, WebDAV, and webmail. System administrators can then use this section to drop a user's current connection if they believe too many connections are being made by a user on a particular protocol, or resync the user's protocols to clear up any potential conflicts or inaccuracies. Using the tabs, users can be viewed all at once or separated by protocol. It's worth noting that the numbers displayed in each tab (i.e., SMTP, IMAP, POP, etc.) is the total connections, not, say, the total number of users that are connecting. So if the IMAP tab displays a "7", that means there's 7 total IMAP connections, which could be from 1 or more users.

When viewing user connections, and depending on the tab being viewed, the following columns are available:

- • User - The address of the user connecting.
- • Enabled - Whether a particular protocol is enabled for the user. A checkmark means the protocol is available for use by the user.
- • IP Connections - The number of connections from an IP address for the user listed. Multiple connections can occur when a user is connecting to their account via email clients spread across multiple devices.
- • Duration - The length of time the user has been connected to the webmail client.

- Last Login - The date and time the user last logged in using the protocol being viewed.
- Last Authenticated IP - The last IP address used to authenticate the user.

The following buttons/actions are available, regardless of which tab is being viewed:

- Refresh - Refreshes the list of online users.
- Actions (□) - Additional actions are available via this dropdown:

- Drop Connections - End the selected user's session.
- Resync Devices - Forces the user's account to re-sync across their various devices, for all protocols (All tab) or for just an individual protocol (when on that protocol's tab).
- Modify [Protocol] Access - When viewing a particular protocol tab (e.g., XMPP), this enables the protocol for the selected user.
- Disable [Protocol] Access - When viewing a particular protocol tab (e.g., XMPP), this disables the protocol for the selected user.
- Modify Protocol Access - When viewing the All tab, this is used for granting or removing specific protocol access for several users at a time.
- View Authenticated IPs - Opens a modal window that shows all IP addresses who have authenticated that account for the particular protocol.

Regarding connections that appear to last longer than they should, this could be due to a number of reasons. For example, SMTP connections that stay active for hours could be due to multiple people connecting from behind a firewall. These people all appear to connect from a single IP, but they're actually individual connections, one for each user. The firewall simply portrays the connections as being from a single source. In addition, some numbers may always show up as 0. For example, EWS and MAPI tabs will only show connections when users connecting via those protocols are actually attempting to connect and are pulling or pushing a sync. MAPI and EWS don't IDLE like EAS or IMAP, so the numbers will fluctuate or possibly show 0.

User Statuses

Domain administrators can use this section to monitor several statuses for each user on the server. Monitoring these statuses can show administrators where there are issues, or inform them of why a particular behavior is occurring. For example, if a user complains of slowness, it could be due to the mail account being indexed. If a new user is missing email, it may be due to it still being migrated into SmarterMail.

When viewing user statuses, the following columns are available:

- User - The full email address of the user.
- Authentication - The type of authentication being used, such as Active Directory or

SmarterMail (user/password).

• Two-Step Authentication - Whether Two-Step Authentication is enabled for that user.

• Enabled - Whether the user is enabled for their domain.

• Migrating - Whether the user is still in the process of migrating to SmarterMail.

• Indexing - Whether the user is indexing.

• Authenticated Connections - The number of logins, across various protocols, the user has.

• Password Changes Disabled - Whether the user is able to reset their own password or not.

• Password Violations - The number of times the user has created/used a password that violates the administrator's password policies.

• Password Expired - Whether the users password is expired.

Actions

The following actions can be taken:

• Refresh - This button refreshes the list of online users.

• Actions (☐)

• Reindex - This action will start reindexing the selected user(s).

• Expire Password - This action will cause the selected user(s) to have to reset their password on next login.

• Export to CSV - This action will export a list of selected users to a CSV file that can be opened/used in a spreadsheet applications like Microsoft Excel.

General Domain Settings

This settings page is only available to domain administrators and system administrators with the proper permissions.

Below are the Domain Settings available for managing and configuring a domain as a domain administrator. The following options will be available:

Jump To:

• Domain Aliases - Add an alternate domain name for users on the domain

• Marketplace Help for Domain Administrators

• User/Alias - Adjust settings that apply to users and user aliases for the domain

• Authentication Providers - Select Active Directory or LDAP as the authentication provider for users. If no authentication method is set, username/password authentication will be used.

• Folder Auto-Clean - Add settings that affect the auto-clean rules set for users' default folders.

• Calendar Auto-Clean - Add settings that affect the auto-clean rules set for users' calendar entries.

• Online Meeting Video / WebRTC - Set up alternate STUN/TURN server(s) for online meetings

• Custom Help - Add a custom Help link to the Logout menu

• Webmail Login - Customize the login page for your domain

• Footer - Add a message footer that appends all outgoing messages

• Email Signing - Protect users from phishing schemes and spam attacks

• Attachments - Set exclusions and inclusions for particular file types that can be attached to messages.

• External Senders - Enables or disables additional text to be added to messages when received from external domains.

• Mailing Lists - Set the Bounces Before Removal threshold for mailing lists

• Block Authentication by Country - Select the country(-ies) you want to block or allow authentication attempts from.

Domain Aliases

A domain alias is basically an alternate domain name for one that already exists in SmarterMail. Domain aliases are useful, as they allow companies with multiple domain name extensions to receive any email sent to any one of their domains. For example, imagine you have a domain, 'example.com' with a user configured under 'user@@example.com'. By adding a domain alias for 'example.net', any email sent to 'user@@example.net' will be delivered to 'user@@example.com'. Note: You must own the domain name in order to create a domain alias. In addition, messages cannot be retrieved with a domain alias email address unless the domain is properly registered at a domain registrar and its DNS configured.

Creating a Domain Alias

To create a new domain alias, click New Domain Alias . Then enter the name of the alternate domain. The name will be used to create the domain alias email address. For example, if the name of the alias is "example2.com", the domain alias email address will be user@@example2.com. Note: By default, before a domain administrator can save a domain alias, SmarterMail will check that the mail exchange record for the domain is pointing to the server. This prevents domain Admins from "hijacking" mail from valid domains. For example, if this check were not in place, a domain admin could add a domain alias of example.com. Then, any mail sent from the server to "anything@@example.com" would go to the domain with the example.com domain alias, rather than to the actual domain. Alternatively, system administrators who impersonate a domain will see an option when adding a domain alias on whether to verify the MX record before saving.

Marketplace Help for Domain Administrators

The Marketplace offers SmarterMail domain administrators a range of add-ons that enhance and extend SmarterMail's functionality. These add-ons include document collaboration tools, chat applications, AI integration, communication platforms, and more. Marketplace streamlines management by providing tools and functionality that require minimal configuration. Domain Administrators can create a more efficient and tailored email and collaboration platform for their teams.

Key Benefits:

• Greater Customization: Adapt the SmarterMail environment to fit the domain's specific operational needs.

• Simplified Management: Easily access tools and features without complex configurations.

• Enhanced User Experience: Provide end-users with additional capabilities such as document sharing, chat functionality, and more.

Visit the Marketplace help topic for full details.

User/Alias

This feature is only available when using SmarterMail Enterprise.

• Force two-step authentication - Two-Step Authentication is a method of providing a second way to verify account ownership before a user can log in or connect to third-party clients and/or devices. For example, when a user has set up Two-Step Authentication, the SmarterMail login page will require their primary password and a secondary verification of ownership before they can log into webmail. The second method of verification will be provided to the user through popular authentication apps, like Google or Microsoft Authenticator, or through a recovery email address. When this feature is enabled for a domain, the domain administrator can choose whether to Enable or Force Two-Step Authentication for their users - With Enable, users can choose whether to implement Two-Step Authentication whereas with Force, users MUST use Two-Step Authentication.

• Show calendar availability for all users in domain - This setting is enabled by default and allows SmarterMail to alert users of any scheduling conflicts when adding a member of the Global Address List as an attendee on a calendar appointment. In addition, this allows users to view an Availability window to review the times that their attendee is free/busy. When disabled, domain users' scheduling information will not be displayed in the appointment window.

• Allow users to edit their profile - When enabled, this allows users to manually edit their profile information. (I.e., modify their Display Name, contact information, etc.) It also makes the "Allow users to opt out of Global Address List" setting visible. Note: For Active Directory

administrators, or companies who use Active Directory for user administration, this setting can be disabled for all users in Domain Defaults, which means any profile information is "read only" for users and, instead, managed by Active Directory.

• Allow users to opt out of Global Address List - The Global Address List (GAL) is basically a listing of all users who have accounts for your particular email domain. However, not all accounts would necessarily need to be listed in the GAL. For example, generic addresses like info@@ or support@@ may not need to be listed as they're used for specific purposes (e.g., support@@ being imported into a ticketing system.) Note: MAPI requires use of the Global Address List (GAL) in order to work properly. Therefore, regardless of whether the domain's Global Address List feature is disabled, or a user/alias has Show in GAL disabled, Outlook MAPI will always show the GAL directory and be available via autocomplete when typing in a recipient's email address.

• Allow users to bypass spam filtering for unverified trusted senders - This will allow users to add in email addresses they want to bypass DKIM, SPF, and DMARC checks. DKIM, SPF, and DMARC form the backbone of the email verification checks SmarterMail performs. If a domain fails one of these checks, SmarterMail will mark it as potentially unverified. However, users can be confused if a "Trusted Sender" still shows as unverified, or if a message from a "Trusted Sender" ends up in their Junk folder. By bypassing the core spam checks for a sender added to this list, emails from these senders will always reach the user's inbox. Note: Enabling this setting is NOT recommended.

• Catch-all Alias - This allows a domain administrator to select an alias as a "catch-all" account. This means that any messages sent to any unknown address at the domain will be delivered to this alias. This includes ßmistyped addresses as well as addresses that simply don't exist. Note: Use of a catch-all is NOT recommended as it can lead to a massive increase in accepted spam-type messages and can lead to disk space issues.

Authentication Providers

By default, SmarterMail uses an internal username/password authentication type for new users. However, SmarterMail can also intreact with Microsoft's Active Directory (as a one-way sync: Active Directory → SmarterMail, not vice versa), as well as LDAP. If a domain administrator wanted to enable AD authentication or LDAP, they'd want to add a New Authentication Provider and fill in the following information:

• Type - The type of authentication provider being set up: Active Director or LDAP.

• Name - Enter or adjust the username to authenticate against.

• Server Address - The Active Directory or LDAP server to be used.

• Port The port to use for the connection to the server. This defaults to port 389.

• Encryption - Select the encryption method to use for connecting to the server. This can be

None (plain text), SSL/TLS, or StartTLS. When selecting an encryption type, the proper port to use will automatically populate.

- Domain Name - (Active Directory) The domain name used for AD authentication.
- Organizational Unit - (Active Directory) The name of the Organizational Unit of the users. (Not required.)
- Base DN - (LDAP) The string used to connect to the server being authenticated against.
- Username - (LDAP) The username of an account with administrative privileges for the authenticating server.
- Password - (LDAP) The password associated to the username entered.
- Save Credentials (LDAP) Toggle this to save the credentials entered above.

Folder / Calendar Auto-Clean

Setting up auto-clean rules for email folders and for calendars is a simple, yet effective, way to limit how much of the domain's disk space is taken up by users' default folders and their calendar appointments. By placing limits on these areas, or by automatically deleting mail and/or appointments older than X number of days, you can help ensure that your domain disk space does not fill up unnecessarily. In addition, if you want to set a size limit on a folder for users, their messages are deleted in the order that they were received so that older messages get deleted first. The same holds true for calendar appointments.

- Allow users to override auto-clean settings - Enable this setting to allow users to override the domain policy and create their own auto-clean rules.
- Override auto-clean settings - Enable this setting to override the settings established by the system administrator, allowing you to create your own rules. Any changes you make will not be affected if the system administrator changes their policy, unless they disable domain overrides.

If "Override auto-clean settings" is off, the auto-clean rules created by the system administrator will be displayed at the bottom of this card. (If no rules were created by the system administrator, a note saying such will be displayed.

However, if "Override auto-clean settings is turned on, you're presented with a New rule button that will allow you to create your own rule(s) for domain users. Auto-clean rules can be created for any default mail folder, and can be created based on a message's age, the length of time a message has been in a folder, or a particular folder's size.

Size of Folder vs. Age Rules for Folder Auto-Clean

It's possible to set an auto-clean rule either based on the size of a folder, or the age of a message (or messages) within a folder. Size-based auto-clean rules are run whenever an action is performed on a particular folder. For example, moving a message into the folder. Once that action occurs, the auto-

clean rule is run, and it runs each time an action is performed. Age-based rules, however, run once per day, on the FIRST folder action for that day. For example, deleting an email first thing in the morning. When you delete an email, it's moved to the Deleted Items folder, which is a folder action. At that point, if there's an age-based auto-clean rule for the Deleted Items folder, the rule is run and then is silent until an action is performed on the next day. If no action is performed on a folder with an age-based rule, the rule still runs automatically shortly after midnight, server time.

When using a folder's size, it's possible to set upper and lower limits for the space used for the folder. For example, you can create an auto-clean rule so that when a folder gets larger than 50MB in size, the rule automatically deletes messages to reduce the folder's size to 5MB. When freeing up space, the total size of each message is used, which includes any message attachments.

When using Age as a guideline, there are two types of age: Message Age and Age in the Folder.

- • Message Date: This is based on the initial receipt date of the message. So if you received a message on January 1st, and the number of days is set to 14, on January 15 the message is automatically deleted.
- • Time in Folder: This is based on when a message is actually moved to the folder that has the auto-clean rule configured. The age of the message itself is not used. That means, if the Age in Folder is set to 14 days, it doesn't matter when the message was received. Instead, the message is deleted 14 days after it's been moved into the folder.

Online Meeting Video / WebRTC

This feature is only available when using SmarterMail Enterprise.

SmarterMail's online meetings use Web RealTime Communication (WebRTC) for peer-to-peer audio and video chat. WebRTC is an open standard that uses plugin-free APIs to connect web browsers (WebRTC compatible web browsers, that is) for the transfer of voice, video and general data.

For most people, using online meetings, without making any changes, is perfectly fine. This is because online meetings use a default STUN service to assist with the transfer of the data from user-to-user. However, larger or more complex networks may have restrictions that limit, if not fully deny, WebRTC requests. For example, the use of firewalls or the use of Network Address Translation (NAT) on routers. In these cases, using a standalone STUN or TURN server may be necessary.

There is an additional benefit to using a secondary STUN/TURN server: when using SmarterMail's STUN/TURN, the maximum number of video participants is 9 (8 + the organizer). With an external STUN/TURN server, that number jumps to 16 participants (15 + the organizer).

To add a separate STUN/TURN server for a domain, simply click the New STUN/TURN Server button. Once you do so, you'll be presented with the following:

- Type - Whether you're adding a STUN or TURN server.
- URI Paths - These are the paths to the STUN or TURN server you're setting up.
- Username - When setting up a TURN server, this is the username used to connect to that server.
- CredentialL - When setting up a TURN server, this is the "password" for connecting to that server.

While STUN servers are very inexpensive for a company to operate (they're basically a glorified "What's My IP" service), TURN servers can consume a significant amount of bandwidth. Therefore, a TURN server may require you to use a paid service to host it for you. Companies like Twilio or Xirsys offer such services. If you want to host your own TURN server, one of the most popular options is Coturn , a Linux-based TURN server. Note: These are simply examples, and are NOT endorsements of any product or service mentioned.

Custom Help Note: This section will only be visible if the system administrator has enabled Login Display Customization for the domain.

- Custom Help URL - Entering a full URL in this field will add a custom button to the Help menu that users can access in the SmarterMail interface. Administrators can link to a variety of things, including server-specific instructions for syncing, help resources, contact information, etc.
- Custom Help Text - The hyperlink text for the custom URL in the Help menu. note: If no text is entered in this field, the hyperlink text in the Help menu will default to "External Help".

Webmail Login

Domain administrators can customize the SmarterMail login page for their domain to add a company logo, provide additional branding text, or simply adjust the default "Login to SmarterMail" text to be more in line with an overall brand message. Note: This section will only be visible if the system administrator has enabled Login Display Customization for the domain. Furthermore, if the system administrator allows a domain to override the custom login display and the domain administrator does not enable customization for their domain, users will see the default SmarterMail login screen, regardless of whether the system administrator has enabled a custom login display for the server.

- Logo Image - Upload an image, like a company logo, by dragging and dropping a file in the highlighted area or clicking to browse for a file (max file size of 3mb). Uploading an image using this upload control will host the image publicly on the server and enter the tag in the HTML section. Note: Uploading an image here alone will NOT display the image on the login screen. The HTML must remain in the Login Page HTML section. This upload control can be used by those who don't have their logo publicly hosted or who wish the

image source to point back to their mail server. Furthermore, regardless of the image uploaded, the image's source URL will remain the same; only one image may be hosted at a time.

• Custom Login Text - Use this setting to customize the login page header to something more in line with an overall brand message. If Custom Login Text is left blank, SmarterMail's login page will show the default text "Welcome to SmarterMail".

• Custom Title Text - Use this setting to customize the title of the login page to something more in line with an overall brand message. If Custom Title Text is left blank, SmarterMail's login page will show the default text of "SmarterMail" in the browser tab title. Note: Users will see this text on the login page only, with their email address displayed as the browser title for all other pages.

• Enable custom login page HTML - Enable this setting to use HTML to further modify the login screen to add additional text or adjust the layout.

• Login Page HTML - Enter the custom HTML that will be used to further modify the login screen (in-line custom CSS can be used as well). note: To include white space around the Image for Login Screen, the div id "companyinfo" must be included. In addition, domain administrators cannot enter scripts as this is considered to be unsafe code; however, system administrators do not have this limitation.

• Preview Login - This button will open a small preview in a pop-up window of the login customizations you've made without you having to save your changes and test it yourself.

Footer

If the system administrator has enabled footer customization for the domain, domain administrators can configure server-wide message footers that SmarterMail will append on all outgoing messages, forwards that do not already have a footer, replies to messages and emails sent to a mailing list from SmarterMail, if enabled. Although similar to signatures, message footers are typically used to convey disclaimers or provide additional information. For example, a domain administrator may want every message to include a notice that the message was scanned for viruses or the text "Sent by SmarterMail." Note: If the system administrator has a footer configured and enabled for all messages, incoming messages will use that footer. If the domain footer is the only one being used, it is only appended to outgoing messages.

The following options will be available:

• Override footer settings for this domain - Enable this setting to customize the footer for your domain.

• Enable footer for all messages - When enabled, all messages — new messages as well as replies and forwards — will have the footer appended. When disabled, only outgoing messages will have the footer appended.

• Apply to mailing lists - By default, footers are not applied to emails posted to mailing lists. To add the footer to mailing list emails, enable the setting. note: Mailing lists have their own configurable footers. If a custom mailing list footer is already configured, enabling this option will append a second footer at the end of each message posted to the mailing list subscribers. Because this may be confusing for mailing list moderators and recipients, most administrators will choose to keep this option disabled.

• Footer - Use this section to create the message footer text. Clicking the edit icon will open a modal that includes an HTML-based editor, allowing admins to create footers that seamlessly fit into any email message. note: The message footer does not support the use of variables.

Email Signing

Email signing protocols, such as DKIM (DomainKeys Identified Mail), can help protect users from phishing schemes or spam attacks by using cryptography to verify the authenticity of an email. This ensures the message came from your server and was not altered in transit.

To enable DKIM Signing in SmarterMail:

• Click the Enable button. SmarterMail will display a unique Text Record Name and Text Record Value.

• Contact your DNS provider to add the TXT record to your DNS server. If you are using a subdomain, you may need to modify the TXT record name to point specifically to that subdomain, especially if your DNS control panel does not automatically handle this for you.

• After the TXT record has been added, click the Enable button again. SmarterMail will attempt to verify the DNS settings, and if successful, DKIM Signing will be enabled.

To view the Text Record Name and Value, click on View Record . To adjust the mail signing settings, click the Settings button. Note: In most cases, these settings do not need to be altered. However, in the event that you would like to specify how closely you want the system to monitor messages in transit, please refer to the DKIM documentation linked below.

• Key Size - The length of encryption key to use. 2048 is recommended. note: Changing the Key Size will require a new DNS entry. This is the only email signing change that requires a new DNS entry.

• Max message size to sign (MB) - This is the largest message size you want to sign using DKIM. DKIM generates a "hash" on the email up to the size limit. Generating the "hash" could be an expensive operation, especially if the domain sends large messages all the time. Limiting it means not having to process the whole message — It would only grab the bytes up to the size limit and sign that.

• Body Canonicalization - The method used to monitor in-transit changes to the body of a

message. Two canonicalization algorithms are defined for the body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping. For more information, please visit https://dkim.org/specs/rfc4871-dkimbase.html#canonicalization .

• Header Canonicalization - The method used to monitor in-transit changes to the header of a message. Two canonicalization algorithms are defined for the header: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping. For more information, please visit https://dkim.org/specs/rfc4871-dkimbase.html#canonicalization .

• Header Field to Use - The header fields included in the hash algorithm. This is further defined by header fields. For assistance in determining the header fields to sign, please visit this Wikipedia page .

• Header Fields - The header fields included in the hash algorithm. note: List only one header field per line break.

Setting Up Email Signing

Setting up email signing and creating the fields necessary to add DKIM to a domain's DNS record is simple within SmarterMail.

• Make sure you're logged in as a Domain Administrator .

• From the list of domains, pick the domain you want to set up Email Signing for.

• Head over to Domain Options , then click on the General tab.

• Look for the Email Signing card.

• Click the Enable link on that card, a modal window will open, and it will contain the text necessary for adding the DNS record. This window contains two important pieces of information: the Text Record Name and the Text Record Value . The Text Record Name contains the DKIM selector , which is the value that precedes ._domainKey . For example, ve8DD7862860859EE . The selector can be used to verify that your DKIM record is set up correctly. (When the Text Record Name is added to DNS, the ".domain" should automatically be appended by DNS.) The Text Record Value is also the public key that's created by the SmarterMail server. Therefore, it's the encrypted key that pairs to the private key that's stored on the mail server. This is why it looks like a random series of characters.• Make any changes you want and click Save . If no changes are made, simply click the Cancel button.

• Now that you have the Name and Value for the TXT record, you will want to log in to your DNS provider and create the actual DNS record. How you do this depends on who your provider is. In general, the DNS TXT record format will be as follows:

Email Signing ?

To finish activating the DKIM signing key, the TXT record below must be added to your DNS server.

Key Size
2048 (Recommended) ▾

Activation
Wait for DNS verification ▾

TXT Record Name
ve8DD7862860859EE._domainKey ⧉

TXT Record Value
v=DKIM1; k=rsa; h=sha256; p=MIIBIjANBgkqhkiG9w0B ⧉

Cancel   Save

• NAME = Text Record Name, which will be something like ve8DD7862860859EE._domainKey

• TYPE = TXT

• VALUE = Text Record Value, which contains the public key created by SmarterMail note: As this is a change to DNS, it may take a few hours for the record to propagate for the domain. Generally that propagation is pretty fast, but it could take 24 hours or more.

Adding a Rollover Record

A Rollover Record is a secondary DKIM record that can be created, and used, as the needs of a business change. Some suggest periodically changing DKIM as a good security practice because DKIM keys are public. In this case, a rollover DKIM record can be created and published to DNS as needed. After the rollover key is created and added to DNS both keys will be used for a period of time. Once DNS verification occurs on the rollover key it becomes the "Active" key in SmarterMail and the old key is removed automatically. Administrators can then remove the old TXT record from DNS.

Validating Your DKIM Record

Once you've made the changes to your domain's DNS, it can take a few hours for those changes to take effect. To test whether you're set it up properly, you can do a search for DKIM record validation or use a site such as MXToolbox . MXToolbox makes DKIM validation simple; you just need your domain name and the selector. The selector is what comes before the "." in your Text Record Name. So if your Text Record Name was ve8DD7862860859EE._domainKey , the selector is ve8DD7862860859EE . Enter those into their form, and they'll let you know a) if the record can be found, and b) if it's valid.

Attachments

Inbound Extension Blacklist - This list allows you to limit the file types that can be attached to emails sent to users on your domain. For example, many email administrators won't allow executable files (EXE) as they can cause issues on the mail server, and possibly across an entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .exe or EXE)

Outbound Extension Blacklist - This list allows you to limit the file types that are users on your domain are allowed to send out of the mail server. For example, many email administrators won't allow batch files (BAT) as they can cause issues on the recipients' mail server, and possibly across their entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .bat or BAT)

External Senders

Some organizations, for example those in banking or finance, want to ensure their users are aware when they receive emails that are from an outside source: external domains, external companies, free email services, etc. They like these extra precautions so that users are wary of clicking links or opening attachments that come from outside their own company as there's no guarantee the links or attachments aren't phishing attempts or items that may compromise the user's account, much less the organization itself. That's where "external sender" notifications come in handy. These notifications make it very clear that messages DO NOT originate from within the company.

- Add text to body - When enabled, this will add a text box to the body of the message that cautions the recipient that the email originated outside their own domain, and to take caution when clicking links or opening attachments.
- Add text to subject - When enabled, this adds the text "[EXTERNAL SENDER]" to the subject line of the message.
- Known External Domains - If there are trusted domains — that is, domains that an organization knows and is comfortable with — they can be exempted from any External Sender text. For example, emails from trusted vendors can bypass the external sender text if their

domain is entered as a "Known External Domain". Domains should be entered one per line, and they should include their domain extension (e.g., .com, .net, etc.).

Mailing Lists

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. Unlike an Alias, a mailing list allows people to subscribe to, or unsubscribe from, email communications. In addition, mailing lists can be public or private, be replied to by all users or managed by a single list moderator and more. Use this card to specify the following mailing list setting:

• Mailing List Command Address - This is, essentially, the "To" address for your listserv. If someone wants to subscribe to a list, for example, they'd email listserv@@your-domain.com with the listname and the word "subscribe" in the body of their message. They'd then be subscribed to that mailing list.

• Bounces Before Removal - The number of times a message to a specific subscriber can bounce before the subscriber is automatically removed from the mailing list. By default, this number is 2.

• Enable threshold for bounce removal - When enabled, domain administrators can add a timeframe that corresponds to when a bounce is added to the number of "Bounces Before Removal" total. For example, if the setting is set to 14 (days), and "Bounces Before Removal" is set to "2", any 2 bounces within those 14 days will remove the subscriber. If a bounce comes in at day 20, it's not counted towards the "Bounces Before Removal" total.

• Command help email - This is the emails that's sent when a subscriber emails the list requesting 'Help'. Domain administrators can edit this message as they see fit. Note: This card will only be displayed if Mailing Lists are enabled for the domain.

Block Authentication by Country

Part of a domain administrator's job is making sure bad actors can't access their domain or attempt to brute force logins to user accounts. Much of this prevention occurs at the system level, but domain administrators also have the ability to add an extra layer of security by blocking authentication attempts from specific countries, or ONLY ALLOW authentication from specific countries. Adding a country to the setting will just block authentication attempts, it won't impact sending or receiving messages from the country. It will simply prevent anyone from the country(-ies) logging into the server, regardless of protocol. In addition, domain administrators won't be able to add their "home" country, which will prevent them from accidentally locking out users. Use this card to specify the following: note: If one or more countries are blocked at the system level, a notification will appear for domain administrators letting them know that "one or more of these settings is controlled by [the] administrator."

• Countries to Block - Use this dropdown to select "Specified Countries" or "All But Specified Countries". When selecting "Specified Countries", authentications attempted from the country(-ies) that are selected will be blocked. When selecting "All But Specified Countries", only authentication attempts from the selected country(-ies) will be allowed. Attempts from any other country will be blocked.

• Country - Use this dropdown to select one or more countries, based on the block type selected.

Chat Search

This settings page is only available to domain administrators.

A major advantage of SmarterMail is that it stores all chats, regardless of whether the chats occur within the webmail interface, using a third-party client or a combination of both. Domain administrators have the ability to perform custom searches by date range, by the users involved in the chat conversations, by specific keywords or phrases used during a chat or a combination of all of these variables.The results can then be downloaded to a desktop or laptop (search results cannot be downloaded to a mobile device due to storage limitations) and reviewed as needed. Note: Chat history search is configured by the system administrator. For more information, see the Features area of the All Domains page of SmarterMail Help.

The options available when performing a chat history search are as follows:

• Date Range - The date range you want to use for your search. You can either type in the date or click on the calendar icon and use SmarterMail's calendar control to select your start and end date.

• User - The username or email address of the person who participated in a chat.

• Name - The Display Name of the person who participated in a chat.

• Text - Any word or phrase that was used during a chat. For example, "2012 sales numbers" or "product ID 33489".

Chat Clients and Encryption

Many XMPP chat clients out these days encrypt the chats that happen between 2 or more users. Unfortunately, this encrypted chat traffic occurs between the client and SmarterMail itself. (Or fortunately, depending on where you fall on the topic of personal encryption.) Therefore, while SmarterMail will see chats occur, it doesn't have the ability to capture and archive the unencrypted text. Therefore, some results returned when you do a Chat History search will appear garbled or show generic text, like this from the XMPP client Gajim: [This is part of an encrypted session. If you see this message, something went wrong.] ([This is part of an encrypted session. If you see this message, something went wrong.])

Content Filtering

Content filtering is a great way for system administrators, domain administrators and/or users to perform actions on incoming emails that meet specific criteria. For example, it's possible to use content filters to delete messages with certain attachments (e.g., attachments with a .exe extension), forward messages from a specific email address to another account, move messages to a certain folder or even alter the subject of a message by appending something to it prior to delivery. While content filters are most commonly used to organize email by moving messages to specific folders, they're extremely flexible and allow you to filter messages the way you want to.

Content Filtering is available to users and domain administrators in the Settings and/or Domain Settings areas. System administrators have a Content Filtering tab available to them for each domain that's managed on the SmarterMail server. In both the Settings and Domain Settings areas, there is a Content Filtering option in the navigation menu that's used to see any existing filters as well as to manage filters. That being said, the filters created are only viewable/editable by the role that created them. That means the domain content filters are only available to domain administrators and users see their own filters. However, any filter created for a domain by a system administrator is available to both the system administrator and the domain administrator.

Once the Content Filtering section is accessed, any existing filters will be listed. Content filters run in order, from top to bottom. In addition, content filters run from top-down: that means that content filters created by system and/or domain administrators run first, then filters created by users. That means that if a message could be managed by more than one, it will be handled by the FIRST content filter encountered. So, if you're seeing weird or unexpected behavior for messages, you may want to re-organize the order of your filters. You do this by moving them by clicking the Up and Down arrows next to the content filter names, moving them up and down in the "order of operations." You may also want to contact your domain administrator to see if they have any content filters created that could be impacting message delivery. Note: Some content filtering actions, such as a Forward action, do not work in conjunction with Plus Addressing as content filters are run BEFORE any plus addressing commands. Using both could lead to duplicate messages or other unwanted/unnecessary behavior. In addition, automatic forwarding is incompatible with certain message types, such as autoresponders and Delivery Status Notifications (DSN). This is to avoid the potential for feedback loops that can cause issues such as the spool filling up.

To delete a content filter, simply select it from the list and click the Delete button.

Create/Edit Content Filters

When adding a content filter, the following cards will be available, each with options pertaining to the conditions you want to use for the rules, and the actions that are taken based on the conditions you set:

General

- Name - The friendly name chosen to describe the rule.
- Match Type - Because multiple conditions can be configured per content filter, SmarterMail provides the option to require ALL conditions to be met or ANY of the conditions to be met in order for the rule's action to be triggered. Select the appropriate option from this list.
- Enable wildcards in search strings (* and ?) - Wildcards can be used to replace a specific word, phrase or character, where a question mark (?) represents a single character and an asterisk (*) represents any text. For example, if you wanted to block sales01@@domain.com, sales02@@domain.com and sales03@@domain.com, you could enter sales??@@domain.com . If you wanted to block all sales addresses, you could enter sales* instead.

Conditions

Click on New Condition to specify the criteria that triggers the rule's action(s). For each condition selected, you will be able to add specifications and enter any necessary details, as required. For example, if you choose to filter on 'From Address', you can enter one or multiple email addresses. If you choose to filter on 'Contains specific words or phrases', you can enter the specific text and choose to look for that text in an email's subject, message body, header, etc.

On many conditions, you also have the ability to reverse the logic of the criteria item by changing the Comparison selection. For example, imagine you only want to accept email from specific domains. You would choose the 'From specific domains' condition and set the Comparison field to 'Does Not Match". Any messages sent from domains that do not match what you've entered in the text box can be deleted. Note: If you select a condition that requires a value to be entered, and the field is left blank, SmarterMail will ignore this rule.

The following conditions are available, separated by Condition Type:

From Address

This condition allows you to select whether you want to run the filter against specific addresses or domains, or trusted senders. Then, you set the comparison type: whether the field matches or doesn't match the condition type. Then, you enter in the addresses or domains you want to use for the filter. The fields to use include:

- From specific addresses
- From specific domains
- From trusted senders

Contains Specific Words or Phrases

This condition allows you to look in various areas for words or phrases, then take action when those words or phrases are found. You can set the comparison type, whether the words/phrases are found or not, and then the words or phrases you want to use for the filter. You can further refine a phrase search by enclosing the phrase in quotation marks. (The same can be done to individual words.) The fields to use include:

- Subject
- Body
- Subject or Body
- From Address
- To Address
- Email header
- Anywhere in message

To Address

This condition allows you to look in the To: or Cc: fields for specific addresses or domains. You can set the comparison type, whether the address or domain are included in the selected field, then the addresses or domains you want to use for the filter. The fields to use include:

- To specific addresses
- To specific domains
- Only to me
- My address in to field
- My address not in to field
- My address in to or cc field

Attachments

This condition allows you to filter emails based on whether or not messages have attachments, or even by specific filename, extension type, or file size. The fields to use include:

- Has any attachment
- Specific filenames
- Specific extensions
- Over specific size

Other

This condition allows you to filter based on a number of different criteria, including flag type, message size, spam probability, etc. The fields to use include:

• Flagged as high priority

• Flagged as normal priority

• Flagged as low priority

• Message automated (no return address)

• Sender authenticated

• Message over size

• Message under size

• Received in date range

• Sent through a specific server (by IP address)

• Spam probability

Actions

Click on New Action to specify what should occur when an email triggers the content filter condition(s). note: If you select an action that requires a value to be entered, and the field is left blank, SmarterMail will ignore this rule.

The following actions are available:

• Delete message - Deletes the message so that it will never arrive at your Inbox. Note: Messages deleted through content filtering cannot be recovered.

• Bounce message - Sends a message back to the sender of the email saying that the message was bounced, and not delivered. Note: If the system administrator has disabled bouncing, the sender is never notified and the message is simply deleted.

• Move message - Delivers the incoming message to the folder you choose from the dropdown list. note: If you later delete that folder and leave the content filter active, the filter will automatically create the folder when the action is triggered.

• Add Header - Adds an email header within the incoming message, which can be useful when performing additional filtering through Outlook or other email clients. Headers should be formatted like "X-someheadername: value"

• Add Text to Subject - Appends a prefix to the subject line of the email. This is useful for categorizing emails as the subject line will be altered to include the text you specify in the text box.

• Forward message - Forwards a copy of the message to another email address and leaves you a copy of the message as well.

• Mark as read - Automatically marks the messages as read, which means it will not show up in your inbox, or any other folder, as unread.

• Set Priority - Automatically elevates the priority of a message. For example, if you create a content filter that flags a message from a VIP, you may want to set the priority of the message

to High as well to denote its importance.

• Flag message - Automatically flags the message for follow-up. This makes it easy to find messages that have been acted upon by your content filter.

Manually Running Filters

Users can manually trigger one or more of their content filters to run against a specified email folder. The ability to run content filters on-demand is a convenient way to clean up the mailbox, as actions can be performed on EXISTING emails rather than incoming email only.

It's possible to run a content filter on a specific folder simply by selecting the folder name and the selecting Run Content Filter from the Actions menu icon that appears at the bottom of the SmarterMail interface. (It's to the right of the folders icon.) Once selected, a modal opens and you are able to select the content filter to run from the dropdown, then clicking OK . The filtering process may take some time to complete, but you may continue to work while the process runs in the background. When the filtering process has completed, an Action Succeeded toast notification will appear within the Email section.

Important notes regarding on-demand filters:

• The 'Sent through specific server (by IP address)' and 'Sender Authenticated' conditions as well as the 'Bounce message' action cannot be used when manually running a content filter. If a filter contains one of the restricted actions or conditions as its only action or condition, the filter should be triggered manually. If a filter contains one of the restricted actions or conditions along with other actions or conditions, please note that the restricted action or condition will be omitted from the filter process.

• The 'Delete message' action will immediately purge the email from the system. Without Message Archiving enabled, these messages may not be recoverable.

• The 'Prefix Subject' action must re-write the message. It will attempt to timestamp the new message with the date from the message header. However, if the date cannot be parsed from the message header, the re-written message will show the current time.

• The 'Trusted Senders' condition will look for Current trusted senders. It cannot look for messages from trusted senders that were configured at the time the message was delivered.

• Running content filters on-demand executes the filters in the order they appear. However, the on-demand process does not loop through messages multiple times to perform the filter actions. Instead, it will gather all of the actions it could run on the message first and then runs them in the order they would have been found.

• When there are multiple actions for one filter, the actions that don't require a re-write of the message will be done first. For example, a message will be marked as read before it is moved to another folder.

Domain Events

This settings page is only available to domain administrators and system administrators with the proper permissions.

The Event system in SmarterMail is an incredibly powerful and flexible tool that allows domain administrators to automatically perform actions based on specific criteria and remain up-to-date with what is going on with the SmarterMail server and user accounts. SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to users that need the information. For example, domain administrators can automatically add an additional recipient on messages sent or received by users on the or receive notifications when a task is due or their domain disk space has met a certain threshold.

When creating a new event for a domain, the following options will be available:

General

- Event Name - The friendly name of the event.
- Event Status - New events default to a status of Enabled. However, to temporarily stop an event from triggering, you can change the status to Disabled.
- Event Category - The feature to which the event pertains: User, Mailing List, Alias, Throttling, Email or Collaboration.
- Event Type - The occurence that triggers the event. Each category has several specific event types that can trigger the action.

Conditions

Each event type has its own corresponding conditions. The global conditions that are seen across all event types are listed below.

- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.

Actions

Each event type has its own corresponding actions. The global actions that are seen across all event types are listed below.

- Show a notification - This option will display a notification to the Notifications window. It can also send a popup browser notification.
- Send an email - This option will send an email to the specified address.

A Practical Example: Receive an Email When a New There's a New Subscriber to a Mailing List

This practical example of setting up an Event is the result of an old knowledge base article we had. It details how to set up an event that sends an email to the list moderator when a new person subscribes to that List Moderator's mailing list. As an aside, while this is an example of setting the Event up as a domain administrator, the process for setting it up as the list moderator is very similar.

- Log into SmarterMail as the domain administrator.
- Go to the Events area. A list of existing events will load.
- Click the New button.
- On the General card, do the following:.

- In the Event Name field, type a descriptive friendly name for the event.
- In the Event Status drop down, select Enabled.
- In the Event Category field, select Mailing.
- In the Event Type field, select Mailing List Subscribe.
- On the Conditions card, a new Condition is possibly already there. This is perfectly fine. However, since we want to be notified when a new person subscribes to a specific mailing list, you'll want to click the New Condition button. Then do the following

- On the Condition modal, select Mailing List Address from the dropdown, then enter the full address for the list. (E.g., testlist@@example.com)
- Click the Save button to add the new Condition.
- On the Actions (…) card, click the New Action button. Then do the following:

- On the Actions (…) modal, select Send and email from the dropdown.
- The modal will change, allowing you to select your Frequency, From Address, To Address, Subject, etc. then add the email contents that will be sent. Your To Address should be the List Administrator. You can leave the email's content the default that's filled out or edit it how you see fit.
- Click the Save button.
- Your new Event is pretty much finished. Just click the Save button to actually save the Event so that it can run.

Message Archive Search

This feature is only available in SmarterMail Enterprise edition.

Message archiving is a method of storing all email traffic for a domain — either incoming messages, outgoing messages, or both — in a separate location on the mail server. Typically, this is a feature

used for companies that need mail servers to be in compliance with certain regulatory guidelines, such as the Sarbanes-Oxley Act of 2002 .

When archiving is set up, messages are automatically archived as soon as they hit the spool and before they are handled by any spam and/or content filters. This means that all messages are archived, not simply those that are delivered to a user's mailbox. (The exception to this rule is messages rejected due to SMTP Blocking. If a message is rejected due SMTP Spam blocking, it will never hit the spool and, therefore, will not be archived.) On a nightly basis, SmarterMail zips up archived messages and stores them to conserve disk space on the mail server. However, zipped messages are still searchable.

By default, SmarterMail does not archive any messages. To specify which domains are archived, the system administrator will need to create archiving rules. Rules can be set up for the system as a whole, so all domains are archived, in the system's General settings, or archiving rules can be set up on a domain-by-domain basis on each domain's Configuration tab.

Search Results

If message archive searches have been performed, they'll be listed when navigating to this page. Otherwise, this page will be blank and a new search needs to be initiated. If there are searches that have been completed, you will see the following:

- Summary - Here, the general details of the search is listed. This includes the search parameters including things like whether the search is for "messages sent to:" a particular user, "messages sent by:" a particular user, the domain or user, and the dates searched.
- Matches - The number of items than matched the search parameters.
- Status - Whether the search completed or not, and date and time the search was performed.

Each set of results can be viewed by simply clicking on it, and the results are displayed. Searches can be manually deleted as well by simply selecting a search and clicking the Delete button.

Searching Message Archive(s)

When performing a message archive search, the following search strings will be available: filter for all domains or a specific one, date range, the sender's address, the recipient's address or the subject.

SmarterMail's archiving feature saves any inbound message, outbound message, or both, depending on the Rules that are set up for the domains. That means any spam message, junk message, messages that are eventually deleted, etc. are all saved. That means the ability to find messages, and then perform some action on those messages once found, is extremely important. This is especially true in environments that have compliance guidelines that need to be followed.

When message archiving is set up for a specific domain, that domain's administrator can find a Message Archive Search within the domain's Settings . System administrators can search across any and all domains, regardless of the Rules that are set up. Regardless of whether a domain administrator or system administrator is performing a search, the following is available for search criteria:

• Start and End - The start and end dates for the search.

• From - The email address the message is sent from.

• To - The email address the message is sent to.

• Subject - A word or phrase that would be in the subject line. If a person wants to find all messages From or To a particular address, this can stay blank.

After a search is performed, and results are found, there are a few actions that can be taken on one or more of the search results:

• Download / Download All - This will download a copy of individually-selected messages, or all messages. Whichever is chosen a .Zip file gets downloaded. The messages are saved in their original .eml format and can be opened by an email client, email utility or any other standard program that can open emails. Note: Downloads are limited to 2GB in total size. Therefore, if you choose "Download All", should the total size of the .Zip file be over 2GB, the download may not complete. If this is the case, it may be necessary to change your search to limit the results, or break your search up into multiple queries. For example, breaking a full year's search into quarterly searches.

• Copy to Mailbox / Copy All - In certain instances, it may be necessary to move messages to a separate mailbox. For example, in a situation where an outside organization, like an auditing company, requires access to certain messages. In these cases, a separate user can be set up for the organization, and any messages found via Archive Search can be moved to that new user for later review. Messages can even be moved to a specific folder, or specific folders, within that new user so they're contained and easily organized. Individually selected messages can be copied using Copy to All, or all results can be copied using Copy All.

Search Results

Results from archive searches persist for as long as they're needed. Each set of results appears in a grid so they can be retrieved as often as necessary. Once they're no longer needed, they can be closed out, and removed from the list.

Password Requirements

To ensure the security of the mail server and its mailboxes, domain administrators can contribute to the minimum requirements for user passwords. This includes things like setting requirements for how a password is generated (character count, upper/lowercase, etc.) as well as whether passwords expire,

whether previous passwords can be used, and more. Note: The system administrator has the ability to set a baseline for password requirements that all users must follow. When this occurs, those password requirement settings will be disabled for domain administrators while others can be toggled on or off. This allows domain administrators to strengthen password requirements for their users, but they will not be able to reduce the requirements that were set as a baseline.

For example, a system administrator may set some password requirements, such as passwords must have a minimum of 12 characters and require at least number, one capital letter, and one lowercase letter. When these are set, the domain administrator can only add additional requirements (e.g., require at least one symbol), but they cannot remove any of the other requirements.

When accessing Password Requirements , the following tabs are available, and each tab has its own cards:

- Options
- Password Violations
- Expired Passwords
- Password Age

Options

This page allows a domain administrator to modify the baseline requirements set by the system administrator.

Requirements

- Minimum Password Length - Enter the minimum number of characters the password must have.
- At least one number - Select this option to force users to include a number in the password.
- At least one capital letter - Select this option to force users to include a capital letter in the password.
- At least one lowercase letter - Select this option to force users to include a lowercase letter in the password.
- At least one symbol - Select this option to force users to include a symbol in the password.
- May not match username - Select this option to ensure that the username and password do not match.

Options

- Prevent common passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords.

• Prevent previous passwords reuse - Select this option to prevent users from using any previously used passwords. Note: This setting prohibits old passwords from being used indefinitely. It is not based on a time interval.

• Previous Passwords to Block - Some administrators will allow re-use of passwords after a certain amount of time, or after some number of rotations. This number reflects the number of times a new password needs to be used before a password can be re-used. By default, this is set to 0, meaning passwords can never be re-used.

• Skip enforcement for existing passwords - Select this option to skip existing users when making changes to password requirements — meaning the changes will only affect new users or new passwords.

• Enable password retrieval - Select this option to allow users to reset their password if they forget it. Note: In order for users to utilize password retrieval, they must have a Recovery Address configured in their account settings.

Expiration

Password expiration is based on the date/age of the user's current password, NOT when the password expiration setting is enabled. This means that users who have not changed their passwords in a long time will be required to change them almost immediately upon enabling the "Passwords expire automatically" setting.

As an example, let's say you enabled password expiration today and set the threshold to 1 month. This is the expected behavior for the following user scenarios:

• If the user changed their password last week, their password will not be expired. Instead, it will expire in 3 weeks (when the password is 1 month old).

• IF the user changed their password last year, their password is over the 1-month threshold and will be expired immediately.

• If the user was created 2 weeks ago and has never changed their password, their password will not be expired. Instead, it will expire in 2 weeks (when the password is 1 month old).

• If the user was created 2 months ago and has never changed their password, their password is over the 1-month threshold and will be expired immediately.

Initially, "Passwords expire automatically" is disabled. Enabling it offers the following settings:

• Password Expiration (Months) - The number of months that a password is valid. After the specified time, a user's outgoing SMTP will be disabled and a password change will be forced upon Web interface login. Move the slider to the right to enable this setting. Note: If a user's 'Disable password changes' setting is enabled, their password will not expire.

• User Notification Timing (Days separated by commas) - The interval(s) used to notify users of

when their password will expire or when their auto-block grace period will end and, subsequently, their outgoing SMTP will be disabled. The default values are 28, 14, 7, 3, 2, 1 days. This means SmarterMail will send out warning messages to the user to change their password 28 days, 14 days, 7 days, 3 days, 2 days and 1 day before their password officially expires or the grace period ends if their password violates the requirements. Note: SmarterMail will send one, single notification for all missed intervals. For example, imagine "Auto-block Grace Period" is set for 30 days and the "User Notification Timing" is set at 60, 45, 25, 10, 2, 1. When a user is in violation, SmarterMail will send a single notification for the 60 and 45 day intervals then continue as normal at the 25-day interval.

• Disable outbound mail after grace period ends - Select this option to disable outgoing SMTP after the auto-block grace period ends when a user's password does not meet the password requirements.

• Auto-block Grace Period (Days) - Available when the "Disable outbound mail..." setting is enabled. This is the number of days a user can wait to update their password before outgoing SMTP is disabled due to password policy violation. Note: This setting only applies if the "Disable outgoing SMTP when auto-block grace period ends" setting is enabled.

Password Violations

The Password Violations tab offers administrators a way to find users that aren't following the password requirements that have been set up. For any Users who appear on this list, the administrator is able to either email the users individually, or force their non-compliant password to expire. This latter action means that the user will be forced to change their password the next time they log in to their email account. In addition, it's possible to export a list of the non-compliant users in CSV format.

When Users appear on this page, the following information will be available:

• Username - The username of the non-compliant account
• Authentication - The Authentication Mode used by the account: SmarterMail or Active Directory.
• Domain - The domain name that's associated to the Username.
• Password Changes Disabled - If a specific user has the ability to change their password disabled, their user is marked accordingly in this column.
• Violations - The number of password requirement violations encountered for the User.

Expired Passwords

By default, this tab displays all accounts set up for the domain. The numbers displayed on the tab show the number of passwords that have expired over the total number of accounts set up. For

example, that tab may show 10/275, meaning 10 accounts out of 275 total have passwords that have expired. This tab could, of course, also show 0/275 if there are no expired passwords.

Depending on the business rules used for the domain, the domain administrator has some actions that can be performed on each account, which are detailed below. Each account is listed and the following information is displayed:

- Username - The account that is set up.
- Authentication - The type of authentication used for the account, either "Local" or "Active Directory", generally. Local authentication means the account owner set their own password.
- Expired - If the user's password is expired, a check mark appears in this column.
- Password Age - How old the password is. For example, 2 years, 3 days, 15 minutes, etc.

As mentioned, administrators have the ability to take action on users, either users who have expired passwords or users who do not. These actions include:

- Send Email - Opens a modal window that allows the administrator to create, and send, an email to the user(s) informing them that they need to reset their password. However, the administrator can customize the entire message to say what they want.
- Expire Password - Will automatically expire password(s) for the user(s), forcing a change the next time the user attempts to log in.

Password Age

By default, this page will list all users and the respective age of the passwords assigned to each. This allows system administrators to find users who may, due to the age of their password, want to change said password. In addition, it can help find little-used accounts that may be ripe for compromise if their password is over a certain age. Each account is listed and the following information is displayed:

- Username - The account that is set up.
- Two-Step Authentication - Whether the username has Two-Step Authentication enabled.
- Expired - If the user's password is expired, a check mark appears in this column.
- Password Age - How old the password is. For example, 2 years, 3 days, 15 minutes, etc.

Shared Resources

This settings page is only available to domain administrators and system administrators with the proper permissions.

On the Sharing page, administrators have the ability to create Resources, Public Folders, and/or User Groups for all users of the domain.

Resources

Resources are, generally, things that can be, or need to be, scheduled for use. These include:

• Conference Rooms - Conference Rooms are used in conjunction with meetings/events that are created, so they have an "availability" attached to them since they can be reserved. When creating a new event in a calendar, a shared conference room can be selected for the location of that meeting/discussion/event.

• Equipment - Equipment acts similarly to Conference Rooms as equipment can be reserved and used as needed. As such, it has an availability, just like a Conference Room. Therefore, a piece of equipment can be something that would require reservation to use, like a set of lights for a photo shoot, a forklift, or other type of equipment.

When clicking the New Resource button on the Sharing card, the domain administrator is presented with a modal window that contains the following information to be filled out:

• Name - The name of the resource. It's always a best practice to name the shared resource something that will be easily identified by users. For example, if the resource will be a conference room name the resource the same as the room designation. For example, South Conference Room or Main Hall. For equipment, something like "Sony Projector" or similar.

• Type - The type of resource being added: Conference Room or Equipment.

• Users - Here, you'll enter individual users that will receive the share. Enter only the username of the account. (For example, for user account, "jdoe@@example.com", you would enter "jdoe".) Once you begin typing the username, you'll notice a second line appears below where you're typing. This allows you to share the resource with any number of individual users.

• User Groups - User Groups can be selected to give permissions to specific subsets of users on the domain. By default, two groups are always available: Everyone and Admins. If other User Groups have been created, they'll appear in this dropdown list.

• Access Permissions - Next to the usernames you've added, or the User Groups selected, you'll want to set the type of access for each:

• None - This option can act as a negator for permission settings. For example, if you provide access to the Admin user group, you can omit one or multiple of those Admins by entering their name in the Users field and selecting None for their access.

• Manage - This option allows Users or User Groups to fully edit the shared data.

Public Folders

Public folders are items that users generally have access to for their own personal use, but rather than being owned and managed by a particular user, they're created by the domain administrator and can be shared with everyone on the domain, individual users, or even one or more user groups. The primary

difference is that Public Folders are NOT connected to a particular account. Instead, they're attached to the domain as a whole. Any domain administrator can manage public folders, making them more versatile for domain users. Public folders include:

- Contacts - Domain Contacts can include individuals or companies that pertain to certain departments, certain groups of people, or even entire divisions. This helps keeps these types of contacts consistent, and up-to-date, as opposed to each person keeping the contact individually.
- Calendar - Domain Calendars can be used for company-wide events such as company holidays, payroll or PTO schedules. Domain calendars show up as "subscribed" calendars for users and can be displayed/hidden in a user's Calendars area just like other calendars.
- Tasks - Domain Tasks can be things like marketing planning, group projects, or quarterly reporting — basically, any task that entails enlisting one or more individuals or groups of people to complete.
- Notes - Domain Notes can be lists for tasks, meeting minutes, or any other type of note that is collaborated on by more than one individual, or a group of people.

To create a public folder, click the New Public Folder button on the Public Folders card. To edit an existing public folder, simply click on its name. A modal window will pop up with the following options:

- Name - The name of the folder. It's always a best practice to name the folder something that will be easily identified by users. For example, if it's a calendar, it can be named for its use. For example, PTO Calendar, or Release Dates.
- Type - The type of folder being added: Contacts, Calendar, Tasks, or Notes.
- Users - Here, you'll enter individual users that will receive the share. Enter only the username of the account. (For example, for user account, "jdoe@@example.com", you would enter "jdoe".) Once you begin typing the username, you'll notice autocomplete suggestions based on what you've typed. Simply continue typing the full address or select the proper address from the suggestions.
- User Groups - User Groups can be selected to give permissions to specific subsets of users on the domain. By default, two groups are always available: Everyone and Admins. If other User Groups have been created, they'll appear in this dropdown list.
- Access Permissions - Next to the usernames you've added, or the User Groups selected, you'll want to set the type of access for each:

- None - This option can act as a negator for permission settings. For example, if you provide access to the Admin user group, you can omit one or multiple of those Admins by entering their name in the Users field and selecting None for their access.
- Read-Only - This option allows Users or User Groups to see the shared data, but they do not

have the ability to edit the item.

• Manage - This option allows Users or User Groups to fully edit the shared data.

User Groups

User Groups are used when permissions need to be give to specific subsets of domain users in order to access shared resources. For example, if a business wanted to make it easy for members of its Sales Department to share their calendars with other team members, the domain administrator would create a User Group for all the Sales Department employees.

By default, there are permanent user groups that cannot be edited:

• Everyone - All users on the domain belong to this group automatically.

• Administrators - All users that are marked as domain administrators for this domain belong to this group.

To create a new User Group, click the New User Group button on the User Groups card. To edit an existing user group, simply click on the corresponding group name. A modal window will pop up with the following options:

• Name - The friendly name of the user group. For example, "Sales Team".

• User - The individual Users you want to add to the user group. Start typing the username and it will be displayed. Simply select it to add it to the User Group. note: Aliases can not be added to a User Group.

Regardless of whether you're creating shared Calendars or Conference Rooms, or setting up User Groups, be sure to save your information after you've finished your edits.

Signatures

This settings page is only available to domain administrators and system administrators with the proper permissions.

An email signature is a block of text automatically appended at the bottom of an email message. Signatures may contain the sender's name, address, phone number, disclaimer, or other contact information.

Businesses that want to ensure a consistent company appearance may require employees to follow a specific signature format. Instead of allowing the users to define their own signatures, the domain administrator can create a domain-wide signature that all employees must use. Depending on the signature configurations set up by the domain administrator, users may or may not be able to override the default signature.

Signatures

To create a new signature, click on New Signature . To edit an existing signature, click on its card.

Whether you add or edit a signature, the signature creation window appears. Here, you can create signatures using a full HTML editor that allows domain administrators to add in stylized text, links to websites, images and even icons linked to social media outlets. In addition, the signature can incorporate variables so that a generic template can be created for all users of the domain. The available variables are listed by clicking the Custom Variables dropdown in the text box's toolbar, which looks like a settings cog. (If the cog icon doesn't appear in the toolbar, you may need to click the + sign to "Show More" tools.)

Default Signatures

Use this card to assign a domain-wide signature for all users on your domain and any Account or Domain Aliases that have been configured. By default, domain aliases will be set to "Use Primary Signature". This means they will use the signature setting for the primary domain. For instance, if the domain's signature settings is set to "None" then the alias will be set to "Use Primary Signature", which means they will also be set to "None". If the domain was configured to use a signature called "Company Signature" and an alias was configured for "Use Primary Signature", then the alias will also be configured to use the "Company Signature".

To allow users to create and use their own signatures, activate the setting Enable users to override . note: If this setting is disabled, users must use the domain-wide signature.

Domain Spam Filtering

This settings page is only available to domain administrators and system administrators with the proper permissions.

SmarterMail includes a variety of antispam measures that will help keep a user's inbox free of unwanted mail. In the Spam Filtering section, domain administrators can review/configure the spam filtering options and trusted senders for users on their domain.

Jump To:

- Options - Configure the filtering Actions for spam messages on your domain
- Trusted Senders - Exempt specific email addresses and domains from spam filtering

Options

In most cases, a system administrator has already configured the filtering options -- spam weights and Actions -- for spam messages on your domain. However, if the system administrator allows it, domain

administrators can override those settings and change the Actions configured for spam messages of varying weights to help further remove potentially unwanted email.

Options

• Override spam settings - Enable this setting to customize the spam filtering Actions for your domain. If this option is disabled, the systems' default spam filtering policy will be displayed.

• Allow users to override spam settings - Enable this setting if, as the domain administrator, you want to allow users to be able to further edit and manage the Actions taken on messages of varying weights.

Editing Actions

Each type of spam check has an associated weight that factors into the spam probability of a message. In addition, a specific Action is set for messages that score the weight set by the system administrator.

To edit the action, click on the card associated with the weight you want to edit. From there, click the dropdown on the Action to change it and click the OK button to save your change.

Trusted Senders

Domain administrators can add specific email addresses (such as jsmith@@example.com) or domains (such as example.com) that will be exempted from most spam filtering. This lets the system know that these messages come from a trusted source and can prevent mail from friends, business associates, and mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's Contacts list is considered a trusted sender and bypasses most spam filtering. When entering trusted senders or domains, enter only one item per line.

Spam Filtering and Trusted Senders

We say that Trusted Senders bypass "most" spam filtering, because while they do bypass things like RBL and URIBL checks, other checks are ALWAYS run (when enabled) on ALL messages, regardless of whether the sender is considered "trusted".

If the system administrator has enabled SPF, DKIM, and/or DMARC, (all of which are strongly recommended), SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses, and IP bypasses. This "trust but verify" approach is important because anyone can write any return path that they want when sending a message. Therefore, this extra layer of protection helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender. If an SPF, DKIM, or DMARC check fails on an incoming message, the "trusted sender" is no longer trusted by SmarterMail, and the weights of all enabled spam checks will be applied to that message.

DMARC, specifically, plays an integral part in determining "trusted" status. DMARC is the only check available that can confirm that the From address listed in the email is associated to the SPF record and return path. DMARC, therefore, ensures that the From address wasn't spoofed and the sender automatically trusted just because the From address is listed as a trusted sender. It is an extra step of security to ensure that senders are only 'whitelisted' if SmarterMail can verify the sender.

The specific spam check results that will bypass the trusted sender status are SPF_Fail, SPF_Softfail, SPF_PermError, or DKIM_Fail.

If the trusted sender status of an email was bypassed due to a failed SPF or DKIM check, the TotalSpamWeight line in the email header would appear in the following format:

```
X-SmarterMail-TotalSpamWeight: {Total Spam Weight} ({Where the trusted
sender status originates}, {Reason the trusted sender status was bypassed})
```

For example:

```
X-SmarterMail-TotalSpamWeight: 9 (Trusted Sender - Domain, failed SPF)
```

This example indicates that the sender is in the domain-level Trusted Senders list, but the email received a total spam weight of 9 because the message failed the SPF check.

Regarding DMARC

We evaluate the DMARC results of an incoming email in order to determine whether the From Address or Return Path will be used for the Trusted Sender verification. If DMARC has a passing result, SmarterMail will use the From Address to determine if the email is in the Trusted Sender's list. In most cases, the Return Path and From Address of an email are the same, and users will likely have the sender's From Address in their Trusted Senders list. In these cases, as long as SPF and DKIM don't fail or error, the email should be delivered to the user's Inbox without a spam weight applied. If DMARC doesn't have a passing result, it will use the Return Path to determine if the email is from a Trusted Sender. If the Return Path address is in the Trusted Senders list as well, the email should be delivered to the user's Inbox without a spam weight applied.If the Return Path address isn't in the user's Trusted Sender's list, the full spam weight of the message will be applied, and the email will be filtered / moved according to the user's spam filtering settings. In these situations, they will likely land in the Junk Email folder, and the X-SmarterMail-TotalSpamWeight header will show why the weight was applied, with something like this:

```
X-SmarterMail-TotalSpamWeight: 37 (Trusted Sender - User, DMARC: None)
```

```
X-SmarterMail-TotalSpamWeight: 24 (Trusted Sender - User, DMARC: Skipped -
DMARC Disabled)
```

These are the DMARC results that are considered "passing" and will allow the From Address to be considered in the Trusted Sender verification process:

- DMARC: [passed]
- DMARC: [skipped - Authenticated] This will appear if the sender is an authenticated domain user or if the sender's IP address is in the whitelist with an SMTP Auth Bypass.
- DMARC: [skipped - Bypassed] This will appear if the sender's IP address is in the IP Bypass with Bypass Spam Checks enabled, and there is only 1 Received line in the email header/delivery.
- DMARC: [skipped - Whitelisted] This will appear if the sender's IP address is in the Whitelist with an SMTP Spam Bypass.

These are the DMARC results that are not considered "passing", and will disallow the From Address from being considered in the Trusted Sender verification process.

- DMARC: [none]
- DMARC: [failed]
- DMARC: [skipped - DMARC Disabled]
- DMARC: [skipped - No Return Path]

We also added this logic for adding or removing Trusted Senders from within the Email section:

- If Return and From match, then we add/remove the From Address.
- If Return and From differ, we look at the DMARC Results of that email.

- If DMARC passed (or was skipped due to authentication, bypass or whitelist), we add/remove the From Address.
- If DMARC didn't pass, we add/remove the From Address and the Return Path address. (This is done to help ensure that the sender will pass the DMARC Trusted Sender verification process on subsequent messages.)

User Defaults

For domains that have a large number of users, it can be time-consuming to make a change to user settings — increase the Mailbox Size Limit or disabling the ability to change passwords, for example — and then ensure the changes are applied to all users. With User Defaults, however, domain administrators can create a template for the default user settings so that they only have to make the change in one location, and then propagate those settings to a select few users or each user on the domain. This makes changing settings quick and easy and ensures each user has the exact same permissions and settings applied.

User Defaults

To review the default configuration for new users, click on the User Defaults button. The default user settings are identical to those found when adding or editing a user. For more information on these settings, refer to the Managing Users page.

You can make whatever changes you want to these settings, and any NEW accounts that are added will use these defaults. However, it's also possible to change these settings, then push those settings to one or more users individually, or to all users. In the case of pushing changes to individual users, say you have a set Mailbox Size Limit set for all users of 2000MB (2GB). However, the C-Level execs need more. It's possible to change that limit to something higher — 8000MB (8GB), for example — and then push that change to all the accounts set up for the C-Level executives.

Propagation

To apply some or all of the default user settings to some or all of the existing users on the domain, do the following:

- First, make any changes you want on this page, then click the Save button.
- Next, click on the Propagate button. A modal window opens up.
- Scroll down the list of settings, placing a check mark next to the settings you want to push to your user(s).
- Once all items have been selected, you can pick who you want to propagate the changes to:

- Specific Users - Selecting this allows you to start entering the users you want to propagate the changes to. These changes will only propagate to the users you enter.
- All Users - This will propagate the changes to all users of the domain.
- Once you've selected your changes, and added the specific users you want to propagate the changes to, click the Propagate button. Note: Simply making a change to the User Defaults doesn't automatically propagate, so a change to default settings does not change users that are already in place for the domain. They only affect any new users that are created. In order for changes to take effect, they must be propagated. In addition, if you're making changes to individual users, you may need to go back and change the propagated settings back to what they were originally. Otherwise, any new users created will use those new settings. Note: If a system administrator is impersonating a domain administrator and wants to propagate settings changes — and, specifically, Exchange Synchronization changes — User Administration for those settings MUST be enabled for the domain. Otherwise, changes will not be saved for users.

Help for System Administrators

Logging in to SmarterMail

The system administrator login is a bit unique, especially in comparison to user logins, or even domain administrator logins.

First off, there's no mail folders, calendars, or other "email features" associated to a system administrator. You're purely managing the SmarterMail installation — adding domains, managing antispam and antivirus, setting up gateways, etc. A domain administrator account is, by and large, just another user of SmarterMail. The difference is they have some management of the domain and its users. System administrators, however, manage everything on the server, so they're not a standard user of SmarterMail. (Though they can be, they'll just need an actual user account set up on a domain.)

Secondly, the system administrator login can be used with any domain or IP address set up within SmarterMail. Simply navigate to any configured domain, such as https://mail.example.com, and type in your credentials. It's also possible to login using the hostname set up for the server itself, via an IP address configured for a domain, or via localhost using port 9998. No matter how you choose to log in, you're presented with all the tools necessary for properly managing a SmarterMail server.

Adding a New Domain

Once SmarterMail has been installed, it's time to start adding domains.

Just a few pieces of information are needed in order to add a domain. Once this information is provided, the new domain is set up using the Domain Defaults that have been configured. However, system administrators can always modify any Domain Details as needed by simply clicking on its name on the Domains page .

Adding a Domain

To create a new domain, click the New button within the Domains section. The following custom configuration options will be available:

- Name - The name of the domain. For example, smartermail.com or example.com.
- Hostname - The URL of the mail server (e.g., mail.domain.com) to be returned for an Autodiscover query by a user of that domain. This will also act as the URL for users to log in to the webmail client. SmarterMail will default this to mail.your-domain-name.com based on the Domain Defaults that are pre-configured on a new installation of SmarterMail. However, hostnames can be edited as needed and that default can be set to whatever the system administrator wants it to be.

• Folder - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. Note: If the directory does not already exist, it will be created. This directory should be solely dedicated to SmarterMail. By default, SmarterMail saves domain information to c:\SmarterMail\Domains\.

• Primary Domain Administrator Username - The primary domain administrator is responsible for adding and deleting email accounts and setting specific configurations for the domain. Domain administrator accounts also have the ability to send and receive email, manage contacts, etc., just like a user account. Enter the identifier the domain administrator will use to log into SmarterMail. Enter only the username, not the full address. For example, the "jdoe" portion of "jdoe@@example.com".

• Primary Domain Administrator Password - Enter the password associated to the domain administrator username.

Microsoft Exchange Functionality

This feature is only available using SmarterMail Enterprise licensed with the EAS and/or MAPI & EWS add-ons.

Microsoft Exchange is the standard for corporate email servers. Whether using an on-premise installation or a Microsoft 365 subscription, there is no doubt that Microsoft Exchange, coupled with Microsoft Outlook, offer the features and functionality that email users require for their day-to-day communication.

For years, there was very little competition with Exchange. While there were competing mail products on the market — third-party products, Yahoo! mail, AOL, and even the rise of Gmail — the functionality users had with Outlook coupled with Exchange were virtually untouchable. Then came SmarterMail.

Over the years, SmarterMail has grown to be one of the primary competitors to Microsoft Exchange. With the addition of EAS support, the power of mobile email was introduced. Now, SmarterMail offers MAPI & EWS, for true, native Microsoft Outlook integration on desktops that gives Exchange a run for its money. And, speaking of money, SmarterMail offers that functionality for a mere FRACTION of what it costs to run Exchange, either on premise or using Microsoft 365.

MAPI & EWS

MAPI is Microsoft's "Outlook protocol". That means it is the foundation by which Outlook on Windows does things like share tasks, calendars and email folders; set up meetings; create contact groups and much more. EWS is a similar protocol, but one that was developed specifically for integration with the Apple ecosystem. While other, non-Mac email clients have adopted EWS (e.g., eM Client), it primarily works with Apple Mail on the Mac.

What makes SmarterMail's use of MAPI different than its competitors is that SmarterMail has native, server-level integration of MAPI, just like Microsoft Exchange. Other products use separate pieces of software that are installed on client machines to "emulate" Exchange functionality. These "Outlook Connectors" don't provide the full suite of Exchange features to Outlook. In addition, they're another piece of software that a client has to install, and that mail administrators or IT staff have to manage. Note: MAPI is only supported in Microsoft Outlook 2016 and above for Windows. Outlook for MacOS uses EWS. Older Outlook clients will need to connect to SmarterMail using POP3 or IMAP. Other clients, such as eM Client amd Apple Mail, can use EWS.

EAS

EAS is the industry standard for synchronizing mobile devices to SmarterMail, in addition to some email clients (e.g., Microsoft Outlook for Mac). It uses direct push technology to sync email and collaboration items to variety of mobile devices, including smartphones and tablets, as well as Windows Mail, which ships as part of Windows for desktops.

Enabling Exchange Functionality

Both MAPI & EWS and EAS are licensed protocols from Microsoft. As such, they're licensed add-ons for SmarterMail. So the first step is to ensure you've licensed the add-on you want and/or need.

Next, the system administrator would need to enable either, or both, for a particular domain. To do this:

- Log in as the System Administrator.
- Go to the Manage area and select a domain from the list.
- MAPI & EWS and EAS are actually enabled separately in the domain's configuration. Therefore, find the card for the protocol you want to enable for the domain.
- Add in the number of Accounts you want to allow to use either protocol.
- Ideally, as a system administrator, you just want to enable the protocols, then allow the domain administrator to manage which accounts actually use the protocols. To achieve this, enable Allow domain administrators to manage [protocol] for users . This allows the domain administrator to assign the protocol to an actual mailbox.

That's it! You've enabled Microsoft Exchange functionality for that domain.

Enabling Exchange Functionality for More Than One Domain

It IS possible to propagate Exchange functionality to more than one domain at a time. You do this using Domain Defaults. You would manage the settings just as you do for a single domain, but then propagate the settings to all domains or even select domains. For more information on this, see the Domain Defaults and Propagation section of the Manage page.

Manage

Domains

System administrators can use the Domains section to add or remove domains, manage the configuration of one or more domains, attach or detach domains, attach or detach users, send messages to users on the server, export a list of domains or users to CSV and more.

SmarterMail accepts both Western and non-Western character sets for domains as it supports UTF8 encoding for POP, SMTP, etc. This means that domains with non-Western characters can be added to SmarterMail, and SmarterMail will handle them just like any other domain. So if a domain contains Japanese characters, for example, SmarterMail will still be able to handle users, sending/receiving email, etc. for that domain just as if it used standard English characters.

If you are looking for a specific setting or for an explanation of a specific domain option (e.g., Forwarding Exclusions), please see the Domain Defaults page of help .

Existing domains will be displayed, but if there are no domains are listed, you will need to Add a New Domain . Basic details about each domain is displayed, which includes:

- • Domain - The list of domains configured on the server.
- • Enabled - Whether the domain is enabled or disabled. A checkmark denotes if the domain is enabled or not.
- • Users - The number of users configured for the domain / the number of users allowed for the domain.
- • Aliases - The number of user aliases configured for the domain / the number allowed.
- • Mailing Lists - The number of mailing lists configured for the domain / the number allowed.
- • EAS Mailboxes - The number of EAS licenses being used / the number allowed.
- • MAPI & EWS Mailboxes - The number of MAPI/EWS users / the number allowed.
- • Message Archiving - Whether the domain has a specific message archiving rule set up for it. (If it does, a checkmark is displayed for the domain.)
- • Disk Usage - Total disk usage by the domain, including user folders, file storage, etc. Mousing over this indicator displays a pop up showing the total disk usage, then a split by Primary and Secondary storage.

Domain Details

If a system administrator has the ability to manage individual domains, when they select a domain they'll see the following tabs. These tabs represent how the domain is set up and are, essentially, the same options available to the domain's administrator(s).

• Options - These are all of the configuration settings for the domain such as disk space and message size limits, available features, autodiscover settings, etc. Generally, these are carried over from Domain Defaults .

• Accounts - The list of all users and user aliases set up for that domain. For more information see Users Overview .

• General - These are general settings for the domain such any Domain Aliases being used, Folder and Calendar Auto-Clean rules, Email Signing and more. For more information see General Domain Settings .

• User Connections - Displays the users for the domain along with the number of connections to the different syncing protocols available. For more information, see User Connections .

• User Statuses - Displays the users for the domain along with the statuses for a variety of things such as indexing, password compliance, etc. For more information, see User Statuses .

• Content Filtering - The content filtering rules set up for all users of the domain. For more information see Domain Content Filtering .

• Events - The events set up for the entire domain. For more information see Domain Events .

• Message Archive Search - If the domain has archiving enabled, this tab allows for a search to be conducted of the archived messages. For more information see Message Archiving .

• Password Requirements - The Password Requirements, if any, configured for the domain. For more information, see Password Requirements .

• Sharing - The Shared Resources and User Groups set up for users of the domain. For more information see Domain Sharing ,

• Signatures - The Signatures and Default Signature mappings set up for users of the domain. For more information see Signatures .

• Spam Filtering - The spam filtering rules set up for users of the domain. For more information see Domain Spam Filtering .

• User Defaults - The default settings for each user of the domain such as the Mailbox Size Limit, Webmail options, Service Access and more. For more information see User Defaults .

Domain Actions (□)

When on the Domains page, there are several Actions available to system administrators. To view these actions, click the Actions (□) button. You'll see the following:

• Enable / Disable / Reload Domain - These actions allow you to change the status of a domain.

• Attach Domain / Attach User / Attach Folder / Rebuild Folder / Detach Domain - These actions allow you to recover a user's account, folder or emails, as well as recover a domain or detach it so it can be moved to another server.

• Export Domains / Users to CSV - These actions allow you to export a list of all domains, or all users for all domains, to a CSV file.

• Send Email / Notification - These actions allow you to send an email or reminder notification to users on the server.

Enable / Disable / Reload Domain

The ability to change the status of a domain — either enabling it, disabling it, or refreshing it.

Enable / Disable Domain

Enabled domains are fully functional. Disabled domains cannot send email and users cannot log in to the web interface. However, the domain will still receive email to prevent email loss. This option is a good way to temporarily shut off a domain without deleting it.

Reload Domain

Reloading a domain is essentially "rebooting" it: it deletes all memory and cache associated with the domain and reloads all settings (domain, user, etc.) from the system files on disk. If you see odd behavior with users or other odd behavior, reloading the domain may clear things up.

Attach User / Attach Folder / Rebuild Folder

System administrators can restore a user's emails, email folders or their entire user account, which is extremely useful if a folder or email is mistakenly deleted or if there is corruption within the mailbox.

To restore user data, click on the Actions (□) button in the Domains section. Then choose the type of restore you would like to perform:

• Attach User - Select this option to attach a user that is on disk but not in the domain. In other words, to restore an entire user's account. Note: The user's folder needs to be correctly placed in the domain folder on the server prior to performing this action.
• Attach Folder - Select this option to attach a folder that is on disk but not in the account. In other words, to restore a user's email folder.
• Rebuild Folder - Select this option to copy .grp files or .eml files into an existing user's folder and have SmarterMail re-build that folder to include the new .grp and .eml files. In other words, to restore a user's emails.

The following options will be available, depending on the restore type selected.

• Email - The full email address of the user being restored or the full email address of the owner of the folder being attached or rebuilt.
• Folder Path - The path of the folder within the web interface that will be used to rebuild or restore an email folder. For example, if you're restoring a subfolder that was created under the Inbox, the folder path would look like: Inbox\Example Folder.
• Recursive - Enable this option to attach any subfolders that are found within a folder that is

being attached or rebuilt. Note: There could be a UID conflict issue if you restore .grp files into an existing folder with existing .grp files. If you are only restoring email messages, it is recommended that you create a new folder within the SmarterMail interface and copy the .grp and/or .eml files to that new folder. Then use the Rebuild Folder function. This issue would not occur when restoring .eml files into an existing folder with existing email.

Attach / Reload / Detach Domain

The ability to quickly and easily move domains from one SmarterMail server to another, without having to stop the mail server or halt the mail service, is crucial for system administrators.

Attach Domain

Attaching a domain makes it easy to add a new domain, complete with users, configuration settings, etc. You simply move the files and folders to a new server, add in the Domain Path , and SmarterMail will add the domain to the domains.json file.

Reload Domain

Reloading a domain is essentially "rebooting" the domain: it clears all webmail sessions, reloads the domain's settings, all user settings and files for the domain. If you see odd behavior with users or other odd behavior, reloading the domain may clear things up.

Detach Domain

Detaching a domain essentially prepares the domain for a move to another server, or even just moving the domain to another drive. Detaching removes the domain from the domains.json file, then, once you've made whatever changes are necessary, you simply attach the domain again. It also logs out any users who are logged in and, more importantly, will remove any Domain Aliases that are set up for the domain. These would have to be re-added once the domain is attached in its new location.

Attaching SmarterMail 16.x and Older Domains

If you try to attach a domain from 16.x or older to a newer installation, you'll get a warning saying: "This domain is not valid for this version. To convert and attach the domain, stop the SmarterMail Service, add the domain path to the domains.json file, then restart. For more information, refer to the Online Help." This warning occurs because the domain needs to go through a significant conversion process before it can be attached to the installation. During the conversion process, XML files will be converted to JSON format, mailboxes will be switched to use the new indexing system, and system files will be modified to help increase SmarterMail speed, reduce disk/CPU and, overall, make for a smoother experience.

If you have a domain from an older version that you want to add to a latest Build, follow these steps:

• Before beginning, make a backup copy of the domains.json file and the domain folder you wish to attach.

• Place the domain folder where you would like it to reside.

• Stop the SmarterMail Service.

• Using Notepad or a similar text editor, open the domains.json file.

• Add the domain path in the same format as the other domains. The domain path should be entered in the format required by your operating system. For example, on Windowds:

```
"domainName.com": { "data_path": "c:\\SmarterMail\\Domains\\domainName.com"
}
• Save the file. Note: You may need to save it to the desktop, then
manually replace the original due to Windows Security.
• Start the SmarterMail Service. IMPORTANT NOTE: It is imperative that the
JSON validation remains valid. Failure to preserve the JSON validation will
prevent the SmarterMail site from loading. You can verify the file
integrity by running the file through an online JSON validator such as
JsonLint Simply copy the contents of one of those files and paste it in the
online validator.
```

Depending on the size of the domain, it may take anywhere from a few seconds or up to an hour for the domain conversion to complete. During this time, the SmarterMail server will be inaccessible. You can access the conversion status page at any time by going to https://your_mail_domain/interface/convert-status. You'll need to log in with a system admin username and password. As the domain conversion runs, you'll see a screen similar to the following:

Details of the conversion process can also be found in the conversion log which is stored by default at C:\SmarterMail\Logs\{date}-conversion.log.

Export Domains / Users to CSV

System administrators can export a list of all domains or users on the server in CSV format. The domain CSV spreadsheet will include every domain name along with its status, size, number of users, number of aliases, user limits, throttling configuration, enabled features and more. The user CSV will list every username, sorted by domain, along with their display name, authentication type, title, full name, birthday, phone number, home address, work address, job title, disk space used, status, last login date and more.

System administrators with Manage Domain permissions can also export the Users for specific domains. All they do is go to the Accounts tab for the domain — there is an Export Users option under the Actions (□) button on the Accounts tab.

To use the export feature, click on the Actions (□) button in the Domains sections and then click on Export Domains to CSV to export a list of domains or Export Users to CSV to export a list of users.

Send Email / Notification

SmarterMail gives system administrators the opportunity to send mass emails and reminders to the users on the SmarterMail server. This can be extremely beneficial for notifying users of a specific domain about any policy changes, announcing work being done that may impact access to the mail server, sending warnings to specific users about any potential mail server abuse, sending emails to all domain administrators regarding settings changes and much more. It's a simple way for system administrators to keep mail server users up-to-date and current about a variety of topics.

Send Email

To send a mass email, click the Actions (□) button in the Domains section and then click Send Email . The mass messaging options will load in a modal window and the following fields should be completed:

- From - The individual sending the email message. "System Administrator" will be entered as a default.
- To - Select the message recipients from the list. Note: If All Users on a Domain is chosen, you will then be asked to enter the domain name. If you choose Specific User you will be asked to enter a Specific User's email address.
- To Friendly Name - This is a friendly name or description for the recipients that will appear in conjunction with their email address in the To field. For example, if you're sending an email to all users of the domain example.com you could use something like "Example.com User".
- Subject - The subject of the email.
- Message - Type the text of the message in this field. Messages can be in plain text or stylized with HTML formatting.

Once you complete all the fields, click the Send button to deliver the message.

Send Notification

Notifications are a quick and easy way to send information to a group of users on the mail server. Similar to sending an email, a notification will stay within the mail server and be displayed in users' notifications area rather than being sent to them as an actual email message. For example, if you send a message to all users of a domain about some upcoming maintenance work on the mail server, you can use Send Notification to do a quick follow up reminding the users of the scheduled work.

To send a mass notification, click on the Actions (□) button in the Domains section and then click on Send Notification . The messaging options will load in a modal window and the following fields should be completed:

- To - Select the message recipients from the list. Note: If All Users on a Domain is chosen, you will then be asked to enter the domain name. If you choose Specific User you will be asked to enter a Specific User's email address.
- Subject - The subject of the email.
- Message - Type the text of the message in this field.

Once you complete all the fields, click the Send button to deliver the notification message.

Relevant Knowledge Base Articles

We have created several knowledge base articles for common situations where use of "Attach Domain" or "Rebuild Folder" are necessary. Below is a partial list of articles that detail the steps necessary to do things such as restore a user's folders, migrating or moving a domain from one server to another, etc.

- Backup and Restore SmarterMail
- Restore a User's Account, Folders, or Emails
- Migrate SmarterMail to a Different Server
- Migrate SmarterMail to a Different Server (Using Robocopy)
- Move a Domain from One SmarterMail Server to Another
- Move a Domain to a Different Hard Drive on the Same Server
- Move SmarterMail from Hosted to Self-Installed
- Marketplace Help for System Administrators

Spool

Spool Overview

The email spool is a list of emails, in order of when they are created, that are available for the server to send out to other mail servers or to deliver locally. Within the Spool Overview section, administrators can monitor a dashboard of common aspects of the email spool, including message activity, top outbound senders, top inbound domains and more. In addition to reviewing the spool activity, Administrators can take action on any messages that are currently being held in the spool. For example, a sending IP address that is inundating the mail server with unwanted messages can be blocked, thereby preventing issues from becoming problems for email users.

And while monitoring the spool regularly is good practice, the Overview section is extremely helpful should the mail server become compromised as you can easily spot a compromised account, block the sender and delete the unnecessary messages. The overview dashboard provides a real-time look at a mail server's activity, refreshing every 20 seconds, so administrators always know what's going on.

Spool Processing

By default, SmarterMail has a three (3) second loop for messages processed across the various queues in the spool. (I.e., spam checks, local deliveries, remote deliveries.) However, messages are processed, and move between spam checks and delivery queues, at random times. Therefore, the "3 second loop" may or may not be strictly enforced and is independent of when the message arrives in the spool. If a message is ready for the next step in the process when it hits a particular queue (e.g., spam checks) it will move on to the next queue (e.g., local delivery). If it isn't ready, it will be checked the next time that queue is processed. So any delays noted in logs can be different as a result.

Message Activity

This section displays the total number of messages that have been sent by, or delivered to, all users, including local and remote deliveries. From this table, see how many messages were sent in the last 5 minutes, last hour, last 24 hours and since the time the server was last started (or restarted.)

Top Outbound Senders

This section displays the users with the highest number of outbound remote deliveries (for the specified time intervals). The following actions can be performed on each user included in the table: Note: The message count does not include local deliveries sent user-to-user.

> • Manage User - Select this option to log in and impersonate the actual user. Impersonating the user allows you to check all of their settings and includes Domain settings if the user is a domain administrator. So if the user appears to be compromised, it can be disabled after due

diligence is performed.

• Change Password - Select this option to change the password for a user. Changing the password is an ideal option when resolving a compromised account.

• Drop Connections - Select this option to end the user's connection(s) via webmail and different syncing protocols, including SMTP, IMAP, POP, XMPP and EAS, and MAPI/EWS.

• Disable User - Select this option to immediately disable the user. This action utilizes the User Status setting found when editing a user . When a user is disabled within the Spool Overview, their User Status will be set to 'Disable and Allow Mail'. This prevents the user from sending outbound messages or accessing webmail; however, the mailbox will continue to receive incoming email. Enabling a user in the Spool Overview will adjust the setting in the user's settings and vice versa.

• Delete Messages - Select this option to permanently delete the messages sent by the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.

• Move Messages - Select this option to move the messages sent by the user that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them. Note: In general, this table will display SmarterMail user accounts only. However, there may be cases where remote email addresses appear, including when the email address is authenticated with a local account, the sending IP address is listed in the SMTP Authentication Bypass list, SmarterMail is acting as an inbound gateway, or messages were manually dropped into the spool with sender addresses that don't exist locally. In these instances, the Manage User and Disable User actions cannot be performed as the accounts are not within SmarterMail.

Top Outbound IP Addresses

This section displays the IP addresses that have sent the highest number of outbound, remote deliveries (for the time intervals specified). The following actions can be performed on each IP address included in the table:

• Blacklist - Select this option to block the IP address from sending messages to the server. When an IP address is blacklisted from the spool, an entry will be added to the Blacklist found in the Security section. The IP address will be blocked on SMTP only, and the entry will be denoted as having been blocked from the spool. Unblocking an IP address in the spool will remove the Blacklist entry in Security settings and vice versa.

• Delete Messages - Select this option to permanently delete all outbound messages sent from the IP address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.

• Move Messages - Select this option to move all the outbound messages sent from the IP address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Top Inbound Recipients

This section displays the users (local user accounts) who have received the highest number of incoming messages (for the time intervals specified). Both local and remote deliveries are included in the message count. This allows administrators to know which accounts on the server are receiving the most mail. The following actions can be performed on each user included in the table:

• Manage User - Select this option to log in and impersonate the actual user. Impersonating the user allows you to check all of their settings. Impersonating the user allows you to check all of their settings and includes Domain settings if the user is a domain administrator. So if the user appears to be compromised, it can be disabled after due diligence is performed.
• Change Password - Select this option to change the password of a user's account. Changing the password is an ideal option when resolving a compromised account.
• Drop Connections - Select this option to end the user's connection(s) via webmail and different syncing protocols, including SMTP, IMAP, POP, XMPP and ActiveSync.
• Delete Messages - Select this option to permanently delete all of the inbound messages sent to the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
• Move Messages - Select this option to move a user's inbound messages that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Top Inbound Senders

This section displays the email addresses that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each email address included in the table:

• Block Inbound SMTP - Select this option to block all incoming mail sent from the email address. This action utilizes SMTP Blocking found in the Security section. When an email address is blocked within the spool, an entry will be added to the SMTP Blocks list for incoming email and the entry will be denoted as having been blocked from the spool. Unblocking an email address in the spool will remove the SMTP block and vice versa.

• Delete Messages - Select this option to permanently delete all inbound messages sent from the email address that are currently in the spool. Note: This will only delete messages that are currently being held in the spool.

• Move Messages - Select this option to move all the inbound messages sent from the email address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Top Inbound IP Addresses

This section displays the IP addresses that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each IP address included in the table:

• Blacklist IP - Select this option to block the IP address from sending messages to the server. When an IP address is blacklisted within the spool, an entry will be added to the Blocked Senders found in the Security section. The IP address will be blocked on SMTP only, and the entry will be denoted as having been blocked from the spool. Unblocking an IP address in the spool will remove the Blacklist entry in Security settings and vice versa.

• Delete Messages - Select this option to permanently delete all inbound messages sent from the IP address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.

• Move Messages - Select this option to move all the inbound messages sent from the IP address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Top Inbound Domains

This section displays the domains that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each domain included in the table:

• Block Inbound SMTP - Select this option to block all incoming mail sent from the domain. This action utilizes SMTP Blocking found in the Security section. When a domain is blocked within the spool, an entry will be added to the SMTP Blocks list for incoming email, and the entry will be denoted as having been blocked from the spool. Note: This action does not block on the EHLO Domain. Instead, it uses the Email Address field and enters only the domain.

Unblocking a domain in the spool will remove the SMTP block and vice versa.

• Delete Messages - Select this option to permanently delete all inbound messages sent from the
domain that are currently in the spool. Note: This will only delete messages that are
CURRENTLY being held in the spool.

• Move Messages - Select this option to move all the inbound messages sent from the domain
that are currently held in the spool to another folder on the server. Use the default path provided
or enter any folder path on the server. Moving the .eml files to their own folder on the server is
useful because it allows an administrator to review the messages before taking actions against
them.

Spool and Waiting to Deliver

The email spool is a list of emails, in order of when they are created, that are available for the server to
send out to other mail servers or to deliver locally. SmarterMail is multithreaded, which means that if
a message cannot process out of the spool, SmarterMail simply moves on to the next message until the
maximum number of threads that are designated in the administrative configurations are in use.
Administrators can use the information here to adjust threads and resources to allocate for concurrent
messages.

Messages enter and leave the spool fairly quickly. In fact, some pass through so quickly that they will
not display in the spool. Most messages in the spool are displayed because they are large, have many
recipients, or are having trouble being sent to their final destination.

The Spool tab displays all inbound and outbound messages, including ones that are attempting to be
delivered or waiting to be delivered. To view a filtered display of the spool for only messages that are
waiting to be delivered, use the Waiting to Deliver tab.

Important Notes:

• Messages that are Waiting to Deliver have typically encountered an error on one or more
recipients of the message and are waiting for the next retry interval to attempt delivery again.
Emails that are stuck on local delivery or waiting to deliver without any retry attempts are
typically the result of IO Bottleneck at the CPU or storage array.

• Spool and Waiting to Deliver tabs will only load a maximum of 50,000 messages combined.
(E.g., 20,000 Spool messages are displayed and 30,000 Waiting to Deliver messages are
displayed - together they'll never show more than 50,000 messages). That means that if the two
numbers add up to 50,000, it's very likely there are MORE than the number of individual emails
for each type than can be displayed.

The following details can be seen for each entry in the spool:

- Filename - The unique name of the EML file on the hard disk of the SmarterMail server.
- Spool Path - The spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.
- Sender - The email address that initially sent the email.
- Recipients - The number of delivered/total recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Attempts - The number of delivery attempts that have been made.
- Time in Spool - The total amount of time the message has been in the spool.
- Priority - The priority level of the message: low, normal or high.
- Status - The current status of the message. Messages in the spool have four delivery statuses:

- Delivery Delay - This is the first status of any message in the spool. Administrators can configure a Delivery Delay within the system's General Settings. This delay represents the number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message.
- Spam Check - At the second stage of an email's delivery process, SmarterMail runs the configured spam checks against the contents of the email. Messages from whitelisted senders will bypass this delivery status.
- Waiting to Deliver - Emails with a status of Waiting to Deliver have typically encountered an error on one or more recipients of the message and is waiting for the next retry interval to hit. On the next retry interval, the delivery process will start from the top with its configured Delivery Delay.
- Remote / Local Delivery - This is the final stage of an email's delivery, where the message is sent to its intended recipients. A status of Local Delivery will appear for messages sent between local users on the server and is shown is when SmarterMail is writing to the actual GRP files. Remote Delivery will appear for any outgoing messages that are destined for outside of the mail server.
- Next Attempt - The date and time of the next delivery attempt, based on the retry intervals configured in General Settings.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window. If you are presented with a note that the "Message no longer exists," it's possible that the message was already delivered or removed by antivirus software or that the spool contains an orphaned HDR file without the associated EML.

The following actions can be taken on selected entries using the Actions (□) button:

• Force - Pushes the selected message(s) to the top of the spool by setting its priority to High. Note: The status of forced messages will not update until the server passes through the spool.

• Reset Retries - Resets the retry counts on the selected message(s) in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.

• Change Priority - Changes the priority level of the selected message(s).

• Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

• Download EML - Allows you to download the raw EML file for the message.

• Delete - Removes the selected message(s) from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.

• Delete All from Sender - Deletes all messages in the spool from the specified sender. Caution should be used with this action as the same email address can be used for different types of messages. For example, a "no-reply" address can be used for bulk notifications but may also be used for promotional emails, etc. Deleting all messages from the no-reply sender may, therefore, have unintended consequences.

• Move All from Sender - Moves all messages in the spool from the specified sender. The same caution should be used as with deleting all messages from sender.

Searching the Spool

Domain administrators can search for messages from particular senders in the spool. To do so, use the Search bar at the top of the content pane. Simply type in the email address of the sender and click the magnifying glass to search for any messages from that sender that are in the spool.

Spool and Waiting to Deliver

The email spool is a list of emails, in order of when they are created, that are available for the server to send out to other mail servers or to deliver locally. SmarterMail is multithreaded, which means that if a message cannot process out of the spool, SmarterMail simply moves on to the next message until the maximum number of threads that are designated in the administrative configurations are in use. Administrators can use the information here to adjust threads and resources to allocate for concurrent messages.

Messages enter and leave the spool fairly quickly. In fact, some pass through so quickly that they will not display in the spool. Most messages in the spool are displayed because they are large, have many recipients, or are having trouble being sent to their final destination.

The Spool tab displays all inbound and outbound messages, including ones that are attempting to be delivered or waiting to be delivered. To view a filtered display of the spool for only messages that are waiting to be delivered, use the Waiting to Deliver tab.

Important Notes:

• Messages that are Waiting to Deliver have typically encountered an error on one or more recipients of the message and are waiting for the next retry interval to attempt delivery again. Emails that are stuck on local delivery or waiting to deliver without any retry attempts are typically the result of IO Bottleneck at the CPU or storage array.
• Spool and Waiting to Deliver tabs will only load a maximum of 50,000 messages combined. (E.g., 20,000 Spool messages are displayed and 30,000 Waiting to Deliver messages are displayed - together they'll never show more than 50,000 messages). That means that if the two numbers add up to 50,000, it's very likely there are MORE than the number of individual emails for each type than can be displayed.

The following details can be seen for each entry in the spool:

• Filename - The unique name of the EML file on the hard disk of the SmarterMail server.
• Spool Path - The spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.
• Sender - The email address that initially sent the email.
• Recipients - The number of delivered/total recipients.
• Size - The total size of the message on the hard drive, in kilobytes.
• Attempts - The number of delivery attempts that have been made.
• Time in Spool - The total amount of time the message has been in the spool.
• Priority - The priority level of the message: low, normal or high.
• Status - The current status of the message. Messages in the spool have four delivery statuses:

• Delivery Delay - This is the first status of any message in the spool. Administrators can configure a Delivery Delay within the system's General Settings. This delay represents the number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message.
• Spam Check - At the second stage of an email's delivery process, SmarterMail runs the configured spam checks against the contents of the email. Messages from whitelisted senders will bypass this delivery status.
• Waiting to Deliver - Emails with a status of Waiting to Deliver have typically encountered an error on one or more recipients of the message and is waiting for the next retry interval to hit.

On the next retry interval, the delivery process will start from the top with its configured Delivery Delay.

• Remote / Local Delivery - This is the final stage of an email's delivery, where the message is sent to its intended recipients. A status of Local Delivery will appear for messages sent between local users on the server and is shown is when SmarterMail is writing to the actual GRP files. Remote Delivery will appear for any outgoing messages that are destined for outside of the mail server.

• Next Attempt - The date and time of the next delivery attempt, based on the retry intervals configured in General Settings.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window. If you are presented with a note that the "Message no longer exists," it's possible that the message was already delivered or removed by antivirus software or that the spool contains an orphaned HDR file without the associated EML.

The following actions can be taken on selected entries using the Actions (□) button:

• Force - Pushes the selected message(s) to the top of the spool by setting its priority to High. Note: The status of forced messages will not update until the server passes through the spool.

• Reset Retries - Resets the retry counts on the selected message(s) in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.

• Change Priority - Changes the priority level of the selected message(s).

• Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

• Download EML - Allows you to download the raw EML file for the message.

• Delete - Removes the selected message(s) from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.

• Delete All from Sender - Deletes all messages in the spool from the specified sender. Caution should be used with this action as the same email address can be used for different types of messages. For example, a "no-reply" address can be used for bulk notifications but may also be used for promotional emails, etc. Deleting all messages from the no-reply sender may, therefore, have unintended consequences.

• Move All from Sender - Moves all messages in the spool from the specified sender. The same caution should be used as with deleting all messages from sender.

Searching the Spool

Domain administrators can search for messages from particular senders in the spool. To do so, use the Search bar at the top of the content pane. Simply type in the email address of the sender and click the magnifying glass to search for any messages from that sender that are in the spool.

Spam Quarantine

System administrators can quarantine outgoing messages that have been flagged as spam by SmarterMail's spam checks for a maximum of 30 days. Quarantining such messages allows administrators to investigate why certain messages are blocked as spam and make appropriate adjustments, if necessary. In addition, system administrators can easily resend any outgoing messages that should not have been quarantined.

The Spam Quarantine tab displays Messages that have been flagged and quarantined by SmarterMail's antispam measures, including the Message Sniffer and/or Cyren Premium Antispam add-ons as well as add-ons from other companies, if enabled. The following details can be seen for each entry:

- • File Name - The unique name of the EML file on the hard disk of the SmarterMail server.
- • Date - The date and time the message was flagged for quarantine.
- • Sender - The email address that initially sent the email.
- • Recipients - The number of delivered/total recipients.
- • Size - The total size of the message on the hard drive, in kilobytes.
- • Attempts - The number of delivery attempts that have been made.
- • Time in Spool - The amount of time the message has been quarantined.
- • Time of Removal - The date and time message will be automatically removed from quarantine and permanently deleted.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window.

The following actions can be taken on selected entries using the Actions (□) button:

- • Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
- • Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.
- • Download EML - Allows you to download the raw EML file for the message.
- • Delete / Delete All - Remove the selected message(s), or all messages, from the quarantine list.

Important Notes:

> • Spam Quarantine settings can be managed on the Antispam page. Make sure the Options tab is highlighted. The quarantine settings can be found on the SMTP Blocking card. For more information, refer to the Antispam page.
>
> • Spam Quarantine and Virus Quarantine tabs will only load a maximum of 5,000 messages combined. (E.g., 2,000 Spam Quarantine items displayed and 3,000 Virus Quarantine items displayed - together they'll never show more than 5,000 messages). That means that if the two numbers add up to 5000, it's very likely there are MORE than the number of individual emails for each Quarantine type than can be displayed. If there are, they will need to be reviewed/handled from within the appropriate directory on the server.

Virus Quarantine

Inbound and outbound messages that have been flagged as containing viruses by SmarterMail's ClamAV are quarantined, by default, for 30 days. Quarantining such messages allows administrators to investigate for any false positives and make appropriate adjustments or notify the developer of the virus scanner, if necessary.

The Virus Quarantine tab displays messages that have been flagged and quarantined by SmarterMail's antivirus measures, including add-ons, if enabled. The following details can be seen for each entry:

> • File Name - The unique name of the EML file on the hard disk of the SmarterMail server.
> • Date - The date and time the message was flagged for quarantine.
> • Sender - The email address that initially sent the email.
> • Recipients - The number of delivered/total recipients.
> • Size - The total size of the message on the hard drive, in kilobytes.
> • Attempts - The number of delivery attempts that have been made.
> • Time in Spool - The amount of time the message has been quarantined.
> • Time of Removal - The date and time that a message will be automatically removed from quarantine and permanently deleted.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window. Note: The message is displayed as "text only", and any formatting is removed in order to ensure nothing malicious runs once the message is opened.

The following actions can be taken on selected entries using the Actions (□) button:

> • Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
> • Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on

the server. For example, it's possible to move messages to a "Moved Items" folder within the Spool folder using this path "C:\SmarterMail\Spool\MovedItems\". Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them. While it is possible to move quarantined messages to another user's folder (the folder path would look like "C:\SmarterMail\Domains\[Domain.com]\Users\[Username]\Mail\[Folder Name]\"), this isn't recommended as these messages have been flagged as possibly containing viruses; moving them to a user folder could "enable" any virus contained in a message if it's not handled properly.

• Download EML - Allows you to download the raw EML file for the message.

• Delete / Delete All - Remove the selected message(s), or all messages, from the quarantine list.

Important Notes:

• Virus Quarantine settings are managed on the Antivirus page. For more information, refer to the Antivirus page.

• Spam Quarantine and Virus Quarantine tabs will only load a maximum of 5,000 messages combined. (E.g., 2,000 Spam Quarantine items displayed and 3,000 Virus Quarantine items displayed - together they'll never show more than 5,000 messages). That means that if the two numbers add up to 5000, it's very likely there are MORE than the number of individual emails for each Quarantine type than can be displayed. If there are, they will need to be reviewed/handled from within the appropriate directory on the server.

Throttled Users

Bandwidth and email throttling allow system administrators to limit the quantity of data that a SmarterMail mail server transmits within a specified period of time. This limit can be set by the amount of outgoing bandwidth used or the number of outgoing emails sent.

The Throttled Users tab displays a list of any user who has violated any throttling rules created on the server. Note: User throttling rules can be configured on the User Defaults template in the Manage > Domains section. This configuration can be further managed by domain administrators on a per-user basis.

The following details can be seen for each entry in the list:

• User - The email address of the user currently being throttled.

• Mailing List - This acts as an indicator to specify whether the 'user' being throttled is a mailing list address. Note: Mailing list throttling is managed by domain administrators on a per mailing

list basis.

- Domain - The domain of the user that is currently being throttled.
- Reason - The type of action that triggered the throttle: Messages Out or Bandwidth Out.
- Date - The date and time the user triggered the throttling action.

Throttled Domains

Bandwidth and email throttling allow system administrators to limit the quantity of data that a SmarterMail mail server transmits and/or receives within a specified period of time. This limit can be set by bandwidth, the number of emails transmitted, and/or by the number of bounced messages received.

The Throttled Domains tab displays a list of any domain that has violated any throttling rules created on the server. Note: Domain throttling rules can be configured in the Manage > Domains section on the Domain Defaults page or on a per-domain basis.

The following details can be seen for each entry in the list:

- Domain - The domain on the server that is currently being throttled.
- Reason - The type of action that triggered the throttle: Messages Out, Bandwidth Out or Bounces Received.
- Date - The date and time the domain triggered the throttling action.

User Connections

SmarterMail will monitor users and display the number of connections to the different syncing protocols, including Webmail, SMTP, IMAP, POP, XMPP, EAS, MAPI & EWS, and WebDAV. System administrators can then use this section to drop a user's current connection if they believe too many connections are being made by a user on a particular protocol, or resync the user's protocols to clear up any potential conflicts or inaccuracies. Using the tabs, users can be viewed all at once or separated by protocol. It's worth noting that the numbers displayed in each tab (i.e., SMTP, IMAP, POP, etc.) is the total connections, not, say, the total number of users that are connecting. So if the IMAP tab displays a "7", that means there's 7 total IMAP connections, which could be from 1 or more users.

When viewing user connections, and depending on the tab being viewed, the following columns are available:

- User - The address of the user connecting. Next to the user is the status of the protocol for the user. If there's a checkmark, that protocol is enabled for that user.
- Enabled - Denotes whether the domain is enabled and active or not.

• IP Connections - The number of connections from an IP address for the user listed. Multiple connections can occur when a user is connecting to their account via email clients spread across multiple devices.

• Duration - (For webmail connections only.) The length of time the user has been connected to the webmail client.

• Last Login - The date and time the user last logged in using the protocol being viewed.

• Last Authenticated IP - The last IP address used to authenticate the user.

The following buttons/actions are available, regardless of which tab is being viewed:

• Refresh - Refreshes the list of online users.

• Actions (□) - Additional actions are available via this dropdown:

• Drop Connections - End the selected user's session.

• Resync Devices - Forces the user's account to re-sync across their various devices, for all protocols (All tab) or for just an individual protocol (when on that protocol's tab).

• Enable [Protocol] Access - Enables the protocol for the selected user.

• Disable [Protocol] Access - Disables the protocol for the selected user.

• View Authenticated IPs - Opens a modal window displaying all of the IP addresses that have authenticated with the user credentials and the associated protocol.

Regarding connections that appear to last longer than they should, this could be due to a number of reasons. For example, SMTP connections that stay active for hours could be due to multiple people connecting from behind a firewall. These people all appear to connect from a single IP, but they're actually individual connections, one for each user. The firewall simply portrays the connections as being from a single source. In addition, some numbers may always show up as 0. For example, EWS and MAPI tabs will only show connections when users connecting via those protocols are actually attempting to connect and are pulling or pushing a sync. MAPI and EWS don't IDLE like EAS or IMAP, so the numbers will fluctuate or possibly show 0.

User Statuses

System administrators can use this section to monitor several statuses for each user on the server. Monitoring these statuses can show administrators where there are issues, or inform them of why a particular behavior is occurring. For example, if a user complains of slowness, it could be due to the mail account being indexed. If a new user is missing email, it may be due to it still being migrated into SmarterMail.

When viewing user statuses, the following columns are available:

- User - The full email address of the user.
- Authentication - The type of authentication being used, such as Active Directory or SmarterMail (user/password).
- Two-Step Authentication - Whether Two-Step Authentication is enabled for that user.
- Enabled - Whether the user is enabled for their domain.
- Migrating - Whether the user is still in the process of migrating to SmarterMail.
- Indexing - Whether the user is indexing.
- Authenticated Connections - The number of logins, across various protocols, the user has.
- Password Changes Disabled - Whether the user is able to reset their own password or not.
- Password Violations - The number of times the user has created/used a password that violates the administrator's password policies.
- Password Expired - Whether the users password is expired.

Actions

The following actions can be taken:

- Refresh - This button refreshes the list of online users.
- Actions (☐)

- Reindex - This action will start reindexing the selected user(s).
- Expire Password - This action will cause the selected user(s) to have to reset their password on next login.
- Export to CSV - This action will export a list of selected users to a CSV file that can be opened/used in a spreadsheet applications like Microsoft Excel.

IP Connections

SmarterMail will monitor the IP addresses connecting to the server and display the number of connections to the server each IP has made, as a whole (All Connections) or to the different syncing protocols, including Webmail, SMTP, IMAP, POP, XMPP, EAS, MAPI & EWS, and WebDAV. System administrators can then use this section to blacklist a certain IP address or drop an IP's current connection if they believe too many connections are being made. It's worth noting that the numbers displayed in each tab (i.e., SMTP, IMAP, POP, etc.) is the total connections, not the total number of IP addresses that are connecting. So if the IMAP tab displays a "7", that means there's 7 total IMAP connections, which could be from 1 or more IP addresses.

In addition, the number displayed on the IP Connections menu may not match, exactly, with the number displayed on the All Connections tab once you go to the page. This is because the count in the navigation menu is updated at a set interval whereas the count on the All Connections tab is static

when you open it, then changes when you click the Refresh button. As a result, while the counts may not always be in sync, the count on the menu is an indicator of activity and can therefore alert system administrators that something may be worth investigating if that number is abnormally high.

When viewing connections, the following columns are available:

- IP Address - The IP address of the user connecting.
- Country - The country associated with the IP address.
- Port - The port the user is connecting on. Generally, this will remain constant when viewing connections by protocol. However, some alternate ports may be displayed as well.
- IP Connections - The number of connections from the IP address listed. Multiple connections can occur when a user is connecting to their account via email clients spread across multiple devices.
- SSL/TLS - Whether the connection is secured via TLS or SSL.

The following buttons/actions are available, regardless of which tab is being viewed:

- Refresh - Refreshes the list of online users.
- Actions (☐) - Additional actions are available via this dropdown:

- Blacklist - Adds the IP address to the server blacklist file.
- Drop Connections - End the selected user's session.

Regarding connections that appear to last longer than they should, this could be due to a number of reasons. For example, SMTP connections that stay active for hours could be due to multiple people connecting from behind a firewall. These people all appear to connect from a single IP, but they're actually individual connections, one for each user. The firewall simply portrays the connections as being from a single source. In addition, some numbers may always show up as 0. For example, EWS and MAPI tabs will only show connections when users connecting via those protocols are actually attempting to connect and are pulling or pushing a sync. MAPI and EWS don't IDLE like EAS or IMAP, so the numbers will fluctuate or possibly show 0.

IDS Blocks

System administrators can use this section to review all IP addresses that have been blocked by the mail server as a result of any IDS (abuse detection) rules that have been configured in SmarterMail's Security area. As a result of these rules, SmarterMail will monitor the server and keep track of all IP addresses that are currently being blocked for SMTP, IMAP, POP, LDAP, XMPP, Webmail or for potential email harvesting abuse. System administrators can view a list of blocked IPs by abuse type or view all blocked connections at one time.

The following information is displayed for each block:

- Source - The IP address that tripped the IDS rule. Note: The use of VPNs and proxies mean that the Source of the intrusion may not be the actual origination of the intrusion.
- Time Left - The time remaining for the specific block. When setting up IDS rules, system administrators can attach time limits for each type of block. Time Left offers a countdown timer based on what is set by the system administrator.
- Country - The country of origin for the Source IP.
- Type - The type of intrusion detection rule that was triggered.
- Action - The action taken against the IP address. For example, whether it's blocked or blacklisted.
- Rule Description - The description of the Rule Type as provided by the system administrator when the Rule was created.
- Blocks in 30 Days - The number of times a particular source has triggered an IDS rule in the previous 30 days.

System administrators can remove the selected Source IP(s) from the list by selecting the IP(s) and selecting Unblock from the Actions (□) menu. However, this does not affect the abuse detection rule that blocked the IP in the first place; it only removes the block from the IP or range. If the system administrator feels the block is warranted, and should be enforced past the Time Left, they can Blacklist the IP.

Blacklisting an Entire Class C

Generally, a single IP will trip a specific IDS rule. However, if that IP address is from a problematic locale, system administrators can decide to blacklist the entire Class C range for the specific IP address that was blocked. In order to do this, simply select the IP address then select Blacklist from the Actions (□) menu. (Alternatively, you can right-click on an IP address and select "Blacklist" from the context menu.) A modal will appear and the system administrator can manually toggle the block for the entire Class C or simply elect to blacklist the single IP address. Note: At least ONE IP address from a range is required in order to blacklist an entire Class C.

Domain Defaults

The job of the system administrator is to make sure that the SmarterMail server runs as efficiently as possible. Part of that responsibility is putting measures in place to limit the potential for system abuses and "user error" that could cause problems.

SmarterMail gives system administrators the ability to create a default template that's used as a starting point for all domains that are added to the mail server. This includes the ability to set disk space limits for the domain, set the number of domain aliases that can be created, the number of users and user

aliases, the features available for users and more. These defaults can be set at any time and any new domains that are added will have the new settings. However, the new settings can also be propagated to all domains on the server if need be. From here, domain administrators can further lock down user accounts and set their own user limits.

You can make whatever changes you want to the settings on the Domain Defaults page, and any NEW domains that are added to the server from that moment on will have these defaults applied for their users. However, it's also possible to change these settings, then push those settings to all domains, changing their settings to match what you've set as the defaults for new domains. To do this, you use the Propagate button .

System administrators who have the ability to manage domains will see the information below as well, when viewing the Options tab for a specific domain. However, some of the information will be filled out with customer information. Fields such as Domain Name, Hostname, Primary Domain Administrator, etc. will have information specific to the domain being managed.

Domain Actions (☐)

When viewing the Options for a specific domain on a SmarterMail server, a system administrator has a few different actions they can perform on that domain:

• Rename Domain - This allows for the domain's name to change. For example, changing from a .com to a .net version. Renaming the domain updates the domain's name across SmarterMail, but it DOES NOT move or rename any of the domain's data. In order to fully rename a domain, do the following:

• Rename the domain.

• Wait for the notification stating that the domain was successfully renamed.

• use the Actions (☐) button and Detach the domain.

• Find the domain's location on the appropriate drive. (It will have the old name).

• Rename the domain directory to the new name.

• Reattach the domain. Once this is done, the domain will be fully renamed.

• Reload Domain - Reloading a domain is essentially "rebooting" the domain: it clears all webmail sessions, reloads the domain's settings, all user settings and files for the domain. If you see odd behavior with users or other odd behavior, reloading the domain may clear things up.

• Detach Domain - Detaching a domain essentially prepares the domain for a move to another server, or even just moving the domain to another drive. Detaching removes the domain from the domains.json file, then, once you've made whatever changes are necessary, you simply attach the domain again. It also logs out any users who are logged in and, more importantly, will

remove any Domain Aliases that are set up for the domain. These would have to be re-added once the domain is attached in its new location.

Default Domain Configuration

Domains have a number of configuration settings the govern the features available, various limits for the domain, security features implemented, and much more. The Domain Defaults area is separated into multiple "cards" that contain these various settings. These cards are also mirrored on each domain's "Configuration" tab when it's selected from the Domains page . These cards, and their associated settings, include:

- Options
- Outbound
- Limits
- Features
- Marketplace
- EAS (Enterprise Only)
- MAPI & EWS (Enterprise Only)
- Email
- Mailing Lists
- Security
- Miscellaneous
- Online Meeting Video / WebRTC (Enterprise Only)
- Priority and Throttling
- Autodiscover
- Propagating Domain Defaults

Options

- Domain Name - When viewing a specific domain, the name of that domain. (When setting up Domain Defaults, this filed is not shown.) For example, example.com. To change the name of a domain in SmarterMail, use the Actions (□) button to click on Rename Domain . Note: If you rename a domain, users will have to adjust any desktop or mobile clients to use the new domain name. While SmarterMail changes the domain name internally, it can not push the name change to email clients directly. Those have to be updated manually.
- Status - The current status of the domain: Enabled or Disabled. Disabled domains cannot send email and users cannot log in to the Web interface. However, the domain will still receive email to prevent email loss. This option is a good way to temporarily shut off a domain without deleting it.
- Hostname - The URL of the mail server (e.g., mail.domain.com) to be returned for an

Autodiscover query by a user of that domain. Instructions on how to Set up Autodiscover for SmarterMail can be found in the SmarterTools Knowledge Base . Note: On the Domain Defaults template, the Hostname field has a default value of "mail.%domain%". This variable allows the Hostname to match the name of the domain, though this setting can be adjusted manually, if desired. This Domain Default setting will be applied to new domains and can be propagated to existing domains on the server.

• Primary Path - The initial directory in which all information (JSON files, mail statistics, alias information, etc.) pertaining to a domain is saved. To modify a specific domain's folder path, use the Actions (□) button and select Change Domain Path .

• Secondary Path - A secondary path can be used for older emails and files in SmarterMail File Storage so as to preserve disk space on a primary drive. SmarterMail allows system administrators to select an "Age" to use for automatically, and continually, moving these files in the background, starting at 90 days and then increasing in 30 day increments. For example, when spinning up a SmarterMail server, administrators can start by configuring a standalone Primary Path. As a server grows, however, a Secondary Path can be added. This secondary path can point to a drive or an array of standard HDDs, which aren't as efficient in terms of disk i/o but can save on overall cost. In addition, should the Secondary Path not prove necessary -- say, a server is being decommissioned or users are being migrated to new hardware -- then the Secondary Path can be disabled, and any files stored there are moved back to the Primary Path. Note: Regarding moving emails and files, SmarterMail will move entire messages, including any attachments associated to the messages. As for File Storage, only files uploaded directly to SmarterMail File Storage are affected. Files associated with (i.e., attached or uploaded to) SmarterMail Chat, Online Meetings, Calendars, Contacts, Tasks, or Notes, are not moved and will use the Primary Path. To change a Secondary Path, please see our KB article: Changing a Secondary Path Location for a Domain .

• Primary Domain Administrator - When viewing a specific domain, the primary domain administrator is the user that has control over all aspects of the domain. Domain administrators are set up when a new domain is added to SmarterMail. If you want to change the primary domain administrator for the domain, start typing the username you want to assign to the role, then select it from the autocomplete options. Only existing users on the domain can be selected as the new primary administrator.

Outbound

• Outbound IPv4 - The IPv4 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown. Selecting "Automatic" will use the primary IP address assigned to the Network Interface Card (NIC). note: If a different IPv4 address is set for SMTP Out on the Protocols page , that IPv4

address will take precedence over what is set up for the domain.

• Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown. Selecting "Automatic" will use the primary IP address assigned to the Network Interface Card (NIC). If there is none, this setting is ignored. Note: If a different IPv6 address is set for SMTP Out on the Protocols page , that IPv6 address will take precedence over what is set up for the domain.

• Outbound Gateway - Outbound gateways can reduce the load on the server by using a secondary server to process outgoing mail. Specify an outbound gateway to use for messages sent from this domain. If no options are available, an outbound gateway has not been configured. Instructions on how to Configure SmarterMail as a Free Gateway Server can be found in the SmarterTools Knowledge Base .

• Use primary IP if selections are unavailable - This will use the IP address that's assigned to the Network Interface Card (NIC) on the SmarterMail server.

Limits

• Disk Space MB (0 = Unlimited) - The maximum number of megabytes allocated for the domain. By default, the domain is allocated 500 MB of disk space. This disk space limit also includes file storage and online meetings for users. Note: When this limit is reached, SmarterMail will send a warning to the domain administrator and mailboxes on the domain will not be able to receive new mail.

• Domain Aliases (0 = Unlimited) - The maximum number of domain aliases allowed for the domain. A domain alias is basically an alternate domain name for one that already exists in SmarterMail. For example, imagine you have a domain, 'example.com', in SmarterMail with a user, 'user@@example.com'. By adding a domain alias for 'example.net', emails sent to 'user@@example.net' will be delivered to 'user@@example.com'. That means that emails sent to either domain will end up in the same mailbox. By default, domains are limited to two domain aliases.

• Users (0 = Unlimited) - The maximum number of mailboxes allowed for the domain. By default, domains are limited to 100 users. Note: If your SmarterMail license limits the number of mailboxes allowed on the domain, your license level will override this setting.

• User Aliases (0 = Unlimited) - The maximum number of alias email accounts allowed for the domain. An email alias is essentially a forwarding email address that can be used to forward messages to a single address or multiple email addresses. By default, domains are limited to 1,000 user aliases.

• Max Message Size (KB) - The maximum size email a user can send. By default, the max message size is 512000 KB. This number includes text, HTML, images and attachments. Note:

Base64 encoding of attachments increases their size by approximately 35%. Knowing this, and in order to provide a better user experience, SmarterMail allows messages to be sent that are technically over the limit set for Max Message Size. For example, a 10MB message with a 490MB attachment will still be sent even though the actual message size, after base64 encoding, would far exceed the 500MB max limit.

• Max Attached File Size (KB) - The maximum size of attachments, regardless of type, to NON-email related areas such as calendars, tasks, notes, signatures, etc. This is because the Max Message Size limit already calculates attachment size for email messages.

• Recipients per Message (0 = Unlimited) - The maximum number of recipients a message can have. By default, users can send messages to 200 email addresses.

Features

• Active Directory Integration (Enterprise Only) - Select this option to enable active directory authentication. By enabling this, domain administrators will be able to add in the necessary LDAP binding string to import LDAP users.

• Automated Forwarding - Select this option to allow users to enter one or more forwarding addresses that automatically forwards any email that reaches their mailbox. When this feature is enabled, domain administrators can enable or disable Automated Forwarding on a per-user basis. Note: Messages routed to other email folders via content filters or plus addressing will also be forwarded to this address. Messages routed to the Junk Email folder will not be forwarded by default. However, these can be included if the domain's "Forwarding Exclusion" is set to "No exclusion - Forward all mail." In addition, even if disabled messages may still be forwarded to alternative addresses via Events, content filtering or using rules created within email clients.

• Catch-All Alias - Select this option to allow domain administrators to create catch-all email addresses. A catch-all alias is an email address that receives all incoming email that goes to invalid email addresses within the domain. Note: This simply enables the ability to set a catch-all alias -- an actual alias will need to be created, or an existing alias edited, and assigned as a catch-all.

• Chat (XMPP) (Enterprise Only) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. Note: This feature is only available when licensed with SmarterMail Enterprise.

• Cloud Storage Connections - Select this option to allow users to connect different services, like OneDrive and Dropbox, to their SmarterMail accounts to facilitate actions like attaching links to shared files.

• Disposable Address - Select this option to allow users to create a temporary, disposable address independent of their email address. Disposable addresses are generally short-lived and

are great for use when signing up for newsletters, getting free downloads, etc. as it means a user doens't have to use they're actual email account when signing up to receive things that could end up putting the user on a mailing list.

• Domain Chat History View - Select this option to allow domain administrators to be able to search through all chat history for any and all users of a domain.

• eM Client - Select this option to allow domain administrators to be able to take advantage of the partnership between SmarterTools and eM Client so that they can receive, distribute, and manage a FREE eM Client Pro license with 3 device activations for their users. For more information, see eM Client Licenses .

• File Storage - Select this option to allow users to access the File Storage section, where users can upload files to the mail server and then share them by sending out links to those files.

• Global Address List - Select this option to provide a listing of all users who have accounts for the particular domain in the Contacts menu icon. If the Global Address List is disabled for a domain, collaboration items, like calendars or notes, will not use autocomplete when adding shared users. Note: This feature is only available when licensed with SmarterMail Enterprise. In addition, MAPI requires use of the Global Address List (GAL) in order to work properly. Therefore, regardless of whether the domain's Global Address List feature is disabled, or a user/alias has Show in GAL disabled, Outlook MAPI will always show the GAL directory and be available via autocomplete when typing in a recipient's email address.

• Webmail Login Customization - Select this option to allow domain administrators to customize the login screen to add a company logo, provide additional branding text, or adjust the default "Login to SmarterMail" text. Note: If you enable this feature to allow the domain to override the custom login display, and the domain administrator does not enable customization for their domain, users will see the default SmarterMail login screen, regardless of whether the login display is customized in the system administrator-level general settings.

• Folder Sharing - Enabled by default, disabling this removes the ability to share items, for users and for the domain as a whole. This includes users sharing folders, calendars, contacts, etc. In addition, it disables the ability for domain administrators to create shared resources such as conference rooms, equipment, domain shared calendars and contacts, etc. Note: If sharing was previously enabled, and customers have shared items with others, these shared items will essentially disappear. However, once Enable Sharing is toggled on again, these shares will reappear as long as they have not been removed/unshared by users or domain administrators.

EAS (Enterprise Only)

EAS is the industry standard for synchronizing email clients and mobile devices with email servers like SmarterMail. Using EAS, users can synchronize email, contacts and calendars (and tasks and notes, on supported devices) with email clients, like Windows Mail, and with smartphones and tablets

from Apple, Samsung and others. When trialing the add-on or using a paid subscription, the following options will be available:

• **Remote Wipe** - When enabled, this allows domain administrators to initiate a remote wipe of a device connected via EAS. For example, if a person leaves an organization, administrators can wipe their mobile device(s) to ensure SmarterMail accounts are removed.

• **Allow Domain Administrators to manage EAS for users** - Enable this setting to allow domain administrators to assign EAS to the number of accounts allocated for the domain.

• **Accounts** - The maximum number of EAS accounts that can be assigned for the domain.

MAPI & EWS (Enterprise Only)

MAPI/EWS are both protocols used for connecting desktop email clients to SmarterMail to give them Microsoft Exchange-level functionality. MAPI is used by Microsoft Outlook 2016 and above for Windows machines while EWS is used by Apple Mail on MacOS and eM Client on both Windows and MacOS.

• **Allow Domain Administrators to manage MAPI/EWS for users** - Enable this setting to allow domain administrators to assign MAPI/EWS to the number of accounts allocated for the domain.

• **Accounts** - The maximum number of MAPI/EWS accounts that can be assigned for the domain.

Email

• **Autoresponder Exclusions** - To prevent SmarterMail from sending automated messages, such as out-of-office replies, to addresses based on the spam level of the original message, select the appropriate option from the list.

• **Forwarding Exclusions** - To prevent the system from forwarding messages based on the spam level of the message, select the appropriate option from the list.

• **Enable Greylisting** - Greylisting is a spam prevention method that temporarily rejects any email from an unrecognized sender. The idea is that a valid message will be re-tried and, therefore, accepted on its subsequent delivery attempt. Though effective, greylisting can lead to a delay in email delivery for a domain. Enable this option to activate greylisting for the domain.

• **Enable Sender Verification Shield** - Administrators can choose to enable the Sender Verification Shield for users. This is a way to help a user understand whether the sender is truly the sender or not by performing checks on DMARC, DKIM, and SPF, the trusted sender status, etc.

• **Inbound Message Delivery** - Administrators can specify the domain location for incoming email delivery. This allows you to specify whether the domain is hosted locally or partially/entirely on an external server. The following options are available:

• Local - Select this option if the mail server is hosted locally.

• External (use MX record) - Select this option if the mail server is hosted partially or entirely externally. Messages will be delivered based on an MX lookup. Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.

• External (use host address) - Select this option if the mail server is hosted partially or entirely externally. Messages will be delivered to the specified host address. The host address can either be entered as an IP address or the Fully Qualified Domain Name (FQDN), such as mail.yourdomain.com. Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.

Mailing Lists

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For example, many companies use mailing lists to email newsletters, promotional offers, or information about product updates to subscribers. Unlike an Alias, a mailing list allows people to subscribe or unsubscribe from email communications.

• Mailing Lists - Enable this option to allow domain administrators to create and manage mailing lists for their domain.

• Mailing List Command Address - The address used for responding to mailing list requests. For example, if a request is sent requesting a list of all available commands. By default, this is "listserv", but it can be changed as needed.

• Mailing Lists (0 = Unlimited) - The maximum number of mailing lists allowed for the domain. By default, this setting is set to Unlimited.

• Max Message Size (KB) - The maximum size message that can be sent to a mailing list. By default, the maximum message size is set to 512000 KB.

Security

• Two-Step Authentication - Two-Step Authentication is a method of providing a second verification of ownership before a user can log in or connect to third-party clients and/or devices. For example, when a user has Two-Step Authentication enabled, the SmarterMail login page will require their primary password and a secondary verification of ownership before the user can log into webmail. The second method of verification will be provided to the user through popular authentication apps, like Google or Microsoft Authenticator, or through a recovery email address. When this feature is enabled for a domain, the domain administrator can override the system setting and choose whether to enable or force Two-Step Authentication for their users. Options for Two-Step Authentication include:

• Enable - Simply enables Two-Step Authentication, but users have the option to use it or not. It is not required.

• Forced - This enables Two-Step Authentication and forces/requires users to set it up. However, domain administrators have the ability to disable it for their own users.

• Forced - Prevent Domain Disabling - This makes Two-Step Authentication required and removes the ability for domain administrators to turn it off.

• Enable TLS if supported by the remote server - This enables TLS (SSL encryption) for outgoing mail.

• Enable SRS when forwarding messages - Enable this to allow the mail server to re-email (as opposed to "forward") an email message so that it passes any SPF checks on the recipient's end.

• Require SMTP Authentication - Enable this option to require SMTP authentication when sending email. Note: If this option is enabled, users must provide an email address and password to send email when using an email client. (Webmail is automatically authenticated.) SmarterMail supports cram-md5 and login authentication methods.

• Force all traffic over HTTPS - Select this option to force all SmarterMail traffic over HTTPS. This improves SmarterMail security by allowing all traffic to be encrypted. Note: Prior to enabling this setting, any hostname set up in SmarterMail must have a valid SSL certificate in place. If this is enabled and a user navigates to the IP address, the server will attempt a rDNS lookup and then redirect accordingly.

• Enable HSTS - HTTP Strict Transport Security (HSTS) is a response header that helps protect against main-in-the-middle attacks by informing browsers that the site being accessed should only be accessed using HTTPs, and that any future standard HTTP requests should automatically upgrade to HTTPS. Therefore this setting is used in conjunction with "Force all traffic over HTTPS" and/or if there are web server rules in place to automatically force traffic to HTTPS connections. (E.g, IIS rules)

• Show passwords to domain administrators - Enable this option to allow domain administrators to view a user's password (and app passwords, if the user is protected by Two-Step Authentication). Note that passwords cannot be viewed when the authentication method is set to Active Directory.

Miscellaneous

• Postmaster Mailbox - The system administrator can specify an email address that's used as the postmaster address for a specific domain. If there's no specific postmaster@@ user set up for a domain, then the primary domain administrator address is generally entered here. The Postmaster address is essentially an Alias: if someone emails postmaster@@, the email is forwarded to the address entered here, just as it is for an Alias. If an Account, Alias or Mailing List already exists with the "postmaster" username/name, then this field is ignored.

• Logout URL - Generally, when users logout of webmail they're presented with the standard webmail login page. However, a system administrator can enter a custom URL to a page that is

presented to users when they log out of webmail.

• Allow domain administrators to create domain aliases - Enable this option to allow domain administrators to create domain aliases. A domain alias is basically an alternate domain name for one that already exists in SmarterMail. For example, imagine you have a domain, 'example.com', in SmarterMail with a user, 'user@@example.com'. By adding a domain alias for 'example.net', emails sent to 'user@@example.net' will be delivered to 'user@@example.com'. That means that emails sent to either domain will end up in the same mailbox.

• Allow domain administrators to manage Mailbox Size Limit for users - When this setting is enabled, domain administrators will be able to modify a user's Mailbox Size Limit and propagate the setting to users. When this setting is disabled, domain administrators will be able to see the current Mailbox Size Limit, but they will be unable to edit the value or propagate changes to users. Note: A system administrator will always be able to manage a user's Mailbox Size Limit when impersonating a domain administrator and editing a user.

• Allow users to edit their profile - When enabled, this allows users to manually edit their profile information. (I.e., modify their Display Name, contact information, etc.) It also makes the "Allow users to opt out of Global Address List" setting visible. Note: For Active Directory administrators, or companies who use Active Directory for user administration, this setting can be disabled for all users in Domain Defaults, which means any profile information is "read only" for users and, instead, managed by Active Directory.

• Exclude IP from received line - Select this option to remove the client's IP address from the received header on messages received through SMTP. Note: Removing the IP address from the received header is not recommended because it violates RFC.

Online Meetings Video / WebRTC (Enterprise Only)

Select this option to allow users to create online meetings, which allow for video chatting and shared documents with users on the domain and guests alike. Technical Note: Video conferencing within online meetings utilizes WebRTC. WebRTC will prefer UDP as the communications protocol, but it will use TCP if it's the only available method through the firewall. For ports, WebRTC will use anything in the 0-65535 range to transfer video and audio. In order to establish the connection, port 3478 should be open. In addition, WebRTC uses VP8 or H.264 for video codecs and Opus for audio, though this can vary depending on device, OS and browser. WebRTC handles this selection automatically.

It's also possible to use a separate STUN/TURN server for online meetings versus using the included STUN/TURN server. This is generally best when multiple domains will be using the Online Meetings feature as it offloads these meetings to a separate server. If no servers are specified, SmarterMail will use the default STUN/TURN settings for online meetings.

Priority and Throttling

Use this card to prioritize the remote delivery of standard messages and configure the throttling options for the domain. By default, all messages for all users are sent at a normal priority with the exception of mailing lists, which default to low priority. Messages that fail the first attempt to deliver get automatically "degraded" in priority to low.

Throttling, on the other hand, allows system administrators to limit the number of messages per hour and/or the amount of bandwidth used per hour to send messages, either at the domain level, the user level, or a mix of both. If the throttling action is set to Reject, SmarterMail will bounce any messages attempting to be sent after the threshold is met, until the next session. If the throttling action is set to Delay, SmarterMail will allow the message into the spool and trickle delivery.

The way throttling works is as follows: Anytime an SMTP session is made to deliver a message to any outside user (i.e., not a local delivery), that session counts against the throttling limits that are set. For example, if a user sends 5000 emails to 5000 Gmail users, that's 5000 messages that count against their "Outbound Messages per Hour" throttling limit, if that user has throttling set up, or their domain's throttling limit. However, if they send 5000 emails but 4000 to Gmail users, and 1000 go to other users on their domain, only 4000 messages count as the other 1000 are delivered locally. So, throttling limits are only counted for messages that are sent to another server; throttling limits do NOT count for local deliveries.

There is also a timing element involved with throttling: things like spool delays, delivery delays, etc. can impact whether or not messages count against whatever throttling limits are set. However, those issues are generally few and far between.

- Delivery Priority - The priority level for messages that don't have another priority affecting it.
- Outbound Messages per Hour - The number of messages sent by the domain per hour. By default, the number of outgoing messages is 5,000.
- Message Throttling Action - The action SmarterMail should take when the message throttling threshold is reached.
- Outbound Bandwidth MB per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.
- Bandwidth Throttling Action - The action SmarterMail should take when the bandwidth throttling threshold is reached.
- Bounces Received per Hour - As bounce messages are received from null senders per RFCs, this setting dictates the number of messages from null senders a domain can receive over SMTP before any further messages from null senders will be rejected. By default, a domain can receive 1,000 bounces per hour.

• Bounces Throttling Action - The action SmarterMail should take when the bounces throttling threshold is reached.

Autodiscover

Autodiscover is a service that allows email clients to automatically determine a user's mail server address and port from that user's email address and password alone. This greatly simplifies a user's setup process when attempting to connect SmarterMail to a desktop client, like Outlook and Apple Mail, as well as mobile clients. Autodiscover settings can be configured per protocol and per domain. Instructions on how to Set up Autodiscover for SmarterMail can be found in the SmarterTools Knowledge Base .

With the appropriate DNS records and IIS configuration in place, you can use this section to enable or disable specific protocols from returning Autodiscover results. When a protocol is enabled for Autodiscover, clicking on that protocol's settings cog will open a window where the encryption type and port can be adjusted. Utilizing Autodiscover with MAPI/EWS or EAS requires encryption over SSL or TLS. Therefore, port 443 MUST be available and not blocked by a firewall. note: If a user has POP disabled for their account, their POP Autodiscover request will not be fulfilled, even if POP is enabled for Autodiscover. This applies to all protocols in their account's Service Access settings.

Overriding the Default Desktop and/or Mobile XML Responses

Administrators with advanced Autodiscover knowledge can override the default XML response that is sent from the domain when Autodiscover is requested. However, please understand that these settings should NOT be modified without advanced knowledge of the XML responses used with Autodiscover. Adjusting the custom XML incorrectly can result in invalid responses returned meaning users will be unable to connect to their email client(s). Furthermore, if you turn on an override but never save any custom XML, SmarterMail will use the default protocol settings. However, if the override is turned on, ANY text you save to the Custom XML area will be used for the Autodiscover response. If you save custom text, then later remove that text and save a blank entry, Autodiscover will send a blank response. Therefore, it is imperative that you only enable the override and enter custom Autodiscover XML if you are absolutely sure what you're using is correct.

There are two types of Autodiscover responses that can be modified: Mobile XML and Desktop XML. The mobile XML response is strictly used with EAS. The desktop XML response is used with everything else, including IMAP, POP, SMTP In, MAPI and EWS.

In the textbox window that appears after enabling the override of the XML, clicking on Generate will show the XML response that SmarterMail would normally send on an Autodiscover request. You can generate this response to make adjustments as needed, or simply enter the XML response you would like to use. When adjusting the XML, don't remove or modify variables such as %EmailAddress%,

%Base64EmailAddress%, %DisplayName% or %LegacyDN% since these are used to identify the user making the Autodiscover request. Also note that although changes are not validated by SmarterMail, any changes made to the XML response should be within RFC guidelines.

Propagation

When changes to domain defaults are made, these changes only apply to any new domains that are added AFTER the changes are saved. However, system administrators can make changes to Domain Defaults then propagate those changes to all domains. In order to apply domain settings to all of the existing domains, do the following:

- First, make any changes you want on this page, then click the Save button.
- Next, click on the Propagate button. A modal window opens up.
- Scroll down the list of settings, placing a check mark next to the settings you want to push to your domains. Not all settings need to be propagated, only those settings that have been changed.
- Once you've selected your changes, click the Propagate button.

Changes to Individual Domains

If changes need to be made for individual domains, these can be handled by clicking on the domain from the Domains page, then making modifications using the tabs available to system administrators. For example, if a system administrator wants all domains to have Cloud Storage Connections disabled, but grant Cloud Storage Connections to individual domains, the setting can be disabled on Domain Defaults, but enabled for specific domains on their Options tab.

User Defaults

The job of the system administrator is to make sure that the SmarterMail server runs as efficiently as possible. Part of that responsibility is putting measures in place to limit the potential for system abuses and "user error" that could cause problems.

SmarterMail gives system administrators the ability to create a default template that's used as a starting point for all users of the mail server. This includes the ability to set size limits for mailboxes, delete email actions, set up throttling for users and more. These defaults can be set at any time and will be used for any new users added to the server. These settings can also be propagated to a single domain, multiple domains or all domains on the server so users have the same settings as the new defaults. From here, domain administrators can further lock down user accounts and set their own user limits.

The default user settings are identical to those found when adding or editing a user. For more information on these settings, refer to the Users page.

You can make whatever changes you want to the settings on the User Defaults page, and any NEW domains that are added to the server will have these defaults applied for their users. However, it's also possible to change these settings, then push those settings to one or more domains, or to all domains.

Propagation

To apply some or all of the default user settings to some or all of the existing domains, do the following:

- First, make any changes you want on this page, then click the Save button.
- Next, click on the Propagate button. A modal window opens up.
- Scroll down the list of settings, placing a check mark next to the settings you want to push to your user(s).
- Once all items have been selected, you can pick how you want to propagate the changes:

- Apply to - This gives you the opportunity to select where you want the settings changes to be propagated:

- User Defaults - This will overwrite any existing User Defaults based on the "Push to" option selected. Namely, All Domains or to specific domains listed.
- Users - This will overwrite any existing User settings based on the "Push to" option selected.
- Both - This will overwrite both the User Defaults and any existing user settings.
- Push to

- All Domains - This will propagate the changes to all domains on the server.
- Specific Domains - Selecting this allows you to start entering the domains you want to propagate the changes to. These changes will only propagate to the domains you enter.
- Domain - Allows you to specify the domain(s) within SmarterMail that you want to propagate the settings to. If "All Domains" is selected, this entry is not available. note: the modal does have a scrollbar, so after a domain is entered you may need to scroll down to see the next line to add in a second domain.
- Once you've selected your changes, and added the specific domains you want to propagate the changes to, click the Propagate button. Note: Simply making a change to the User Defaults doesn't automatically propagate, so a change to default settings does not change users that are already in place for any domain. They're only a user template any new domains that are added to the server. In order for changes to take effect, they must be propagated.

Password Requirements

To ensure the security of the mail server and its mailboxes, system administrators can specify minimum requirements for user passwords. This includes things like setting requirements for how a

password is generated (character count, upper/lowercase, etc.) as well as whether passwords expire, whether previous passwords can be used, and more.

These settings are then propagated down to domain administrators who can add to the password requirements for their own users. Domain administrators can not edit any requirements set at the system level, they can only add to those settings. (Any setting configured at the system level will appear greyed out for domain administrators.)

When accessing Password Requirements , the following tabs are available, and each tab has its own cards:

- Options
- Password Violations
- Expired Passwords
- Password Age

Options

This page allows a system administrator to set up the actual requirements users need to follow when creating passwords. These settings, then, are used as the baseline should a domain administrator want to increase the requirements. Note: Domain administrators cannot lessen requirements set by the system administrator, they can only increase the requirements.

Requirements

- Minimum Password Length - Enter the minimum number of characters the password must have.
- At least one number - Select this option to force users to include a number in the password.
- At least one capital letter - Select this option to force users to include a capital letter in the password.
- At least one lowercase letter - Select this option to force users to include a lowercase letter in the password.
- At least one symbol - Select this option to force users to include a symbol in the password.
- May not match username - Select this option to ensure that the username and password do not match.

Options

- Prevent common passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords.

• Prevent previous passwords reuse - Select this option to prevent users from using any previously used passwords.

• Previous Passwords to Block - Some administrators will allow re-use of passwords after a certain amount of time, or after some number of rotations. This number reflects the number of times a new password needs to be used before a password can be re-used. By default, this is set to 0, meaning passwords can never be re-used.

• Skip enforcement for existing passwords - Select this option to skip existing users when making changes to password requirements — meaning the changes will only affect new users or new passwords.

• Enable password retrieval - Select this option to allow users to reset their password if they forget it. Note: In order for users to utilize password retrieval, they must have a Recovery Address configured in their account settings.

Expiration

Password expiration is based on the date/age of the user's current password, NOT when the password expiration setting is enabled. This means that users who have not changed their passwords in a long time will be required to change them almost immediately upon enabling the "Passwords expire automatically" setting.

As an example, let's say you enabled password expiration today and set the threshold to 1 month. This is the expected behavior for the following user scenarios:

• If the user changed their password last week, their password will not be expired. Instead, it will expire in 3 weeks (when the password is 1 month old).

• IF the user changed their password last year, their password is over the 1-month threshold and will be expired immediately.

• If the user was created 2 weeks ago and has never changed their password, their password will not be expired. Instead, it will expire in 2 weeks (when the password is 1 month old).

• If the user was created 2 months ago and has never changed their password, their password is over the 1-month threshold and will be expired immediately.

Initially, "Passwords expire automatically" is disabled. Enabling it offers the following settings:

• Password Expiration (Months) - The number of months that a password is valid. After the specified time, a user's outgoing SMTP will be disabled and a password change will be forced upon Web interface login. Move the slider to the right to enable this setting. note: If a user's 'Disable password changes' setting is enabled, their password will not expire.

• User Notification Timing (Days separated by commas) - The interval(s) used to notify users of when their password will expire or when their auto-block grace period will end and,

subsequently, their outgoing SMTP will be disabled. The default values are 28, 14, 7, 3, 2, 1 days. This means SmarterMail will send out warning messages to the user to change their password 28 days, 14 days, 7 days, 3 days, 2 days and 1 day before their password officially expires or the grace period ends if their password violates the requirements. Note: SmarterMail will send one, single notification for all missed intervals. For example, imagine "Auto-block Grace Period" is set for 30 days and the "User Notification Timing" is set at 60, 45, 25, 10, 2, 1. When a user is in violation, SmarterMail will send a single notification for the 60 and 45-day intervals then continue as normal at the 25-day interval.

• Disable outbound mail after grace period ends - Select this option to disable outgoing SMTP after the auto-block grace period ends when a user's password does not meet the password requirements.

• Auto-block Grace Period (Days) - Available when the "Disable outbound mail..." setting is enabled. This is the number of days a user can wait to update their password before outgoing SMTP is disabled due to password policy violation. Note: This setting only applies if the "Disable outgoing SMTP when auto-block grace period ends" setting is enabled.

Password Violations

The Password Violations tab offers system administrators a way to find users that aren't following the password requirements that have been set up. For any Users who appear on this list, the system administrator is able to either email the users individually, or force their non-compliant password to expire. This latter action means that the user will be forced to change their password the next time they log in to their email account. In addition, it's possible to export a list of the non-compliant users in CSV format.

When Users appear on this page, the following information will be available:

• Username - The username of the non-compliant account

• Two-Step Authentication - Whether the username has Two-Step Authentication enabled.

• Password Changes Disabled - If a specific user has the ability to change their password disabled, their user is marked accordingly in this column.

• Violations - The number of password requirement violations encountered for the User.

Expired Passwords

By default, this tab displays all accounts set up in SmarterMail. The numbers displayed on the tab show the number of passwords that have expired over the total number of accounts set up. For example, that tab may show 10/1232, meaning 10 accounts out of 1232 total have passwords that have expired. This tab could, of course, also show 0/1232 if there are no expired passwords.

Depending on the business rules used by the system administrator, they have some actions that can be performed on each account, which are detailed below. Each account is listed and the following information is displayed:

- Username - The account that is set up.
- Two-Step Authentication - Whether the username has Two-Step Authentication enabled.
- Expired - If the user's password is expired, a check mark appears in this column.
- Password Age - How old the password is. For example, 2 years, 3 days, 15 minutes, etc.

As mentioned, administrators have the ability to take action on users, either users who have expired passwords or users who do not. These actions include:

- Send Email - Opens a modal window that allows the administrator to create, and send, an email to the user(s) informing them that they need to reset their password. However, the administrator can customize the entire message to say what they want.
- Expire Password - Will automatically expire password(s) for the user(s), forcing a change the next time the user attempts to log in.

Password Age

By default, this page will list all users and the respective age of the passwords assigned to each. This allows system administrators to find users who may, due to the age of their password, want to change said password. In addition, it can help find little-used accounts that may be ripe for compromise if their password is over a certain age. Each account is listed and the following information is displayed:

- Username - The account that is set up.
- Two-Step Authentication - Whether the username has Two-Step Authentication enabled.
- Expired - If the user's password is expired, a check mark appears in this column.
- Password Age - How old the password is. For example, 2 years, 3 days, 15 minutes, etc.

Impersonate User

There are times when a system administrator will need to access domain or user specific information. SmarterMail uses impersonation to accomplish this goal. When you impersonate a user, you essentially log in to SmarterMail as them without having to actually log in. This can be a useful method to examine settings or diagnose a problem directly. Note: When a system administrator is impersonating a user, the interface will be displayed using the language that is set for system administrator, NOT in the language of the account/User they are impersonating.

To impersonate a user, do the following:

- Use Impersonate User on the navigation pane. A modal window opens.
- From the modal, select the Domain from the dropdown, then start typing the User's name. If you're already on the Configuration tab for a domain, that domain's name will automatically populate the Domain dropdown in the modal. (However, you can change this if needed.) When you start typing the User's name, SmarterMail should offer some autocomplete options. You can select one of those options or finish typing out the User's name.
- Once you've selected the Domain and User, click the Impersonate button. A new window will open and you'll be logged in as that user. By default, you'll be placed in that User's Settings.
- You can tell you're impersonating a user because an orange "Impersonating" flag is displayed in the upper, right corner of the SmarterMail interface.
- To exit impersonation, you can either log out of the impersonated user or simply close the browser window.

Once impersonating, you are able to edit user/domain settings, content filters, or other settings that need to be changed or reviewed.

Alternatively, you can impersonate a user by going to a Domain's Accounts tab, right-clicking on a user and selecting Impersonate User from the context menu. (Or by selecting "Impersonate User" from the Actions (□) dropdown.)

Changing Impersonated Users

It's also possible to change the User you're impersonating, or even change the domain and user, from the Impersonating window. Simply click the orange Impersonating flag in the upper right corner of the interface and a new Impersonate User modal window opens. Here, you can change the domain or user you want to impersonate and, by clicking the Impersonate button, change to that user or to a new domain and user. note: Only the primary system administrator has impersonation privileges by default. If you are logged in as a secondary system administrator and do not see the Impersonate User menu item in the Navigation pane, then impersonation privileges have not been enabled for your account. Please contact your primary system administrator to request to have "Allow Impersonation" and, in addition, "Allow domain management" enabled for your account.

Message Archive Search

Message archiving is a method of storing all email and live chat traffic for a domain — either inbound messages, outbound messages or both — in a separate location on the mail server. Typically, this feature is used for companies that need mail servers in compliance with the Sarbanes-Oxley Act of 2002 or other regulatory compliance.

It is important to note that message archive search is available to domain administrators only when rules are set for their specific domains. If archiving is set up for "all domains" on a server, then only the system administrators will be able to search the message archive. Therefore, if a domain administrator needs access to the email archive for the domain "example.com", then a message archiving rule specifically for example.com needs to be set by the system administrator.

When using Message Archive Search, administrators can search for a message by domain, date range, the sender's address, the recipient's address, or the subject.

When message archiving is set up for a specific domain, domain administrator can search for a message by date range, the sender's address, the recipient's address, or the subject.

For more detailed information on archiving, see Message Archiving .

Troubleshooting

SmarterMail makes managing the mail server a breeze by isolating the monitoring and management aspects from the setup and configuration. In the Troubleshooting section, administrators can access settings, tools and dashboards that will help them better understand what's occurring on their mail server and quickly take action while troubleshooting any issues that may arise.

A major part of troubleshooting issues is logging. By default, SmarterMail logs virtually every process and protocol available within the system. Having these logs means that, when issues DO occur, administrators can quickly and easily find out the what's going on and get the problems resolved. If nothing else, having access to logs makes working with SmarterTools much easier as it gives our support agents access to information that can then be used to further find and fix issues, or work with our developers to figure out what's going on so a fix can be implemented.

That said, logs CAN take up space on a server. By default, most of SmarterMail's log levels will be defaulted to "Exceptions Only". This means that the logs will capture and write out errors but not details. This keeps the log files small. At the other end of the spectrum, Detailed keeps the most amount of information available, but also means the log files can get quite large, quite quickly. However, this gives administrators the most information possible to help find the root cause of a problem.

System administrators have access to the following Troubleshooting tabs:

- Options - Configure the log and indexing settings for the server
- View Logs - Review the logs to look for errors or monitor recent activity
- Services - Enable or disable specific services, including IMAP, SMTP, etc.

• Mailbox Indexing - View the status of user indexing occurring on the server

• Mailbox Migration - View the mailbox migrations occurring on the server

Options

Use this section to manage how the logs are written and to customize the indexing configuration:

Log Files

• Compress Log Files After - The number of days after which log files are automatically compressed. This preserves existing log files but also saves server space.

• Delete Log Files After - The number of days after which log files are automatically deleted. To enable this automatic deletion of log files.

• Debug Log IDs (one per line) - This section should only be used when instructed by SmarterTools Support. In order to better troubleshoot an issue within SmarterMail, SmarterTools Support may require additional logging. In this section, Debug Log IDs can be entered. Entering a log ID in this box will enable the creation of a separate log file which will contain information Support needs for troubleshooting. To disable a specific log, simply remove it from the list.

Protocol Logging

By default, SmarterMail sets all log detail levels to Exceptions Only. Use this section to adjust the log detail levels for the protocols used with SmarterMail. When set to Exception Only, SmarterMail will produce small-sized logs that record only errors. When set to Normal, SmarterMail will produce medium-sized logs that record most activity taken on the mail server. When set to Detailed, SmarterMail will produce log files that can get very large and contain extensive logging. Only change logs to Detailed when asked by SmarterTools Support or when troubleshooting server operations.

The following log file types can be adjusted:

• Autodiscover - The log level for Autodiscover. Useful for helping figure out why a particular user can't automatically connect to an email client.

• EAS - The log level for EAS connections. Useful for helping find issues with things like why a user on an iPhone is having an issue syncing their calendar properly, etc.

• EWS - The log level for EWS sessions. Useful for helping find issues trying to connect to a client such as Apple Mail.

• IMAP - The log level for IMAP sessions. Useful for helping to figure out why a user can't connect to any email client that supports IMAP.

• LDAP - The log level for LDAP sessions. Useful for helping find issues when using Active Directory as an authentication method.

• MAPI - The log level for MAPI sessions. Useful for helping find issues trying to connect a

user to a client such as Microsoft Outlook 2019 for Windows.

• OAB - The log level for Offline Address Book (OAB). Useful for helping find issues with a user's offline address book, especially when using Microsoft Outlook.

• POP - The log level for POP sessions. Useful for helping to figure out why a user can't connect to any email client that supports IMAP.

• Sharepoint - The log level for Sharepoint Sync (Add to Outlook). Useful for helping to figure out why a client can't connect to any email client that supports Sharepoint Sync.

• SMTP - The log level for SMTP sessions. Useful for helping figure out why a message wasn't delivered to a recipient, and helps ensure the message was, in fact, sent by the user.

• WebDAV - The log level for CalDav and CardDav sessions. Useful for helping to figure out why a calendar or contacts app can't connect to any email client that supports CalDAV or CardDAV.

• XMPP - The log level for Live Chat and online meetings. Useful for helping with issues such as a user that is unable to connect to a live chat client. Note: More detailed logs require more disk space. If you choose a detailed log, you may want to enable the auto-delete setting on the Options tab.

Process Logging

By default, SmarterMail sets all log detail levels to Exceptions Only. Use this section to adjust the log detail levels for common processed within SmarterMail. When set to Exception Only, SmarterMail will produce small-sized logs that record only errors. When set to Normal, SmarterMail will produce medium-sized logs that record most activity taken on the mail server. When set to Detailed, SmarterMail will produce log files that can get very large and contain extensive logging. Only change logs to Detailed when asked by SmarterTools Support or when troubleshooting server operations.

Process Logging can help administrators in a number of ways. For example:

• Delivery Logs can help find out what happened to a particular message: if it was delivered, if it was delivered but rejected due to spam rules, whether it was moved based on a content filter, etc.

• SMTP Logs can show why a message was rejected by the recipient's mail server.

• Administrative Logs can show when a setting was changed, and which system administrator made the change.

The following log file types can be adjusted:

• Administrative - The log level for any changes and/or modifications made by system administrator accounts.

• Calendars - The log level for calendar appointments.

• Content Filtering - The log level for any changes made due to Content Filtering rules.

• Conversion - The log level for any domain that is converted to SmarterMail.

• Delivery - The log level for message delivery and spool operations.

• Error - The log log for capturing any Errors returned by SmarterMail.

• Events - The log level for event sessions put in place for the system or user.

• EWS Retrieval - The log level for EWS retrieval sessions. (This also log information for mailbox migrations.)

• Folder Auto-Clean - The log level for any folder auto-clean rules in place for the system or user.

• IIS - The log level for IIS sessions. This can be helpful for diagnosing issues with the SmarterMail website, app pool, etc.

• IMAP Retrieval - The log level for IMAP retrieval sessions. (This also log information for mailbox migrations.)

• Indexing - The log level for SmarterMail indexing.

• Licensing - The log level for any Licensing issues, such as activation issues.

• Mailing Lists - The log level for items pertaining to Mailing Lists.

• Maintenance - The log level for maintenance tasks performed by SmarterMail.

• Message-ID - The log level for logging Message-ID's of all messages sent to mailing lists.

• POP Retrieval - The log level for POP retrieval sessions. (This also log information for mailbox migrations.)

• Spam Checks - The log level for all Spam Checks set up and in use. Note: More detailed logs require more disk space. If you choose a detailed log, you may want to enable the auto-delete setting on the Log Files tab.

Performance Tuning

Performance Tuning allows a system administrator to manage some settings that may cause an increase in server utilization of memory and CPU. For example, there are several settings surrounding search indexing. Search indexing allows users to instantly find files in their mailbox, including messages, attachments, appointments, contacts, tasks, or notes. Following the initial scan of the server, SmarterMail continually monitors each user's mailbox for changes and then updates the index accordingly. This method of indexing reduces server utilization while increasing the speed with which search results are returned. However, especially on larger installations, search indexing can cause an increase in memory usage. Use this section to adjust the indexing configuration and cache size for your server:

• Max Indexing Threads - The maximum number of threads to use for search indexing. Increasing this value will cause SmarterMail to use more CPU, but will allow the system to simultaneously index more users. (By default, this value is set to 2 less than the server's

processing count. For example, if your server has 32 processors, this value will be set to 30.)
Please note that this value cannot be set to 0.

• Items to Index Per Pass - The number of items to index per user per index attempt. Increasing
this number will increase memory usage and decrease the time it takes to index one user.
However, it will increase the length of time it takes to index many small users if there are a few
large users. (By default, this value is set to 2500.)

• Seconds In Queue Before Indexing - The amount of time a user must be in the indexing queue
before being indexed. This setting provides a buffer for many changes to a mailbox to ensure
the same user is not indexed multiple times. Increasing this number will cause search results to
be delayed further, but will result in indexing heavier users less frequently. (By default, this
value is set to 60.)

• OpenTelemetry Endpoint - This is the URL of the OpenTelemetry collector/receiver set up to
receive data from SmarterMail. Generally, this is in an HTTPS format.

• Config File Cache Size - This is what stores all JSON configuration files in memory. By
default, this is set to Automatic, but will most likely be set to 2GB, initially. This setting should
only be changed when suggested by SmarterTools Support.

• Track Config File Cache Statistics - This is disabled, by default, as it can cause a decrease in
performance due to CPU usage. As with the Config File Cache Size, it should only be enabled
— temporarily — when suggested by SmarterTools Support. Enabling this will start tracking
cache statistics in a performance counter on the system which can then be used to determine if a
change in File Cache Size should be made.

View Logs

Use this section to quickly view the server's log files. Viewing a server's log files, especially when it's
possible to narrow down the type of server action or protocol that is being viewed, allows system
administrators to look for any specific errors that could cause reliability issues on the server or narrow
down reasons why a specific behavior is being seen. For example, system administrators can review
SMTP logs to see if an email was delivered or check ActiveSync logs to see if they can narrow down
synchronization issues between a specific user's mailbox and their mobile device.

When viewing the SmarterMail logs, the following search strings will be available:

• Start and End - The start and end dates for the log files you want to view.

• Type - The type of log file that you would like to view.

• Search - Type the words or phrases should be contained in the log files that SmarterMail
returns.

• Filter - When searching the logs, you can choose whether to display only lines that match the
search definitions or to display related traffic as well. Change this selection from Only Matching

Rows to Display Related Traffic in order to display extra data that occurred within the same session.

To search for a specific log, complete the date range, select the log type, and enter a search string. Then click Search . Any matching log files will be displayed. Note: SmarterMail will only display up to 1MB of any specific log.

To download the entire log file in a .zip format — NOT just search results — click on Download . This allows you to get quick access to a domain's entire log file so that it can be reviewed more thoroughly on a local machine. If you only need the search results, click on Copy to Clipboard to copy the results to your clipboard, then past those results into your favorite text editor. (We recommend Notepad ++)

Services

Use this section to enable and/or disable specific services on the mail server. Generally, all of these services should be enabled. However, there are cases where an administrator may want to disable one or more. For example, a web host or ISP may want to limit users' access to incoming mail to POP only when they connect with an email client in order to conserve disk space on the mail server. In this case, the system administrator would want to stop the IMAP services. Another example would be a mail administrator for a large corporation who doesn't want users to add multiple email accounts and therefore read and reply to email from personal accounts as well as their corporate accounts. In this case, the administrator would want to disable the IMAP Retrieval and POP Retrieval services.

The following services can be enabled or disabled on the server:

- EWS Retrieval - EWS retrieval is similar to IMAP Retrieval except it uses the EWS protocol for downloading messages from Exchange servers as well as from other SmarterMail servers.
- IMAP - A client/server protocol in which email is received and held by the mail server. IMAP requires continual access to the client during the time that it is working with the mail server.
- IMAP Retrieval - With IMAP retrieval, mail is retrieved from external IMAP servers (e.g., another mail server like GMail) and saved in a mailbox on the mail server.
- Indexing - Indexes messages, contacts, calendars, tasks and notes so that users can search for specific mailbox items via the Web interface.
- LDAP (Enterprise Edition Only) - A communication protocol for accessing online directory services. Programs like Outlook and Thunderbird use LDAP to retrieve contact lists from SmarterMail. SmarterMail will validate email addresses for user accounts, aliases, and mailing lists.
- POP - An email protocol in which mail is saved in a mailbox on the mail server. When the end user reads the mail, it is immediately downloaded to the client computer and is no longer

maintained on the mail server.

• POP Retrieval - Similar to IMAP Retrieval, with POP retrieval, mail is retrieved from external POP3 servers and saved in a mailbox on the mail server.

• SMTP - A TCP/IP (Internet) protocol used for sending and receiving email. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending email and either POP or IMAP for receiving messages from their local server.

• Spool - The internal message queue used to deliver messages locally and to remote services.

• XMPP (Enterprise Edition Only) - An open-source IM protocol designed to allow interoperability between different IM client programs. SmarterMail uses this protocol to power its chat functionality in the Web interface and/or third-party chat clients.

To modify the status of a service, select the desired service and click Start or Stop .

Mailbox Indexing

SmarterMail Search Indexing allows users to instantly find any files in the mailbox, including messages, attachments, appointments, contacts, tasks or notes. Following the initial scan of the server, SmarterMail continually monitors each user's mailbox for changes and updates the index accordingly. This method of indexing reduces server utilization while increasing the speed with which search results are returned.

System administrators can use this section to view the status of SmarterMail Search Indexing. Viewing the status of indexing can be beneficial when troubleshooting a problem. For example, if the mail service seems to be using a large amount of CPU, the system administrator can check to see if the cause of the temporary increase in CPU usage is due to indexing.

Mailbox Migrations

SmarterMail's Mailbox Migration tool makes it easy for users to switch email providers by giving them the ability to import emails, contacts, calendars, tasks, and notes to SmarterMail from most third-party mail servers.

That being said, users can do this on their own, with little input from a SmarterMail system administrator. While this normally is not an issue, there are times when an administrator may need to stop a migration altogether. That's where the Mailbox Migrations page comes in.

The following details can be seen for each entry in the list:

• Email Address - The email address of the user performing the migration.

• Status - The status of the migration being performed. The status displayed will be one of the following:

• Queued - The migration was initiated and is waiting to start.

• In Progress - The migration was started and is currently processing.

• Completed - The migration is finished for that user.

To end the selected user's migration, select the user and click on the Actions (□) button and select Cancel Migration . The migration will be stopped, regardless of where it is in process. Mailbox migrations are an "all or nothing" proposition. If a migration is stopped in the middle, none of the migration steps will be finalized, unless the migration showed as "Completed."

For more information on the Mailbox Migration process, including the fields necessary for different migration types, see the Migrating a Mailbox section of a User's Connectivity settings.

In addition, if there are issues with a migration, SmarterMail logs all migration activity. Therefore, a system administrator can check the Mailbox Importing logs for a user to see what happened, and find a resolution.

Reports

Overview

SmarterMail includes several detailed, real-time performance dashboards that supply system administrators with important, on-demand statistics about their server as a whole as well as information on the traffic coming into and going out of, their servers.

Each card, on each dashboard, represents an overview of a specific metric. Clicking on the card takes system administrators to the overall report that gives a more detailed breakdown of what is being displayed. The exception is the general Dashboard, which gives overall information that doesn't have a specific report associated to the metrics shown.

The Dashboards available include:

Dashboard

The first dashboard covers general information on server hardware performance and the mail service.

Cards include:

• Service Uptime

• System Information

- Protocol Activity
- DNS Cache Utilization
- CPU Usage
- Memory Usage
- Messages in Spool

Protocol

This dashboard provides information on message traffic and bandwidth usage across the server, as well as statistics for SMTP, IMAP and POP. Clicking on an individual card opens up the report for that specific item.

Cards include:

- Bandwidth Overview
- Inbound Messages
- Outbound Messages
- Message Traffic
- Message Bandwidth
- Throttled Messages
- SMTP Out Sessions
- SMTP In Sessions
- IMAP Sessions
- POP Sessions

Server Health

This dashboard provides information on server hardware and performance. Clicking on an individual card opens up the report for that specific item.

Cards include:

- Average Hardware Usage
- Drive C: Average Statistics

Security

This dashboard provides information on security-related items such as viruses, abuse detection and more. Clicking on an individual card opens up the report for that specific item.

Cards include:

- IP Connections

> • IDS Violations
>
> • Viruses Caught

<u>Antispam</u>

This dashboard provides information on the various antispam measures in place for the server, including any paid add-ons. Clicking on an individual card opens up the report for that specific item.

Cards include:

> • Inbound Spam
>
> • Cyren Premium Antispam
>
> • Message Sniffer
>
> • SpamAssassin Processing
>
> • Rspamd Processing
>
> • Greylisted Connections
>
> • Outbound Spam Note: Some Dashboard reports are only active on current data. For example, Service Uptime and Disk Average Statistics. Once a service reboots, the current data showing in the report would be lost, or changed, as these statistics are stored in memory only and not stored to disk.

Protocol

Bandwidth Overview

This report tells you the total bandwidth used by all users on the server, per protocol, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period for both incoming and outgoing bandwidth.

A system admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the Step, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the

system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The date the messages were sent.
- SMTP In - The total bandwidth used for incoming messages.
- SMTP Out - The total bandwidth used for outgoing messages.
- IMAP - The total bandwidth used for IMAP traffic. This is generally bandwidth used by email clients connected to the mailbox using IMAP as the connection method.
- POP - The total bandwidth used for POP traffic. This is generally bandwidth used by email clients connected to the mailbox using POP as the connection method.

The primary benefit of this report is when tracking down email abuses. If a particular day shows a significant amount of bandwidth used for sending or receiving messages, there's a good possibility that either a user on a domain is spamming the server or that a user was compromised. If a day shows a significant amount of bandwidth used, the admin can change the report's Mode and pull up the list of domains, then click on that domain to further troubleshoot which user is causing the increased load. Understanding "how" the bandwidth is being used — for example, if IMAP shows a significant increase for a particular user — makes it easier for an admin to track down what exactly is happening and where.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Inbound Messages

This report tells you the total number of inbound messages by all users on the server for whatever time period you specify. There is also a handy chart that displays the trend line for the time period for both inbound messages and inbound spam messages.

A system admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the Step, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The date the messages were received.
- Inbound Messages - The total number of messages received that are NOT spam or NOT from a Trusted Sender.
- Inbound Spam Messages - The total number of messages received that were marked as spam.
- Inbound from Trusted - When viewing a domain's report, this is the total number of messages received that were sent from a Trusted Sender.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

A Note About Inbound and Outbound Message Counts

At the system-level, message Trend reports (i.e., inbound/outbound messages and message traffic reports) are hard to nail down as it comes down to how one defines what inbound and outbound messages are.

- Is an inbound message any message that enters the server? Is it any message received by a local user?
- This, in and of itself, can be debated. Then you factor in things like should system messages count as inbound messages?
- What about messages sent to an alias?
- Is that counted as one message or is it X messages based on how many users are in that alias?

So, it's not an easy question to answer, but SmarterMail makes some assumptions when it comes to calculating trends. These assumptions are why there may be discrepancies in how inbound and outbound messages are calculated at the system level, especially with Trend reports, and why those reports don't match what you see when you look at domain-level reports.

Inbound Messages

The Inbound Message Trend report counts "inbound" messages in two ways:

• They're messages going to a local user, which includes messages generated by the spool, etc. If it's being delivered to a local user it's an inbound email. And,

• They're messages coming in through SMTP, which includes deliveries from external senders and deliveries from local domain users connected to SMTP via IMAP or POP.

Knowing this, you can see where messages can be counted more than once in Trend reports: if a local user sends an email to a local user it's counted ONCE for the SMTP In connection and ONCE for the delivery to the local mailbox.

Additionally, there's external messages that come INTO your server but don't actually reach a local user. Those would count in the Trend report as an inbound message for their SMTP In connectivity, even though they never actually landed in a user's mailbox. For example, when the server is acting as a domain forward gateway, when an automatic-forward exists that deletes after delivery, or when a domain is split onto two servers.

Outbound Messages

Outbound messages follow, essentially, the same logic. For Trend reports, SmarterMail counts any message delivered to a remote recipient once for each recipient of that message. This, then, can be multiple outbound messages for a single sent item as there may be more than one recipient for that message.

From a domain perspective, SmarterMail counts any message from a local sender on a local domain that's processed by the spool. That means that even if a message has multiple recipients, it's only counted once as there's only one message that's processed by the spool.

As an example, If a SmarterMail user sends a single email to 2 different Gmail recipients (2 addresses in the To: field), the Trend report counts that as 2 outbound messages, but the Domain report only counts it as 1, since a single message is being processed by the spool.

Outbound Messages

This report tells you the number of standard messages, spam messages, then total messages which were sent by all domain for whatever time period you specify. There is also a handy chart that displays the trend line for the time period, for each message type that's identified.

An admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The date the messages were sent.
- Outbound Messages - The total number of messages sent that are NOT spam.
- Outbound Spam Messages - The total number of messages you sent that were marked as spam.

- Total Outbound Messages - The total number of outbound messages, including outbound spam messages.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Message Traffic

This report will tell you the number of "legitimate" messages that are being sent and received by all domains on the server. (I.e., messages not categorized as spam.) System administrators may use this report for overage billing, to identify potential spammers on the server or to identify high-usage domains.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the

system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Inbound Messages - The total number of messages the user has received.
- Outbound Messages - The total number of messages the user has sent.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Message Bandwidth

This report tells you the total bandwidth used by all domain on the server for whatever time period you specify. There is also a handy chart that displays the trend line for the time period for both data sent and data received.

An admin can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The date the messages were sent.
- Data Sent - The total bandwidth used for outgoing messages.
- Data Received - The total bandwidth used for incoming messages.

The primary benefit of this report is when tracking down email abuses. If a particular day shows a significant amount of bandwidth used for sending messages, there's a good possibility that either a user

is spamming the server or that a user was compromised. If a day shows a significant amount of bandwidth used, the domain admin can change the report's Mode and pull up the list of mailboxes to further troubleshoot which user is causing the increased load.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

SMTP In Sessions

This report tells you the number of connections plus the different types of issues reported from SMTP incoming mail for your specific domain. System administrators may use this report to identify high usage accounts, or accounts that have seen particular types of issues. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The day of the week covered by the report.
- New Connections - The total number of overall, inbound connections to the mail server on that day.
- Blocked Connections - The number of inbound connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.
- Bad Commands - This is the total number of connections that had invalid SMTP commands, poor syntax, etc.
- Terminations - The total number of permanent errors for incoming messages due to spam

weight, too many recipients, bad commands, etc.

• Bandwidth - The total amount of bandwidth used for all connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

SMTP Out Sessions

This report tells you the number of connections plus the different types of issues reported from SMTP outgoing mail for all domains on the server. Administrators may use this report to identify high usage domains, or individual accounts that have seen particular types of issues. This information can be used to evaluate whether to move such domains to another server or to set limits on domains or individual accounts. This report can also be used to find potentially compromised accounts because the administrator would see a jump in outgoing SMTP connections over time, and possible a jump in errors.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

• Day - The day of the week covered by the report.
• New Connections - The total number of overall outgoing connections from the mail server on that day.
• Blocked Connections - The number of outgoing connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.
• Bad Commands - The total number of connections that had invalid SMTP commands, poor

syntax, etc.

• Terminations - The total number of permanent errors for outgoing messages due to spam weight, too many recipients, bad commands, etc.

• Bandwidth - The total amount of bandwidth used for all connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

IMAP Sessions

This report tells you the number of connections plus the different types of issues reported for clients or other services connected to user accounts using the IMAP protocol. Administrators may use this report to identify high usage domains, or individual accounts that have seen particular types of issues. This information can be used to evaluate whether to move such domains to another server or to set limits on domains or particular accounts. This report can also be used to find potentially compromised accounts because the administrator would see a jump in outgoing IMAP connections over time, and possible a jump in errors, for a domain. Then they can dig into that domain to find potentially compromised accounts.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

• Day - The day of the week covered by the report.

• New Connections - The total number of IMAP connections from the mail server on that day.

• Blocked Connections - The number of IMAP connections blocked due to IDS rules, SMTP

blacklist, blocked senders, etc.

• Bad Commands - The total number of IMAP connections that had invalid SMTP commands, poor syntax, etc.

• Terminations - The total number of permanent errors for IMAP messages due to spam weight, too many recipients, bad commands, etc.

• Bandwidth - The total amount of bandwidth used for all IMAP connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

POP Sessions

This report tells you the number of connections plus the different types of issues reported for clients or other services connected to user accounts using the POP3 protocol. Administrators may use this report to identify high usage domains, or individual accounts that have seen particular types of issues. This information can be used to evaluate whether to move such domains to another server or to set limits on such domains or accounts. This report can also be used to find potentially compromised accounts because the administrator would see a jump in outgoing POP connections over time, and possible a jump in errors for a domain. Then they can dig into that domain to find potentially compromised accounts.

A domain administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Domain Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

• Day - The day of the week covered by the report.

• New Connections - The total number of POP connections from the mail server on that day.

• Blocked Connections - The number of POP connections blocked due to IDS rules, SMTP blacklist, blocked senders, etc.

• Bad Commands - The total number of POP connections that had invalid SMTP commands, poor syntax, etc.

• Terminations - The total number of permanent errors for POP messages due to spam weight, too many recipients, bad commands, etc.

• Bandwidth - The total amount of bandwidth used for all POP connections.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Throttled Messages

This report shows the number of messages that have been throttled for domains, for whatever time period you specify. There is also a handy chart that displays the trend line for the time period.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

Administrators may use this report to identify issues with high usage domains, and then individual users. For example, if a user is sending a high number of messages, and is, therefore, hitting a throttling threshold, that is an unnecessary use of system resources that can be easily corrected.

The following report items are available:

- Day - The day of the week covered by the report.
- Throttled - The total number of messages throttled by the server.
- Delayed - The total number of messages that were delayed — or not sent out immediately — due to a throttling violation.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Server Health

Average Hardware Usage

This report provides statistics regarding average CPU and memory usage on the SmarterMail server. System administrators may use this report to correlate high CPU and/or memory usage on the server with SmarterMail activity and identify areas in which adjustments can be made. Ideally, SmarterMail will use a small percentage of the overall CPU and memory available on the server. However, there can be spikes during times of high activity, such as when a domain sends a large number of messages, like a newsletter going to tens of thousands of customers.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- CPU - The average percentage of CPU used.
- Memory - The average amount of memory used.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want. Note: Average Hardware Usage is just that: an average. Therefore, if your CPU doesn't spike or isn't running high enough it is possible this report won't show any usage data.

Drive C: Average Statistics

This report provides statistics regarding input/output operations of the system's hard drive, also known as "disk i/o". System administrators may use this report to correlate high disk usage on the server with SmarterMail activity and identify areas in which adjustments can be made.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Read - The average size in KB/sec of disk reads.
- Write - The average size in KB/sec of disk writes.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Security

Viruses Caught

SmarterMail comes equipped with powerful antivirus using ClamAV. ClamAV is an open-source antivirus engine for detecting trojans, viruses, malware, and other malicious threats. SmarterMail also can be used in conjunction with Windows Defender, Microsoft's anti-malware engine that comes standard on most Windows servers. System administrators can also integrate SmarterMail with Cyren's Zero-hour Outbreak Detection, a complementary solution that can help detect, and handle, new outbreaks well before their signatures have been added to more traditional antivirus products. System administrators can, therefore, use this report to see how efficiently the various antivirus products in use are handling malware.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is

sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- ClamAV - The total number of viruses detected and handled by ClamAV.
- Cyren Zero-hour Outbreak Detection - The total number of viruses detected and handled by Cyren, if it's in use.
- Microsoft Defender - The total number of viruses detected and handled by Windows Defender, if it's in use.
- Viruses Caught - The total number of viruses caught by all antivirus products in use.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

IDS Violations

This report shows the number of attacks on the server. For example, if a system administrator notices an increase in DOS or harvesting violations, he may review server logs to determine the IP address that is triggering the violations and consider permanently blocking the IP.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The day of the week covered by the report.
- Brute Force by Email - The number of brute force attacks handled that come in for one or more email addresses. (E.g., login attempts.)
- Brute Force by IP - The number of brute force attacks handled that come in from one or more IP addresses.
- DoS - The total number of Denial of Service (DoS) violations.
- Harvesting - The total number of harvesting violations.
- Internal Spammer - The total number of spam violations from users on the SmarterMail server.

• Password Retrieval - The number of "Forgot Password" attempts that were handled.

• Spammer by Bounces - The number of users quarantined or disabled who have sent a large number of messages that received bounces. (This could indicate spamming.)

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

IP Connections

SmarterMail includes several detailed, real-time performance dashboards that supply system administrators with important, on-demand statistics about their server as a whole as well as information on the traffic coming into and going out of, their servers.

Each card, on each dashboard, represents an overview of a specific metric. Clicking on the card takes system administrators to the overall report that gives a more detailed breakdown of what is being displayed. The exception is the general Dashboard, which gives overall information that doesn't have a specific report associated to the metrics shown.

The Dashboards available include:

Dashboard

The first dashboard covers general information on server hardware performance and the mail service.

Cards include:

• Service Uptime
• Protocol Activity
• DNS Cache Utilization
• CPU Usage
• Memory Usage
• Messages in Spool

Protocol

This dashboard provides information on message traffic and bandwidth usage across the server, as well as statistics for SMTP, IMAP and POP. Clicking on an individual card opens up the report for that specific item.

Cards include:

- Bandwidth Overview
- Inbound Messages
- Outbound Messages
- Message Traffic
- Message Bandwidth
- Throttled Messages
- SMTP Out Sessions
- SMTP In Sessions
- IMAP Sessions
- POP Sessions

Server Health

This dashboard provides information on server hardware and performance. Clicking on an individual card opens up the report for that specific item.

Cards include:

- Average Hardware Usage
- Drive C: Average Statistics

Security

This dashboard provides information on security-related items such as viruses, abuse detection and more. Clicking on an individual card opens up the report for that specific item.

Cards include:

- IP Connections
- IDS Violations
- Viruses Caught

Antispam

This dashboard provides information on the various antispam measures in place for the server, including any paid add-ons. Clicking on an individual card opens up the report for that specific item.

Cards include:

- Inbound Spam
- Cyren Premium Antispam
- Message Sniffer
- SpamAssassin Processing
- Rspamd Processing

• Greylisted Connections

• Outbound Spam Note: Some Dashboard reports are only active on current data. For example, Service Uptime and Disk Average Statistics. Once a service reboots, the current data showing in the report would be lost, or changed, as these statistics are stored in memory only and not stored to disk.

Antispam

Inbound Spam

This report tells you the number of spam messages which were received at different tolerance levels for domains on the server. (And for individual domains.) There is also a handy chart that displays the trend line for the time period.There is also a handy chart that displays the trend line for the time period.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

• Day - The day of the week covered by the report.

• Spam Low - The total number of messages received with a low spam tolerance level.

• Spam Medium - The total number of messages received with a medium spam tolerance level.

• Spam High - The total number of messages received with a high spam tolerance level.

• Spam Total - The total number of messages received will any spam tolerance level assigned to it.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right

hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Outbound Spam

This report tells you the number of outgoing messages that were blocked due to spam for all domains on your server. System administrators can use this report to determine if the server is sending out a large amount of spam, then use the Mode to see which domain is potentially responsible.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour (when viewing a domain's detail), day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Outbound Spam Messages - The total number of messages that were sent and blocked as spam.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want. Note: The system administrator must enable outgoing spam checks or this report will not contain data.

Greylisted Connections

This report tells you the number of allowed connections and delayed connections for all messages sent to all domains on the server, for whatever time period you specify. Blocked connections would be those that were greylisted, meaning there was a slight delay between when the message was sent and

when it was actually delivered. There is also a handy chart that displays the trend line for the time period.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

System Admins can also switch the report from a "Trend" report, which shows the data for the server as a whole, or display information by Domain. This is called the report's "Mode". Changing the mode to display information by domain also allows a system admin to dig into that specific domain, by clicking on its name, to view the report just as a domain admin would view the report. This means the system admin can delve into individual user data simply by changing the Mode, again, to view the report by User.

The following report items are available:

- Day - The day of the week covered by the report.
- Passed - The total number of messages that passed greylisting and were delivered to the mailbox without delay.
- Blocked - The total number of messages that were delayed due to greylisting.
- Total - The total number of connections made to the domain. (I.e., SMTP, POP, IMAP, etc.)

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Cyren Premium Antispam

Cyren Premium Antispam is a paid add-on to SmarterMail that uses Cyren's patented Remote Pattern Detection (RPD) technology to help catch messages categorized as spam, suspected as spam, or categorized as Bulk messaging. It also includes Cyren's IP Reputation service to help classify IP addresses that are known as being used for spamming and sending bulk email. Therefore, System Administrators can use this report to see how much spam Cyren actually catches and categorizes. This can help determine the efficiency and efficacy of using Cyren.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a

quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Confirmed - The total number of messages that were confirmed to be spam by Cyren, and scored accordingly.
- Suspected - The total number of messages Cyren deemed as "suspect" — not confirmed but potentially spam.
- Bulk - The total number of messages Cyren deemed as being bulk email — that is, not spam per se but newsletters, etc.
- Unknown - The total number of messages Cyren was unable to confirm as spam, suspect, or bulk email.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Message Sniffer

Message Sniffer is a paid add-on to SmarterMail that uses advanced pattern detection and collaborative learning technologies to accurately identify spam, scams, viruses, and other email borne malware before it hits inboxes. Therefore, System Administrators can use this report to see how much spam Message Sniffer actually catches and categorizes. This can help determine the efficiency and efficacy of using Message Sniffer.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Confirmed - The total number of messages that Message Sniffer confirmed were blocked as

spam.

- Unknown - The total number of messages that Message Sniffer was unable to confirm as spam.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

SpamAssassin Processing

SpamAssassin is the #1 Open Source antispam platform giving system administrators a filter to classify email and block spam (unsolicited bulk email). It uses a robust scoring framework and plug-ins to integrate a wide range of advanced heuristic and statistical analysis tests on email headers and body text including text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases. It is included in SmarterMail, for free, and is a powerful part of SmarterMail's included spam fighting capabilities. However, it can also be run remotely. As SpamAssassin is open-source, and available from the Apache SpamAssassin Project, many administrators will run SpamAssassin separately from SmarterMail on Linux servers. As a result, this report tells an administrator how efficiently SpamAssassin is running on a remote server by detailing the number of successful and failed connections to the remote SpamAssassin service.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Successful Connections - The total number of successful connections to the remote server.
- Failed Connections - The total number of failed connections to the remote server.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Rspamd Processing

Rspamd is an advanced spam filtering system that allows evaluation of messages by a number of rules including regular expressions, statistical analysis and custom services such as URL black lists. Each message is analysed by Rspamd and given a spam score. According to this spam score and the user's settings, Rspamd recommends an action for the MTA to apply to the message, for example, to pass, reject or add a header. Rspamd is designed to process hundreds of messages per second simultaneously, and provides a number of useful features. As Rspamd is open-source, many administrators will run it separate from SmarterMail as a remote service on Linux servers. As a result, this report tells an administrator how efficiently Rspamd is running on a remote server by detailing the number of successful and failed connections to the remote SpamAssassin service.

An administrator can change the dates of the report as well as the "Step", which means whether you want to see the report by hour, day, week, month or quarter. (Based on the start and end dates — so a quarterly report would need a full 3 months selected.) Admins can change the chart type by clicking the chart icon next to the date, or even export the report as needed. Each column in the report is sortable, either ascending or descending, and the sort can change simply by clicking the column header.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Successful Connections - The total number of successful connections to the remote server.
- Failed Connections - The total number of failed connections to the remote server.

It's also possible to export this data in CSV format for use in other applications, such as Microsoft Excel, Google Sheets, Apple Numbers, etc. To do this, simply click the page icon in the upper right hand corner of the reports page. Once clicked, you'll be able to save the data and name the file to whatever you want.

Settings

Administrators

SmarterMail allows a single installation to have multiple system administrator logins, each with their own unique login and password. Once the page loads, you'll see a list of the administrators that are set up for the SmarterMail installation.

Administrators

Initially, there will be a single "Primary" administrator showing. As new administrative accounts are created, they will also be displayed. By default, the following columns are displayed:

- Account - The login name associated with the account.
- Name - The friendly name associated with the account.
- Type - The account type: Primary Administrator or Administrator.
- Manage Admins - If the administrative user has been granted permissions to create/manage other administrative accounts, a checkbox will appear next to their name.
- IP Restrictions - If the administrative user is restricted to connecting from a specific IP address, or an IP range, a checkbox will appear next to their name.
- Created - The creation date/time of the administrative user.
- Enabled - Whether the specific user is enabled or disabled. No checkmark means disabled.
- Last Login - The date/time the specific user last logged into.

Password Requirements

SmarterTools gives primary system administrators the ability to set password requirements for any other system administrator that's created. This can help ensure that administrators create strong passwords since their accounts hold the keys to the entire SmarterMail system.

Requirements

- Minimum Password Length - Enter the minimum number of characters the password must have.
- At least one number - Select this option to force users to include a number in the password.
- At least one capital letter - Select this option to force users to include a capital letter in the password.
- At least one lowercase letter - Select this option to force users to include a lowercase letter in the password.
- At least one symbol - Select this option to force users to include a symbol in the password.
- May not match username - Select this option to ensure that the username and password do not match.

Options

- Prevent common passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords.
- Prevent previous passwords reuse - Select this option to prevent users from using any previously used passwords.

• Previous Passwords to Block - Some administrators will allow re-use of passwords after a certain amount of time, or after some number of rotations. This number reflects the number of times a new password needs to be used before a password can be re-used. By default, this is set to 0, meaning passwords can never be re-used.

• Skip enforcement for existing passwords - Select this option to skip existing users when making changes to password requirements — meaning the changes will only affect new users or new passwords.

• Enable password retrieval - Select this option to allow users to reset their password if they forget it. note: In order for users to utilize password retrieval, they must have a Recovery Address configured in their account settings.

Adding New Administrators

To create a new administrator, click the New button. Note: Only the primary administrator and secondary administrators with 'Manage secondary administrators' permission can create new or modify existing administrators.

When adding or editing an administrator, the following settings will be available:

Options

• Username - The identifier used to log in to SmarterMail.

• New Password - The password used to log in to SmarterMail.

• Confirm Password - Re-type the password used to log in to SmarterMail.

• Display Name - A friendly name for the administrator. For example, "Dan Henderson".

• Status - Enabled or Disabled.

• Language - The language to be used by the system administrator. The language set for a system administrator is EXTREMELY important. That's because it's much more than simply what is seen in the webmail interface. SmarterMail's language selection is the basis for everything: the things seen in the webmail interface as well as what's returned to an email client when connecting using Outlook, eM Client, iOS Mail and more. That includes things like settings labels, folder names, calendars and calendar appointment, contact groups, email message content, log files and essentially everything within SmarterMail. Therefore, it is extremely critical that whatever language is set in SmarterMail is the exact language the system administrator is going to use.

• Manage secondary administrators - Select this option to allow the administrator to create new and modify existing administrator accounts. This setting is dependent on "Allow system settings management", so if that is disabled, this setting is as well. A system administrator is not able to

manage secondary administrators if they do NOT have the ability to manage system settings.

• Allow impersonation - Select this option to allow the administrator to impersonate a user. Impersonating a user opens a new browser session that allows an administrator to be "logged in" as that user.

• Allow show passwords while impersonating - User passwords are hidden, by default. Select this option to allow an administrator with impersonation permissions to also view the passwords associated with users. This option also allows the administrator to retrieve passwords via the API. Note: The primary system administrator can view and retrieve user passwords and app passwords by default. In addition, when using Active Directory authentication, passwords are NOT displayed.

• Restrict login access by IP - Select this option to only allow the administrator to log in from certain IP addresses. Then enter the authorized IP address(es) on the IP Restrictions card.

• Force two-step authentication - Select this option (if not already set for all administrators) to enable two-step authentication for this administrator.

Two-Step Authentication

Two-Step Authentication is a great way to further secure the logins for system administrators.

IP Restrictions

If an administrator has "Restrict login access by IP" enabled for their account, this is where you add any IP addresses that are allowed access to the SmarterMail server.

Change Password

Administrators can reset their password at any time by logging into the web interface. In addition, the primary system administrator and administrators with "Manage secondary administrators" permission can modify another administrator's password. To modify an administrator password, select the administrator and click the Change Password button. Then enter and confirm the new password that will be used. Note: Secondary administrators cannot modify any settings for the primary administrator.

Primary administrators who cannot remember their password can find instructions to reset their username and password in the SmarterTools Knowledge Base .

Antispam

Antispam Options

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combating spam. Default antispam settings were configured during installation, but these settings can be modified at any time.

Due to the flexible nature of SmarterMail's antispam setup, spam checks can influence the spam decision as much or little as you want. When spam protection runs on a particular message, all enabled spam checks are performed on the message. The total weight of all failed tests is what comprises the ultimate spam weight for the message. A spam probability level is then assigned to the email using the Filtering settings and an action is taken on that message based on its total spam weight.

An added benefit to SmarterMail's antispam administration is the ability to combat both inbound and outbound spam messages. Most mail servers only allow system administrators to keep spam from entering the mail server. However, system administrators can set up global filtering rules, but allow domain administrators to override those settings to help protect their own users. Regardless of who manages the settings, SmarterMail helps protect mail users from inbound spam but also keeps mail servers from actually sending spam, thereby helping to protect the mail servers from being blacklisted.

On the Options tab, the following settings will be available:

Actions (□) Button

　　• Import/Export Settings - Import or export a JSON file containing a server's antispam configuration
　　• Reset Antispam Settings - Reset the antispam options and spam checks to the default configuration

Cards

　　• Filtering - Define the weight thresholds and default actions for each spam level.
　　• Trusted Senders - Exempt specific email addresses or domains from spam filtering.
　　• SMTP Blocking - Configure the thresholds for blocking inbound and outbound spam messages

　　• Options - Adjust basic options relating to the processing of spam and the ability for individual domains to override system-level settings.
　　• DMARC - Enable or disable use of DMARC.
　　• Greylisting Options - Temporarily reject email from unrecognized senders.
　　• Remote SpamAssassin Servers - Configure an external SpamAssassin server for identifying

and reporting spam.

> • Remote Rspamd Servers - Configure remote Rspamd servers for identifying and reporting spam.

Import or Export Spam Settings

SmarterMail can export all global spam settings as a single JSON file then allows that JSON file to be imported to other SmarterMail servers as needed. This means system administrators can configure a solid set of antispam rules on one server, then easily move those settings over to any additional SmarterMail servers by importing the antispam JSON. Email administrators can even work together to create and share their antispam JSON files, combining their experience and understanding to create the most reliable settings available.

It's important to note that the spamConfig.json file is not actually part of the SmarterMail system files — it's generated during export by pulling individual spam settings from the Settings.json file. These settings are then merged with existing Settings.json files when the spamConfig.json file is imported. Therefore, spamConfig.json files can only be shared between servers running the same version of SmarterMail.

To import or export SmarterMail's spamConfig.json file, click on the Actions (▢) button. Then click on Import Spam Settings or Export Spam Settings accordingly. When importing spam configurations, custom rules in the JSON will be merged with existing rules in SmarterMail; the imported JSON will not replace all existing rules. For example, if you import an JSON from another system, it will simply add any custom spam checks, RBLs and URIBLs that do not exist in SmarterMail. If you prefer that all existing rules are overwritten, you must delete those rules prior to importing.

Reset Antispam Settings

SmarterMail's antispam configuration can easily be reset to the default configuration by clicking on the Actions (▢) button and selecting Reset Antispam Settings . Note that this reset will impact ALL sections of the Antispam area, with the exception of IP Bypasses. Resetting the antispam options will revert all settings on the Options tab, Spam Checks tab, RBLs tab, URIBLs tab, and Greylist Filters tab to their default configuration. This means all trusted senders and domains, SpamAssassin servers, custom spam checks/RBLs/URIBLs and greylist filters will be deleted. To confirm that you would like to erase all customized antispam options, click Reset on the confirmation modal.

Filtering

Emails are filtered into one of three categories based on their total weight: Low Probability of Being Spam, Medium Probability of Being Spam and High Probability of Being Spam. For example, if an

email's spam weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use this section to define the weight thresholds and the default actions at each level.

- • Allow domains to override spam settings - Many domain administrators have their own preference of how potential spam email should be handled for their domain. Enable this to allow them to override the spam filtering actions, if they wish. Note: Enabling this will NOT allow domain administrators to manage the spam Weights — they can only manage how they want messages flagged as spam, based on the weights set by the system administrator, to be handled.
- • Weight - The email is sorted into probability levels based on the weight threshold values. Adjust the weight threshold according to the probability status selected.
- • Action - The action to take when a message ends up with this level of spam probability: No Action, Delete Message, Move to Junk Email Folder or Add Text to Subject. Note: The Delete Message action will permanently delete messages that match the corresponding weight, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via spam filtering cannot be recovered.
- • Text to Add - If the Action is set to Add Text to Subject, enter the text that will be appended to the beginning of a subject when a message reaches a particular level of spam.

Trusted Senders

Use this section to globally exempt specific email addresses (such as jsmith@@example.com) or domains (such as example.com) from SmarterMail's spam filtering. This lets the system know that these messages come from a trusted source and can prevent mail from friends, business associates and mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's Contacts list is considered a trusted sender and bypasses spam filtering.

If the system administrator has enabled SPF, DKIM, and/or DMARC, (all of which are strongly recommended), SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses, and IP bypasses. This "trust but verify" approach is important because anyone can write any return path that they want when sending a message. Therefore, this extra layer of protection helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender. If an SPF, DKIM, or DMARC check fails on an incoming message, the "trusted sender" is no longer trusted by SmarterMail, and the weights of all enabled spam checks will be applied to that message.

DMARC, specifically, plays an integral part in determining "trusted" status. DMARC is the only check available that can confirm that the From address listed in the email is associated to the SPF record and return path. DMARC, therefore, ensures that the From address wasn't spoofed and the sender automatically trusted just because the From address is listed as a trusted sender. It is an extra step of security to ensure that senders are only 'whitelisted' if SmarterMail can verify the sender.

The specific spam check results that will bypass the trusted sender status are SPF_Fail, SPF_Softfail, SPF_PermError, or DKIM_Fail.

If the trusted sender status of an email was bypassed due to a failed SPF or DKIM check, the TotalSpamWeight line in the email header would appear in the following format:

```
X-SmarterMail-TotalSpamWeight: {Total Spam Weight} ({Where the trusted
sender status originates}, {Reason the trusted sender status was bypassed})
```

For example:

```
X-SmarterMail-TotalSpamWeight: 9 (Trusted Sender - Domain, failed SPF)
```

This example indicates that the sender is in the domain-level Trusted Senders list, but the email received a total spam weight of 9 because the message failed the SPF check.

Regarding DMARC

We evaluate the DMARC results of an incoming email in order to determine whether the From Address or Return Path will be used for the Trusted Sender verification. If DMARC has a passing result, SmarterMail will use the From Address to determine if the email is in the Trusted Sender's list. In most cases, the Return Path and From Address of an email are the same, and users will likely have the sender's From Address in their Trusted Senders list. In these cases, as long as SPF and DKIM don't fail or error, the email should be delivered to the user's Inbox without a spam weight applied. If DMARC doesn't have a passing result, it will use the Return Path to determine if the email is from a Trusted Sender. If the Return Path address is in the Trusted Senders list as well, the email should be delivered to the user's Inbox without a spam weight applied. If the Return Path address isn't in the user's Trusted Sender's list, the full spam weight of the message will be applied, and the email will be filtered / moved according to the user's spam filtering settings. In these situations, the message will likely land in the Junk Email folder, and the X-SmarterMail-TotalSpamWeight header will show why the weight was applied, with something like this:

```
X-SmarterMail-TotalSpamWeight: 37 (Trusted Sender - User, DMARC: None)
```

```
X-SmarterMail-TotalSpamWeight: 24 (Trusted Sender - User, DMARC: Skipped -
DMARC Disabled)
```

These are the DMARC results that are considered "passing" and will allow the From Address to be considered in the Trusted Sender verification process:

- DMARC: [passed]
- DMARC: [skipped - Authenticated] This will appear if the sender is an authenticated domain user or if the sender's IP address is in the whitelist with an SMTP Auth Bypass.
- DMARC: [skipped - Bypassed] This will appear if the sender's IP address is in the IP Bypass

with Bypass Spam Checks enabled, and there is only 1 Received line in the email
header/delivery.
• DMARC: [skipped - Whitelisted] This will appear if the sender's IP address is in the Whitelist
with an SMTP Spam Bypass.

These are the DMARC results that are not considered "passing", and will disallow the From Address
from being considered in the Trusted Sender verification process.

• DMARC: [none]

• DMARC: [failed]

• DMARC: [skipped - DMARC Disabled]

• DMARC: [skipped - No Return Path]

We also added this logic for adding or removing Trusted Senders from within the Email section:

• If Return and From match, then we add/remove the From Address.

• If Return and From differ, we look at the DMARC Results of that email.

• If DMARC passed (or was skipped due to authentication, bypass or whitelist), we add/remove
the From Address.

• If DMARC didn't pass, we add/remove the From Address and the Return Path address. (This is
done to help ensure that the sender will pass the DMARC Trusted Sender verification process
on subsequent messages.)

SMTP Blocking

The idea behind SMTP blocking of inbound and outbound email is to filter out spam messages before
they can be delivered. With SMTP Blocking enabled, messages that are rejected don't even hit the
spool. That means that they can't be delivered, but it also means they bypass any other function, like
content filtering and even message archiving. This is because messages rejected due to SMTP blocks
simply don't exist to SmarterMail, so they aren't processed in any way by the server. Therefore, it's
important to exercise caution when enabling SMTP Blocking as rejected messages can not be
recovered.

Regarding the weight calculation, when setting up your Spam Checks, RBLs and URIBLs you have
the ability to enable each of those for Inbound and/or Outbound SMTP. When enabled for either
inbound or outbound, SmarterMail uses the weights associated with those various checks when
determining whether a message should be blocked at the SMTP level or not.

For example, imagine you have four spam checks enabled for Inbound SMTP blocking and each of
those spam checks have a weight of 10. If the Inbound Weight Threshold is set to 30, that means
incoming messages will be rejected if they fail at least three of the four spam checks.

• Inbound Weight Threshold - By enabling this field, an inbound email must have a total spam weight score of this value or higher in order to be blocked. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 50 and is disabled.)

• Greylist Weight Threshold - By enabling this field, an inbound email must have a total spam weight score of this value or higher in order to be greylisted. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 30 and is disabled.)

• Outbound Weight Threshold - By enabling this field, an outbound email must have a total spam weight score of this value or higher in order to be blocked. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 30 and is disabled.)

• Outbound Block Action - This setting is used in conjunction with the Outbound Weight Threshold and allows administrators to quarantine outgoing messages that have met the specified spam weight threshold or block them entirely. When Quarantine Message is selected, messages are quarantined for 30 days. (The quarantine period cannot be changed.) The quarantine can be found by clicking on the Manage icon, clicking on Spool in the navigation pane, then selecting the Spam Quarantine tab.

• Bounce messages when blocked by Outbound SMTP Blocking - Enable this to send a user a bounce email notification when their outbound message has not been sent due to its spam probability.

Options

• Autoresponders - This setting allows you to add restrictions to a user's ability to create or send autoresponders outside of the domain. (Autoresponders sent locally, to others on your domain, are not affected by these settings.) Certain antispam organizations will block servers that auto-respond to spam traps. To reduce the possibility of this occurring, set the autoresponder option to be as restrictive as your clients will permit:

• Enabled - Users' autoresponder messages will be sent without any restrictions.

• Disabled - Users will not have the ability to configure an autoresponder.

• Require message pass SPF - A user's autoresponder will not be sent if the original sender's message failed the SPF spam check or if the sender's SPF record is not configured. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the user's autoresponder from being sent if the original sender's SPF record is not configured or if the SPF check has failed. Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, autoresponder messages will not be sent. (By default, this option is selected.)

• Require message pass SPF if SPF record exists - A user's autoresponder will not be sent if the original sender's message failed the SPF spam check. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the user's autoresponder from being sent if the original sender's SPF check fails. (This option is distinguishable from the option above as it will only impact messages where the SPF record IS configured and fails the check. If the original sender doesn't have SPF configured, the autoresponder message will be sent.) Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, autoresponder messages will not be sent.

• Content Filter Bouncing - This setting allows you to add restrictions to the content filter action 'Bounce message'. Certain antispam organizations will block servers that send bounce messages back to spam traps. To reduce the possibility of this occurring, set the bounce option to be as restrictive as your clients will permit:

• Enabled - Content Filter bounces are enabled without any restrictions.

• Disabled -Content Filter bounces are disabled.

• Require message pass SPF - An incoming message that triggers the content filter will not have the bounce message sent if the original sender's message failed the SPF spam check or if the sender's SPF record is not configured. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the bounce message from being sent if the original sender's SPF record is not configured or if the SPF check has failed. Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, bounce messages via content filtering will not be sent. (By default, this option is selected.)

• Require message pass SPF if SPF record exists - An incoming message that triggers the content filter will not have the bounce message sent if the original sender's message failed the SPF spam check. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the bounce message from being sent if the original sender's SPF check fails. (This option is distinguishable from the option above as it will only impact messages where the SPF record IS configured and fails the check. If the original sender doesn't have SPF configured, the bounce message will be sent.) Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, bounce messages via content filtering will not be sent.

• Internal Spam Check Behavior - This setting allows you to add (or restrict) spam checks for messages sent internally. That means, when messages pass between domains that are hosted on the same SmarterMail server. This setting affects any non-IP based authentication spam check, which includes SPF, DKIM, RBLs, and URIBLs. IP-based checks, such as Cyren Premium Antispam, Cyren IP Reputation, and Message Sniffer are not affected.

• Bypass Spam Checks - This disables all relevant spam checks for internal messages.

• Check All Messages - Spam checks all internal messages regardless of sender or recipient.

• Check Other Domains - Spam checks messages only when the sender's domain does not match the recipient's domain, when both are hosted on the same server. That means spam checks are not performed on messages from user1@domainA.com to user122@domainA.com, but WOULD be run on messages sent from user1@domainA.com to user1@domainX.com when both domains are hosted on the same SmarterMail server.

• Max message size to content scan (KB) - The maximum message size for which content-based spam checks will run. Content-based spam checks include spamAssassin-based Pattern Matching, Remote SpamAssassin, and any custom rules. Note: Increasing this number will also increase the mail server's memory usage. (By default, this limit is set to 4096.)

• Max Spam Check Threads - SmarterMail allows administrators to assign the number of threads used when processing spam checks. (Threads will, essentially, match the max number of messages that can be spam checked at one time.) The default is 30, and increasing that number can have an impact on the mail servers's performance.

• Enable spool proc folder - Enable this to have SmarterMail place messages into a Spool\Proc folder to be analyzed in the background, usually by third-party products such as Declude or custom-built applications. (By default, the location of the Proc folder is C:\SmarterMail\Spool\Proc.) While the messages are in the Proc folder, .hdr can manipulate elements of the message, such as edit, write, and add headers. Once the scan has been completed, the third-party app is responsible for moving the message back into the spool to be handled by SmarterMail from that point on. This option is most often necessary when using the third-party program, Declude. However, this setting can be used to prevent the disruption of mail flow with any other third-party app that manipulates messages.

• Enable catch-all accounts to send autoresponders and bounce messages - Enable this if you rely on autoresponders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.

• Send user spam feedback to antispam providers - When enabled, every time a user marks a message as spam (or unmarks as spam), that information is sent to antispam providers. This type of user feedback helps improve the accuracy of these partnered providers. Reports are aggregated and send every five (5) minutes, so if a message is marked as spam, then unmarked as spam, within that timeframe, no message is sent.

• Send user spam feedback to training folder - When enabled, this will temporarily copy .EML files to a separate folder on disk. This allows any third-party products that allow for "training" of their systems to review messages that have been marked as spam. .EML files are stored for approximately one (1) hour before they are deleted.

DMARC

What is DMARC?

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a newer form of email authentication. It makes sure that legitimate email authenticates against 2 DNS record types: DKIM and SPF. Also, it ensures that fraudulent email that tries to look legitimate gets blocked. It's worth noting that, when enabled, all messages will be checked against DMARC (along with SPF and DKIM), including those from Trusted Senders, IP bypasses, and whitelists.

The alignment of these DNS entries, which is the heart of DMARC, prevents spoofing of the return path's "from" address. It matches the return path domain name with the visible From address domain name from the SPF check. Then, it matches the return path domain name with the domain name in the DKIM signature. In order to pass DMARC, an email must pass ONE OR BOTH of the following:

- It must pass SFP authentication and SPF alignment.
- It must pass DKIM authentication and DKIM alignment.

If one of the above is met, the message will pass the DMARC check.

Why use DMARC?

More and more email providers are using DMARC as a way to authenticate email. Companies like Microsoft (Microsoft 365 (Office)), Google (Google Workspace), and Yahoo! all use DMARC and its associated DNS entries when checking messages. As a result, have valid DKIM and SPF records, and enabling DMARC, can help ensure your emails are accepted with larger email providers. In addition, it helps keep your users from seeing legitimate-looking email.

Disadvantages of Using DMARC

The primary disadvantage is that not all email providers, and not all businesses, know about DMARC, SPF and DKIM. As a result, it's possible it's being implemented improperly, if at all. As a result, legitimate email may be flagged as suspicious, even if it's not.

DMARC Quarantine/Suspicious Weight

This is similar to a spam weight: it's the weight assigned to a message if it "fails" the DMARC check. When enabled, the weight is 10 by default.

Understanding DMARC Header Entries

When viewing an email header, it's possible to see the various scores given to the spam checks that are enabled. However, some scores depend upon how certain checks are interpreted by SmarterMail.

DMARC is one of those checks. Therefore, here's a breakdown of what DMARC header entries can show and what they may mean, specifically when you see DMARC [Failed] in the header.

- Typically, DMARC [failed]: will indicate that the DMARC check failed, and the score applied is based on your policy. For exampe, when the domain's DMARC policy is set to None, the score will be 0.
- DMARC [failed]: "Any Other Number" indicates that the DMARC check failed, and the domain's DMARC policy is set to Quarantine/Suspicious. When this is how DMARC is configured, the weight associated with the DMARC Quarantine / Suspicious Weight is applied. (Which defaults to 10, but can be changed as needed.)
- If DMARC fails and the sender's policy is set to Reject, the email will be rejected in SMTP session, before it's even created as an email. Therefore, no score is assigned.

See Trusted Senders for more information on DMARC responses and what they mean.

- Enable DMARC - Toggle this to use DMARC as an antispam option.
- Quarantine/Suspicious Weight - The weight to use if a DMARC policy uses the "quarantine" option. This weight is then added to the overall spam score. By default, this is set to 10.
- Custom Domain Suffixes - SmarterMail, and most mail servers that support DMARC (which is just about all of them), use the Public Suffix List (PSL) to determine "same organization" for DMARC purposes. Previously, if an administrator needed to add a domain to the PSL, they needed to contact the PSL administrators so that SmarterMail, and other mail servers, could identify the new domain as an organization. However, now system administrators can add a domain to this area and it's added to the parsed PSL that SmarterMail uses. This DOES NOT add domains to the PSL directly. Instead, it inserts these domains into the list SmarterMail retrieves from the PSL.

Custom Domain Suffixes

By default, SmarterMail will pull data for standard Top Level Domain extensions from the Public Suffix List , a community managed list of suffixes that can be registered at various domain registrars. Common suffixes include .com, .com.uk, or even pvt.k12.ma.us. While this list is updated automatically within SmarterMail, there may come a time when a system administrator needs to add a suffix before the public list can be updated, and before SmarterMail can update its internal list. This is where these "custom domain suffixes" can be added.

A common need for adding a Custom Domain Suffix is for DMARC policy for domains that are independent organizations from a larger domain. For example, (and solely as an example as this may or may not be true) if Yahoo! had independent domains for geographic locations such as akyahooemail.com for Alaskan Yahoo! email users. In this case, akyahooemail.com may not

necessarily pass DMARC policy checks for regional third level additions to the main domain. Therefore, a system administrator would add akyahooemail.com as a Custom Domain Suffix so that DMARC checks would treat regional Alaskan domains (e.g., juneau.akyahooemail.com) as an organizational domain.

Greylisting Options

What is greylisting and how does it work?

Greylisting has proven itself to be an effective method of spam prevention. When enabled, the system will keep track of the sending IP address, sending email address and recipient's email address for every message received. If an incoming message has a combination of a sending IP, sending address and recipient address that has not previously been seen, it will return a temporary failure to the sending server, effectively saying, "Try again later." Valid servers will retry the email a short time later, which would be permitted. Spammers, on the other hand, typically create scripts that bombard your server with emails, and they rarely retry on temporary failures. When these messages are bounced back because of greylisting, they are typically not retried, therefore reducing the amount of spam that your customers receive. (Emails sent from whitelisted and authenticated senders will automatically bypass greylisting and are delivered directly to the spool.)

For those messages that are sent from valid email servers, the sending server should retry at least four times. If the first retry is beyond the block period (default 15 minutes) and within the pass period (default 6 hours), the message is passed to the spool and it goes through its normal processing without a delay. A record is also created that says this is a valid email address from that server to the given recipient and keeps it for 36 days (default). If another email from the same email address is received from the same server to the same recipient within the 36 days, the clock is reset for an additional 36 days and delivered directly to the spool.

Why use greylisting?

Greylisting is a very effective method of spam blocking that comes at a minimal price in terms of performance. Most of the actual processing that needs to be done for greylisting takes place on the sender's server. It has been shown to block upwards of 95% of incoming spam simply because so many spammers don't use a standard mail server. As such, spam servers generally only attempt a single delivery of a spam message and don't reply to the "try again later" request.

Disadvantages of greylisting

The biggest disadvantage of greylisting is the delay of legitimate email from servers not yet verified. This is especially apparent when a server attempts to verify a new user's identity by sending them a

confirmation email. Some email servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

Greylisting configuration options

- Block Period (Minutes) - The period of time that mail will not be accepted. The default 15 minutes.
- Pass Period (Minutes) - The period of time in which the sender's mail server has to retry sending the message. The default 360 minutes.
- Record Expiration (Days) - The period of time that the sender will remain immune from greylisting once it has passed. The default 36 days.
- Enable Greylisting - Select this option to enable greylisting.
- Allow users to override greylisting - Select this option to allow users to selectively turn off greylisting. This is useful if you have a user who receives time sensitive mail. Note: The following cases are exempt from greylisting: SMTP Whitelisted IPs, IP Bypasses that are specified to skip greylisting, anyone who authenticates (includes SMTP Auth Bypass list), trusted senders (includes users' contacts), anyone who has already sent you an email (this list generates only after greylisting has been enabled), any IP address or country code specified as being exempt in the Greylist Filters tab.

Remote SpamAssassin Servers

SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam, including header and text analysis, Bayesian filtering, DNS blocklists and collaborative filtering databases. While SmarterMail includes SpamAssassin by default, it's also possible for system administrators to set up an external SpamAssassin server. To set up an external server, simply click New Server . The following options will be available:

- Name - The name of the SpamAssassin server.
- IP Address - The IP address of the server running SpamAssassin.
- Port - The port on which the SpamAssassin server should listen. By default, the port is 783.

Remote Rspamd Servers

Rspamd is a very popular and advanced spam filtering system that uses various methods, such as regular expressions, statistical analysis, and custom services like URL blacklists, to evaluate email messages. It assigns each message a spam score that can be used by system administrators as another way to mark potential spam and then handle it appropriately before it reaches end users. More information can be found at https://rspamd.com/doc/index.html Note: When using a Remote Rspamd server, it's best to disable SpamAssassin-Based Pattern Matching and/or Remote SpamAssassin. This

is because both use the same engine, so you run the risk of double scoring messages, and could, therefore, falsely increase the spam score of messages.

For information on setting up a remote Rspamd server, see this knowledgebase article: Deploying Rspamd For Use With SmarterMail .

- • Name - The name given to the Rspamd server.
- • Rspamd Server Address - The complete URL for the remote server. This can be a FQDN (e.g., rspamd01.mail-domain.com), but generally will be an IP address and port. E.g., https://127.0.0.1:11335
- • Checkv2 Endpoint - This is the endpoint used for checking messages and returning an action. By default, it's /checkv2
- • Learnspam Endpoint - This is the endpoint for messages "marked as junk" by users, or messages moved by the user into the Junk Email folder. By default, it's /learnspam.
- • Learnham Endpoint - This is the endpoint for messages moved out of the Junk Email folder and into another folder. By default, it's /learnham.

Spam Checks

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combating spam. Default antispam settings were configured during installation, but these settings can be modified at any time.

Due to the flexible nature of SmarterMail's antispam setup, spam checks can influence the spam decision as much or little as you want. Each spam check has one or more associated weights. When spam protection runs on an email, all enabled spam checks are performed. The total weight of all spam checks is what comprises the final spam weight for the email. A spam probability level (Low, Medium or High) is then assigned to the email using the weights configured by the system administrator on the Filtering card of the Options tab. Based on the email's total spam weight / probability of being spam, the corresponding spam filtering action is taken.

An added benefit to SmarterMail's antispam administration is the ability to combat both inbound and outbound spam messages. Most mail servers only allow administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from inbound spam and also includes the added benefit of keeping mail servers from actually sending spam, thereby helping to protect the mail server from being blacklisted.

The Spam Checks , RBLs and URIBLs tabs can be used to create or modify existing spam checks and RBLs for the system. Note: Only enabled spam checks, RBLs and URIBLs are used when calculating

spam weight. To enable or disable a check, enable the appropriate spam check in its configuration options.

- Cyren IP Reputation
- Cyren Premium Antispam
- Declude
- DKIM
- Honey Pot
- Message Sniffer
- Null Sender
- Remote Rspamd
- Remote Spam Assassin
- Reverse DNS
- SpamAssassin-based Pattern Matching
- SPF
- Creating Custom Rules

Spam Checks

The Spam Checks tab shows all non-RBL/non-URIBL checks that are performed on a message. These checks can include licensed add-ons such as Message Sniffer, as well as standard checks such as DKIM, SPF and more. Any of these checks can be enabled or disabled for Inbound and/or Outbound SMTP, and each can be edited or removed. To edit a check, simply click it to open its settings. To add a new Spam Check, such as adding in an antispam appliance, click the New button.

SmarterMail includes several spam checks by default. Each check is described in detail, below.

In general, one or more of the following options may be available when creating a custom spam check or modifying an existing one:

- Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.
- Enable Inbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this spam check is counted toward the weight threshold for the blocking of inbound emails. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking. If this option is not available, then that particular spam check does not offer SMTP blocking and must rely on content filtering instead.
- Enable Outbound SMTP blocking - This option is used in conjunction with the SMTP

Blocking settings configured in Antispam Options . When enabled, this spam check is counted toward the weight threshold for the blocking of outbound emails. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking. If this option is not available, then that particular spam check does not offer SMTP blocking and must rely on content filtering instead.

• Weight - The weight range available for the spam check. Each spam check may utilize unique spam weight options.

Cyren IP Reputation Note: Cyren IP Reputation is included with a Cyren Premium Antispam license.

Cyren IP Reputation builds upon what existing RBLs and URIBLs provide by handling the vast gray area of IPs and IP sources that have little or no information. For example, machines that are hijacked and used by botnets that dynamically use, and abuse, the innocuous IP addresses on those hijacked machines. Cyren analyzes hundreds of millions of messages every day, so they are able to classify (and re-classify), in real-time, the reputation of each IP source.

Cyren evaluates an IP, then returns to SmarterMail a "Risk Score". Cyren also categorizes IPs in what they call "Class Groups". These groups represent a composite value based on whether an IP is a high volume IP (i.e., has a substantial volume history), is a transitory or low volume IP, or if there is an IP that has a "fixed decision" regardless of its volume (e.g., whitelisted or blacklisted sources.) SmarterMail then uses these values and classifies the score as Good (or no risk), Low risk, Medium risk, or High risk.

• Enable Spool Filtering - See above for details.

• Enable Inbound SMTP Blocking - See above for details.

• Good Weight - Defaults to 0. Based on the Class Group from Cyren, these are IPs that have high volume but low risk or are whitelisted IPs PLUS their overall risk score is 0.

• Low Weight - Defaults to 0. The risk score from Cyren is 79 or below.

• Medium Weight - Defaults to 5. The risk score from Cyren is between 80 and 89.

• High Weight - Defaults to 10. The risk score from Cyren is 90 or above.

Cyren Premium Antispam

The Cyren Premium Antispam add-on is a service that uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time as messages are mass-distributed over the internet. Rather than evaluating the content of messages, the Cyren Detection Center analyzes large volumes of internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. Cyren then categorizes messages as Confirmed, Bulk, Suspect, Unknown, or None.

This add-on can be purchased directly from the SmarterTools website by logging into your account and adding it to any SmarterMail license.

> • Enable Spool Filtering - See above for details.
>
> • Enable Inbound SMTP Blocking - See above for details.
>
> • Confirmed - Defaults to 20. The message is confirmed as being spam.
>
> • Bulk - Defaults to 10. The message is categorized as bulk mail, so it's likely spam.
>
> • Suspect - Defaults to 10. The message is suspicious and likely either bulk email or spam.
>
> • Unknown - Defaults to 0. Cyren is unable to categorize the message as there's not enough data.
>
> • None - Defaults to 0. The message was not scored by Cyren, so it's likely legitimate.

Declude Note: Declude, while functional, is an older antispam system that is being completely re-written as "Declude Reboot", a more modern and updated version of the older Declude engine.

Declude integration allows you to use Declude products in conjunction with the SmarterMail weighting system. Declude addresses the major threats facing networks, and are handled by a multi-layered defense. Configuration of Declude is done through the Declude product, so all you need to do in SmarterMail is enable the spam check and the Declude score will be included when calculating the total spam weight of a message. For more information, visit the Mail's Best Friend website as they currently manage and support Declude and the "Declude Reboot" product.

> • Low Spam Weight - The weight that will be assigned if Declude determines a low probability of spam.
>
> • Medium Spam Weight - The weight that will be assigned if Declude determines a medium probability of spam.
>
> • High Spam Weight - The weight that will be assigned if Declude determines a high probability of spam.

DKIM

DKIM is an email authentication systems designed to verify the DNS domain of an email sender, and the authenticity of a sender as well as the sender's message. DKIM is the combination of Yahoo's Domain Keys and Cicso's Identified Internet Mail (IIM) standard.

> • Enable Spool Filtering - See above for details.
>
> • Pass Weight - Indicates that the email sender and message integrity were successfully verified (less likely spam). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
>
> • Fail Weight - Indicates that the email sender and message integrity verifications failed (most likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is

very high.

• None Weight - Indicates that there was not a valid DomainKey/DKIM signature found to validate the sender and message integrity. Except in very special circumstances, leave this set to 0.

• Max message size to verify (MB) (0 = Unlimited) - The maximum inbound message size you want the mail server to verify.

Honey Pot

A "honey pot" spam check derives its name because implementing it can attract spammers — or, more likely, spam bots — like "bees to honey." Basically, a system administrator populates the honey pot spam check with email addresses that are designed to be seen by, or otherwise used by, spammers. These addresses can be commonly used addresses that spammers will automatically target such as admin@@your-domain.com, info@@your-domain.com, hr@@your-domain.com, etc. These types of addresses are commonly targeted, but SHOULD NOT be addresses that are actually used by any user of a given domain. You don't want to add admin@@your-domain.com IF that is an actual address used BY a user on that domain. In fact, any addresses added as honey pot addresses DO NOT need to be an actual users. So if you DO use admin@@yourdomain.com as a honey pot address, you do NOT need to add that as an actual user TO the domain. In addition, there's no limit to the number of addresses you can add. It's totally up to the system admin.

Another common way to instantiate a honey pot spam check is to add a hidden email address to a form used on a website. Spambots can scrape email addresses from these forms, then populate spam lists that are used by, or potentially sold to, spammers. By adding in a hidden (using CSS) honey pot email address to a form, you can essentially trick these bots into scraping that email address, then block any sender who uses the address.

Regardless of HOW you set your trap, honey pots can be a simple, yet effective, way of finding, scoring and then disposing of email spam for your users as well as blocking sending IP addresses.

• Enable Spool Filtering - See above for details.

• Reject found entries at SMTP level - Enabling this will automatically reject the message prior to it being delivered if the IP of the sending mail server has already been listed. Note: This will occur as long as the IP is not whitelisted, is not a gateway and is not IP Bypassed.

• Pass Weight - The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating. (Setting negative numbers is not recommended.)

• Listed Weight - This is the weight that is assigned to a message sent from an IP address that was already part of the honey pot.

• Triggered Weight - This is the weight that is assigned to a message that is sent to one of your Honey Pot Addresses. The email address must match one in the list of Honey Pot Addresses for

this weight to be added to the message.

• Honey Pot Addresses - These are the actual, full email addresses you're targeting for use by spammers. For example, generic email addresses can be used such as info@@example.com or contact@@example.com. These should NOT be actual email addresses that are used by anyone on any domain. Ideally, they're addresses that are general enough that spammers would target them with blanket spam attacks, but not addresses that are posted anywhere or used to actually send email. They are explicitly to be used ONLY for trapping potential spammers.

Message Sniffer

The Message Sniffer add-on is an intelligent antispam scanner that uses advanced pattern recognition and collaborative learning technologies to accurately identify spam, scams, viruses, and other email borne malware before it gets to a user's mailbox.

This add-on can be purchased directly from the SmarterTools website by logging into your account and adding it to any SmarterMail license.

• Enable Spool Filtering - See above for details.
• Enable Outbound SMTP Blocking - See above for details.
• Confirmed Weight - The weight that will be assigned if Message Sniffer determines the message as coming from known spam sources.
• None Weight - The weight that will be assigned if Message Sniffer deems the message is not spam.

Null Sender

A common spam technique is to send messages with missing, or "Null" sender values in the return path. That means that the message appears to come from no one as the return path is blank. This check allows you to assign a spam weight to messages that meet this criteria. note: Because some valid emails contain no return-path (such as notifications, bounce messages, automated messages, etc.), we recommend giving the Null Sender spam check a low weight, allowing it to only mark an email as spam in conjunction with other failed spam checks. By default, the weight is 5.

• Enable Spool Filtering - See above for details.
• Enable Outbound SMTP Blocking - See above for details.
• Weight - The weight assigned to messages that fail this check.

Remote Rspamd

Rspamd is a fast, free, and open-source spam filtering system that, as a Linux distribution, requires installation on a remote system. However, it ties in nicely with SmarterMail. For information on

setting up a remote Rspamd server, see this knowledgebase article: Deploying Rspamd For Use With SmarterMail .

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Scoring Factor - Instead of attaching weights, like other checks, Rspamd uses a "scoring value" to normalize the value used when weighing results. This normalization takes the raw score and multiples it by a Scoring Factor (that is fully customizable) to come up with a final spam score.
- Client Timeout (seconds) - The timeout that SmarterMail will impose on a server if it cannot connect.
- Max Attempts per Message - The number of times SmarterMail will attempt to acquire an Rspamd score for an email.
- Failures Before Disable - The number of times a remote Rspamd server can fail before it is disabled.
- Disable Time (minutes) - The length of time before the Rspamd server is re-enabled.

Remote SpamAssassin

SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside SmarterMail. It utilizes a wide array of tools to identify and report spam. By default, SpamAssassin will run on 127.0.0.1:783. For more information, or to download SpamAssassin, visit spamassassin.apache.org .

SmarterMail can use SpamAssassin with its weighting system:

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Scoring Factor - Instead of attaching weights, like other checks, Remote SpamAssassin uses a "scoring value" to normalize the value used when weighing results. This normalization takes the raw score and multiples it by a Scoring Factor (that is fully customizable) to come up with a final spam score.
- Client Timeout (seconds) - The timeout that SmarterMail will impose on a server if it cannot connect.
- Max Attempts per Message - The number of times SmarterMail will attempt to acquire a SpamAssassin score for an email.
- Failures Before Disable - The number of times a remote SpamAssassin server can fail before it is disabled.
- Disable Time (minutes) - The length of time before the SpamAssassin server is re-enabled.

• Header Log Level - The amount of information SpamAssassin inserts into the header of the message

Reverse DNS

Reverse DNS checks to make sure that the IP address used to send the email has a friendly name associated with it.

• Enable Spool Filtering - See above for details.
• Enable Inbound SMTP Blocking - See above for details.
• Weight - The default weight for this spam check. If an email sender does not have a reverse DNS entry, this is the value that will be added to the message's total spam weight.
• Forward Confirm Fail Weight - Forward Confirm Reverse DNS means that an hostname has both forward and reverse DNS entries that utilize the same IP address. Using this check, SmarterMail checks the rDNS and fDNS and if there is no A record, the check fails.
• Forward Confirm Mismatch Weight - Using this check, SmarterMail checks the rDNS and fDNS and if the IPs exist, but don't match, the check fails.

SpamAssassin-Based Pattern Matching

SmarterMail includes a proprietary pattern matching engine built upon the SpamAssassin technology as part of the default installation of the product. It includes a number of spam detection techniques, including DNS-based and fuzzy-checksum-based spam detection, Bayesian filtering and more.

• Enable Spool Filtering - See above for details.
• Enable Outbound SMTP Blocking - See above for details.
• Scoring Factor - Instead of attaching weights, like other checks, a "scoring value" is used to normalize the value used when weighing results. This normalization takes the raw score and multiples it by a Scoring Factor (that is fully customizable) to come up with a final spam score.
• Header Log Level - The amount of information the pattern matching engine inserts into the header of the message. For example, a line in the header would look like the following: X-SmarterMail-SpamDetail: 2.0 BASE64_LENGTH_79_INF base64 encoded email part uses line length greater than 79 characters.

• Score only - This only adds the numeric value of the returned check to the header. In the above example, that would be "2.0"
• Score with test name - This adds the numeric value and the test name to the header. In the above example that would be "2.0 BASE64_LENGTH_79_INF"
• Score with test name and description - This adds all of the information returned: score, test name, and test description. In the above example, that would be the entire line: "2.0

BASE64_LENGTH_79_INF base64 encoded email part uses line length greater than 79 characters"

SPF (Sender Policy Framework)

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. Therefore, as it's verifying the sending server, SPF is set up by the sending server's system administrator or the domain owner as a DNS record. (More information can be found at DMARC Analyzer .) As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

Just as with RBL/URIBL lookups, SmarterMail has a built-in 15-second timeout that will prevent excessively long SPF lookups to occur, which can impact email delivery.

- Enable Spool Filtering - See above for details.
- Enable Inbound SMTP Blocking - See above for details.
- Scan From header instead of Return Path - Enabling this means the check will use the From address for the SPF check as opposed to the message's RETURN-PATH, which is where NDRs (bounce messages) are sent. Many times spammers will spoof messages by changing the From address to make it appear like a message is coming from a legitimate person/organization even though the RETURN-PATH may be for the actual source of the message. While it is possible to spoof a message's RETURN-PATH, spoofing the From address is a much more common method used by spammers.
- Pass Weight - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
- Fail Weight - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
- SoftFail Weight - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.
- Neutral Weight - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.
- PermError Weight - Indicates that there is a syntax error in the SPF record. Since SPF is relatively new, some domains have published improperly formatted SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.
- None Weight - Indicates that the domain has no published SPF record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

Creating Custom Rules

Custom spam rules can be created based on the header, body text or raw content of a message. For example, BestAZLawFirm.com, which is hosted on a SmarterMail server, constantly receives important emails from the "VeryImportantClientDomain.net" domain, which is hosted on an external server. However, VeryImportantClientDomain.net is constantly getting listed on one or more blacklists because it is hosted on a mail server that isn't using properly vetted and cleansed IP addresses. To bypass any potential negative spam score senders from this domain receive when their messages hit SmarterMail, the SmarterMail system administrator can create a custom spam rule for the sending domain that artificially removes any negative spam score. That way, emails from VeryImportantClientDomain.net don't end up in the Junk Email folders of BestAZLawFirm.com users.

To configure weights for custom rules, click New , then complete the following fields:

- Rule Name - The name of the rule.
- Rule Source - What you want the rule to be based on: a message's header, body text or raw content. When selecting "body text" or "raw content", you'll need to supply additional information that is applied to the Rule Text: whether the Source "contains" the information, whether the wildcard is used for a range of information or whether you want to supply a regular expression. If you select Header you will need to supply header details separately from the Rule Text.
- Rule Text - The text that will be used in conjunction with the Rule Source. For example, if you use create a Rule Source based on Body, then an additional Rule Source for "Contains", Rule Text can include words such as "Cialis", "Viagra", "male enhancement", etc.
- Weight - The amount to add to the email message's spam weight.
- Match Multiple - Enabling this allows the spam weight calculated for the rule to increase based on multiple instances of the Rule Text that's added. In general, a custom spam check based on any Rule Source will check for the FIRST instance of a word or phrase that's been added to the Rule Text and apply that weight. It doesn't matter if all of the words or phrases are found — only the FIRST instance is counted and the weight applied. When Match Multiple is enabled, the first instance of ALL words or phrases in the Rule Source is counted and the total score is used. Note: when using Body as the Rule Source, the spam check looks at both the HTML and plain text versions of a message, primarily because these versions may differ in content. As a result, the total weight may vary.
- Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.
- Enable Outbound SMTP Blocking - See above for details.

Match Multiple Examples

The concept of the Match Multiple settings can get a bit confusing. Below are a couple of examples of how Match Multiple works.

Rule Source: Header

Custom Rule ?

Rule Name *

Match Multiple

Rule Source

Header ▾

Header *

Test

Rule Source

Contains ▾

Rule Text (one per line) *

Pickles

Tomato

Weight *

10

⬤ Match Multiple

⬤ Enable Spool Filtering

◯ Enable Outbound SMTP Blocking

Cancel   Save

• An incoming email that contains two separate headers of "Test: Pickles" will get a weight of 20 for this spam check. ("Pickles" in the first header will trigger a weight of 10, and "Pickles" in the second header will trigger a weight of 10.)

• An incoming email that contains a single header of "Test: Pickles Pickles" will get a weight of 10 for this spam check. (The first instance of "Pickles" in the header will trigger a weight of 10.)

• An incoming email that contains a header of "Test: Pickles Pickles" and a header of "Test: Tomato" will get a weight of 20 for this spam check. (The first instance of "Pickles" in the first header will trigger a weight of 10, and the instance of "Tomato" in the second header will trigger a weight of 10.)

Rule Source: Body

Custom Rule ?

Rule Name *

Match Multiple Testing

Rule Source

Body ▾

Rule Source

Contains ▾

Rule Text (one per line) *

Pickles

Tomato

Weight *

10

🔵 Match Multiple

🔵 Enable Spool Filtering

⚪ Enable Outbound SMTP Blocking

Cancel   Delete   Save

• An incoming HTML + plain text email that contains "Pickles Tomato" in the message body will get a weight of 40 for this spam check. ("Pickles" in the HTML content will trigger a weight of 10, "Pickles" in the plain text content will trigger a weight of 10, "Tomato" in the

HTML content will trigger a weight of 10, and "Tomato" in the plain text content will trigger a weight of 10.)

• An incoming HTML + plain text email that contains"Pickles Pickles Tomato Tomato" in the body will get a weight of 40 for this spam check. (Only the first instance of the Rule Text words in the HTML content and plain text content will trigger the weight.)

• An incoming plain text only email that contains "Pickles Tomato" in the body will get a weight of 20 for this spam check. ("Pickles" in the plain text will trigger a weight of 10, and "Tomato" in the plain text will trigger a weight of 10.)

RBLs and URIBLs

Real-time Blackhole lists, or remote block lists, (RBLs) and URI Blacklists (URIBLs) are publicly accessible lists of known spammer IP addresses. (Though some also use domain names.) Each list is managed and maintained independently, and each has its own criteria for listing IP addresses as "spam". SmarterMail has a number of RBLs and URIBLs available by default. Therefore, system administrators have the ability to manage the default lists and enable/disable any they want to use for protecting against spam. In addition, system administrators can add their own RBLs or URIBLs as they see fit.

As these lookups can cause delays in email delivery, especially when many RBLs and/or URIBLs are being used, SmarterMail has a built-in timeout the prevents lookups from slowing down deliveries and/or causing servers to disconnect due to timing constraints. In addition, RBL/URIBL lookups are handled asynchronously, further speeding up the process, and any list that doesn't return a result in 5 seconds is excluded from the lookup process.

The landing pages for both RBLs and URIBLs will display the various lists that have been added to the server. Details of each include:

• Name - The list's name.
• Average Time - The average time it takes for a result to be returned when checking the list, in milliseconds (ms). It should be noted that each check aggregates the amount of time needed for a message to be delivered. Generally, this will not be noticed by the end user. However, should a specific list take an inordinate amount of time to return a result, it could indicate that there's an issue with the list, so that particular check could be disabled until the issue is resolved to ensure the timely delivery of email.
• Timeouts - The number of times the hostname has been unavailable for spam checks. This could be due to network issues, issues with the List, etc.
• Host - The hostname of the list.
• Weight - The default weight (or range) assigned for this list.

• Spool Filtering - A checkmark appears if the list is used as part of the overall spam score assigned to a message.

• Inbound SMTP - A checkmark appears if the list (RBLs only) is being used to check messages sent TO the server.

• Outbound SMTP - A checkmark appears if the list is being used to check messages sent FROM the server.

Managing a List

Clicking on a specific list opens up a modal window. Here, system administrators can edit the list's details as needed. Depending on the list selected, the following settings are available:

• Name - The friendly name for the list that will help you and your customers identify it.

• Description - Any additional information about the list.

• Hostname - The hostname of the RBL as provided by the list moderators.

• Lookup Prefix - This is the IP address that is appended to the request sent to the RBL. For example, if you have a routed network that requires an IP address prepended to everything for it to work, that IP address should be added here.

• Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.

• Enable Inbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this RBL/URIBL is counted toward the weight threshold for the blocking of incoming emails.

• Enable for Outbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this RBL/URIBL is counted toward the weight threshold for the blocking of outgoing emails.

• Required Lookup Values

• IP Address - The expected IP address that's returned from the list if the sender's IP is listed with the provider. This value can be found in the setup documentation from the RBL/URIBL provider.

• Weight - The default weight for this spam check. If an email sender is listed with the spam list, this is the value that will be added to the message's total spam weight.

Adding new RBLs or URIBLs

Adding a new RBL or URIBL is as simple as clicking the New button. The same modal opens as described above. System administrators simply need to fill out the relevant information in order to get the new list in the lineup. Complete documentation on how to include the list should be made available

by the list provider. For example, here is the information for the SpamCop Blocking List . It clearly states the hostname to use (bl.spamcop.net) and IP that's returned (127.0.0.2). From there, system administrators simply need to fill out the other options.

Greylist Filters

SmarterMail's antispam options include greylisting, which is a very effective method of spam blocking that comes at a minimal price in terms of performance. When enabled, the system will keep track of the sending IP address, sending email address and recipient's email address for every message received. If an incoming message has a combination of a sending IP, sending address and recipient address that has not previously been seen, it will return a temporary failure to the sending server. This temporary failure essentially tells the sending server to "Try again later." Valid servers will retry the email a short time later, at which point SmarterMail accepts the message. Spammers, on the other hand, typically create scripts that bombard your server with emails, and they rarely retry on temporary failures. When these messages are bounced back because of greylisting, they are typically not retried, therefore reducing the amount of spam that your customers receive.

In addition to the greylisting configuration on the Antispam | Options tab, administrators can use Greylist Filters to prevent greylisting based on the sender's country or IP address. To add an IP address or country code, click New . To edit an existing filter, simply click on it from the list. The following options will be available:

- Filter Type - Select the type of filter you would like to add: IP Address or Country Code.
- IP Address - If the filter type is set to IP Address, enter the IP address that should bypass greylisting / be greylisted.
- Country Code - If the filter type is set to Country Code, select a country code from the list. The greylisting exception / limitation will apply to all messages that are identified as coming from an IP address matching that country.
- Description - The friendly name or descriptor you want to give to the IPs. For example, Microsoft 365 or Yahoo! Note: Some greylist filters are included by default and cannot be modified or removed. These default filters are indicated in the grid by having a checkmark in the Internal column.

Recommended Antispam and Antivirus Settings

SmarterMail comes equipped with several industry-standard antispam options that can block up to 97% of all spam from entering or leaving the server and help keep mail systems running smoothly. These built-in protections include SPF, DKIM, reverse DNS, greylisting, pre-configured settings for multiple popular and effective RBLs and URIBLs, and more. However, when considering your spam

configuration, it's important to remember that spam administration is not a "fire and forget" task. Using these built-in options requires constant tweaking to keep that level of effectiveness, and mail administrators will need to monitor incoming and outgoing spam as spammers frequently change their tactics. (Learn more about configuring the built-in antispam options below.)

In addition, SmarterMail comes equipped with industry-standard, and open source, antivirus protection using ClamAV. It also supports quarantining messages, and the ability to manage messages in the quarantine, an Events system for dealing with quarantined items and much more.

On top of the included options, SmarterMail supports third-party protections like:

- • Message Sniffer
- • Declude
- • Command-line antivirus
- • Antispam appliances, such as Barracuda
- • Many more

Paid add-ons like Message Sniffer and more can definitely come in handy. These third-party services act as additional spam and virus checks and may be worthwhile investments as a multi-tiered solution is the best course of action when it comes to dealing with spam and antivirus. Often times, users are not satisfied with 97% spam protection out-of-the-box — keeping in mind that, at this level of protection, for every 100 messages a user receives per day, only 3 of these could be spam. Message Sniffer (and other add-ons) will catch a higher percentage of spam than the default options, and better yet, neither require consistent updating by a SmarterMail system administrator - updates are handled by the service provider. Using one of these services, or ideally both together, is easily the most effective option in battling spam.

Regarding antivirus, when proper antivirus solutions are in place within SmarterMail using an antivirus solution at the network level is not necessary. In fact, antivirus solutions at the network level can cause numerous issues for system administrators and/or users. Therefore, it is NOT recommended. That's because antivirus solutions at the network level can't relay information to SmarterMail in a reliable way. If a network antivirus solution removes suspected virus attachments from an incoming email, the email will still be delivered to the recipient. However, while the message list will show that the email contains an attachment, no attachments will be available. Not only does this leave the user with no information regarding the missing attachments, it leaves them vulnerable to receiving, and perhaps responding to, email from malicious sources.

In the Spam Checks, RBLs and URIBLs sections, you can enable individual spam checks for email spool filtering and inbound/outbound SMTP blocking. (Checks that are not available for inbound or

outbound SMTP blocking are denoted with 'N/A'.) Each spam check comes with unique spams weights, which can be adjusted as desired.

Determining the weight values of each spam check depends on how accurately you believe that check identifies spam messages. If you're confident that it accurately identifies spam and has very few false positives, you would give its weight a higher value. If you are less confident in a spam check's accuracy, assign it a lower value. By configuring your spam checks this way, those that you have less confidence in will not cause a message to be marked as spam on its own. However, if multiple checks that you have lower confidence in all consider a message to be spam, their combined weights would likely cause the messages to be marked as spam. Find our recommended spam weight values below:

Below are some default recommendations for the various spam settings SmarterMail has to offer. Please keep in mind that these are only suggestions. Administrators can, and should, keep an eye on these settings and adjust them as necessary to concoct a viable antispam solution for their end users.

SPAM CHECKS

Message Sniffer

(Leave disabled if you do not have the Message Sniffer add-on)

- Confirmed Weight = 20
- None Weight = 0

DKIM

(DKIM is the primary mechanism for signing messages which proves to the receiving user that the message was not altered during transit and was sent from the signing domain. Not all valid messages are signed however so no spam weight should be given for no signature.)

- Pass Weight = 0
- Fail Weight = 10
- None Weight = 5
- Max message size to sign (MB) = 100
- Max message size to verify (MB) = 100

Null Sender

A common spam technique is to send messages with missing, or "Null" sender values. That means that the message appears to come from no one as the sender details are blank.

- Weight = 5

Reverse DNS

Reverse DNS checks to make sure that the IP address used to send the email has a friendly name associated with it.

- Fail Weight = 15
- Forward Confirm Fail Weight = 10
- Forward Confirm Mismatch Weight = 5

SpamAssassin

SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside, or in place of, SmarterMail's spam settings. It utilizes a wide array of tools to identify and report spam.

SPF

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. Therefore, as it's verifying the sending server, SPF is set up by the sending server's system administrator or the domain owner as a DNS record.

- Pass weight = 0 (Sender's IP is valid for sender's domain)
- Fail weight = 30 (Sender's IP is not valid for sender's domain)
- Soft Fail weight = 10 (Sender's IP is questionable for sender's domain)
- Neutral weight = 5 (No strong statement can be made for or against sender's IP)
- PermError weight = 10 (The SPF record could not be processed.)
- None weight = 15 (No SPF record has been configured.)

RBLs

Backscatter

- Weight = 5

Barracuda

- Weight = 5

HostKarma (various lookup values)

- Weight = 0 to 10

SEM - Black

- Weight = 10

SpamCop

- Weight = 10

Spamhaus (various lookup values

- Weight = 0 to 15

Surriel

- Weight = 10

Truncate

- Weight = 5

UCEProtect Level 1

- Weight = 5

UCEProtect Level 2

- Weight = 10

URIBLs (Max / Min)

SEM-URI

- Weight = 5
- Max Weight = 15

URIBL Black (various lookup values

- Weight = 5
- Max Weight = 15

FILTERING

On the Filtering card within the Options tab, you can adjust the global actions taken on emails that are considered to be spam, based on one of three probabilities determined by their spam weights: Low Probability, Medium Probability and High Probability. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam and the corresponding action is taken. The defaults for Filtering are as follows:

Low Probability of Spam weight = 10

- Default Action: None

Medium Probability of Spam weight = 20

> • Default Action: Move to Junk Email folder

High Probability of Spam weight = 30

> • Default Action: Move to Junk Email folder

Once you are comfortable with your antispam settings and have a better understanding of the spam messages that impact your domain, you may wish to adjust these settings. For example, you may consider changing the default action on the Low Probability to Move to Junk Email folder or the High Probability to Delete Message. Important Note: Email that is deleted via spam filtering cannot be recovered.

SMTP BLOCKING

On the SMTP Blocking card within the Options tab, you can access the configuration options for SMTP Blocking. The idea behind SMTP blocking of incoming and outgoing email is to filter out spam messages before they are delivered. For example, imagine you have six spam checks enabled for Incoming SMTP Blocking and each of those spam checks have a weight of 10. If the Incoming Weight Threshold is set to 50, that means messages being received via SMTP will be rejected if they fail five or all six of the spam checks. (Because SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer incoming or outgoing SMTP blocking.)

Choosing which spam checks are used for Incoming/Outgoing SMTP Blocking is done on the Spam Checks, RBLs and URIBLs tabs. In order to actually enable the blocking feature, enable the corresponding weight threshold on the SMTP Blocking card. When an email arrives or is attempted to be sent that exceeds the threshold value, the email will be blocked and never delivered. note: By default, the Incoming Weight Threshold is enabled and set to 50. This means that messages that have a spam weight of 50 will be blocked and deleted before they reach the spool. You can decrease that weight threshold once you have a better understanding of the spam that impacts your domain.

In addition to SMTP Blocking, this section also contains settings for the Outgoing Quarantine and Greylisting. If Outgoing Quarantine is enabled, SmarterMail will quarantine any outbound blocked messages for the specified time period. (If set to 'None,' messages are immediately deleted from the spool.) The Greylisting Threshold allows you to add extra options for what items get greylisted. If you prefer that messages with a high potential of spam are delayed, you can set the greylist weight threshold on the SMTP Blocking card. We recommend starting the threshold at 30 and decreasing to 20 if you're confident in your spam checks.

GREYLISTING

On the Greylisting Options card within the Options tab, you can enable greylisting. Greylisting is a popular method of fighting spam as it temporarily rejects unrecognized incoming emails that are not sent by whitelisted or authenticated users, effectively saying, "Try again later." Valid servers will retry the email a short time later, which would be permitted and delivered. Spammers, on the other hand, rarely retry on temporary failures, therefore reducing the amount of spam that customers receive. Find our recommended values below:

- Block Period = 3 minutes
- Pass Period = 360 minutes (6 hours)
- Record Expiration = 36 days

As part of the greylisting configuration, you can choose to greylist messages from everyone, greylist messages from the specified countries / IP addresses, or greylist messages from everyone except the specified countries / IP addresses. If the greylisting 'Applies To' is set to 'Only specified countries / IP addresses' or 'Everyone except specified countries / IP addresses', you use the Greylist Filters tab to add those exceptions / limitations.

Summary

When it comes to antispam and antivirus administration, it's important to keep in mind that spammers change their tactics often and each installation/setup is unique. What one person may consider the ideal spam configuration, others may find too restrictive. What works for one mail server, may not work for all. Discussing your configuration with other server administrators is a great way to get ideas flowing on what will work best for you. If you've still got more questions or want additional ideas on how to configure SmarterMail's antispam, please consider posting in the Community or reviewing one of the many threads discussing antispam topics.

Antivirus

SmarterMail supports multiple methods of antivirus protection for securing your mail server. The default installation includes, at no additional cost, effective and self-updating antivirus protection with ClamAV, plus integration with Microsoft Defender. SmarterMail also supports additional third-party solutions, including command-line antivirus solutions. In addition, SmarterMail has the ability to quarantine messages that are suspected as containing viruses, and, using system events, can respond to senders that attempted to send an email containing a virus.

From an email processing standpoint, when all forms of antivirus are in use (or even if just one or two are used), the "order of operations" for antivirus is as follows:

- Microsoft Defender Antivirus
- ClamAV
- Cyren Zero-Hour Outbreak Detection (if enabled)
- Command-Line Antivirus

Also, in order to preserve resources, antivirus checks will stop as soon as a virus is detected by the FIRST antivirus solution. For example, if a third-party product detects a virus in the spool or in an uploaded file, any other antivirus programs will not process the same message.

When accessing Antivirus settings, the following options will be available. Note: The virus Quarantine Directory — or Quarantine Path — is part of the General Settings .

Microsoft Defender Antivirus

Microsoft Defender is part of the default installation for most Windows server operating systems and delivers the comprehensive, ongoing, and real-time protection you expect against software threats like viruses, malware, and spyware across email, apps, the cloud, and the web. SmarterMail ties into the antivirus portion of Defender to offer an added layer of protection system administrators can employ. (If Microsoft Defender is not supported, a note is displayed letting the system administrator know.)

- Scan Uploaded Files - Enabling this will scan all files uploaded to File Storage, group chat, online meetings, and attachments to outgoing messages composed in webmail.
- Scan Messages With Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that have attachments. Attachments are scanned as well.
- Scan Messages Without Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that do NOT have any files attached.
- When Virus is Found in Spool - This dropdown allows you to select what you want done with a message if Microsoft Defender detects it contains a virus. These options include:

- No Action - Do nothing with the message.
- Delete Message - Delete the entire message. Note: The Delete Message action will permanently delete messages, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via virus filtering cannot be recovered.
- Quarantine Message - Move the message to the quarantine folder on the server. These messages can then be found on the Virus Quarantine tab on the Spool page. By default, messages remain in quarantine for 30 days, after which time the .eml is deleted, unless other action is taken to move the message out of quarantine.

ClamAV

ClamAV is a third-party open source antivirus toolkit that is included, at no additional cost, in the default installation of SmarterMail. For more information on ClamAV, visit: www.clamav.net Note: ClamAV's virus definitions are updated every 6 hours and its last updated date/time is displayed on the card. To manually update the ClamAV definitions, click on the Actions (□) button and select Update ClamAV Definitions .

- Scan Uploaded Files - Enabling this will scan all files uploaded to File Storage, group chat, online meetings, and attachments to outgoing messages composed in webmail.
- Scan Messages With Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that have attachments. Attachments are scanned as well.
- Scan Messages Without Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that do NOT have any files attached.
- When Virus is Found in Spool - This dropdown allows you to select what you want done with a message if ClamAV detects it contains a virus. These options include:

- No Action - Do nothing with the message.
- Delete Message - Delete the entire message. Note: The Delete Message action will permanently delete messages, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via virus filtering cannot be recovered.
- Quarantine Message - Move the message to the quarantine folder on the server. These messages can then be found on the Virus Quarantine tab on the Spool page. By default, messages remain in quarantine for 30 days, after which time the .eml is deleted, unless other action is taken to move the message out of quarantine.
- ClamAV is on a remote server - Enable this setting if the server is a remote server.
- IP Address - The IP address of the ClamAV server to use. When running ClamAV as part of the SmarterMail install, this will default to localhost. (127.0.0.1)
- Port - The port that the ClamAV server is listening on. When running ClamAV as part of the SmarterMail install, this will default to port 3310.
- Timeout (Seconds) - The maximum number of seconds SmarterMail should wait for ClamAV to respond before moving on to the next message. By default, the timeout is 10 seconds.
- Failures Before Disable - The maximum number of ClamAV timeouts allowed before it is disabled. By default, ClamAv is limited to 5 failures.

Cyren Zero-Hour Outbreak Detection

Cyren Zero-Hour Outbreak Detection is a paid add-on that The Cyren Zero-hour Outbreak Detection uses Recurrent Pattern Detection to identify "zero hour", or recently released, viruses based on their unique distribution patterns and provides a complementary shield to built-in antivirus technologies. In addition, by offloading the intensive CPU cycles onto Cyren's servers, you're protected from outbreaks the moment they occur with zero impact on your server.

- • Scan Messages With Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that have attachments. Attachments are scanned as well.
- • Scan Messages Without Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that do NOT have any files attached.
- • When Virus is Found in Spool - This dropdown allows you to select what you want done with a message if ClamAV detects it contains a virus. These options include:

- • No Action - Do nothing with the message.
- • Delete Message - Delete the entire message. Note: The Delete Message action will permanently delete messages, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via virus filtering cannot be recovered.
- • Quarantine Message - Move the message to the quarantine folder on the server. These messages can then be found on the Virus Quarantine tab on the Spool page. By default, messages remain in quarantine for 30 days, after which time the .eml is deleted, unless other action is taken to move the message out of quarantine.

Command-Line Antivirus

Administrators can integrate SmarterMail with third-party antivirus programs via a command-line execution. This can be an efficient solution for high-volume mail environments by reducing the burden on the mail server itself.

Once a message comes into the SmarterMail spool, it will then be scanned for viruses using the command-line antivirus and any built-in antivirus measures that have been enabled in SmarterMail. If the command-line scanner picks up a virus, it will be up to the command-line antivirus program to delete/quarantine the message according to the application's configuration.

- • Scan Uploaded Files - Enabling this will scan all files uploaded to File Storage, group chat, online meetings, and attachments to outgoing messages composed in webmail.
- • Scan Messages With Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that have attachments. Attachments are scanned as well.

• Scan Messages Without Attachments - Enabling this will only scan incoming or outgoing messages that are sent through the SmarterMail spool that do NOT have any files attached.

• Command Line - Enter the executable for the antivirus program. For example, if you'd like to integrate with ESET Endpoint Antivirus on Windows, you might enter something like:

```
C:\Program Files\ESET\ESET Endpoint Antivirus\ecls.exe /base-
dir="C:\Program Files\ESET\ESET Endpoint Antivirus" /aind /arch /sfx
/adware /clean-mode=Delete %FILEPATH Note: %FILEPATH will be replaced with
the path to the file to be scanned.
```

Bindings

System administrators can use this section to specify on which ports the server IP address(es) — both IPv4 and IPv6 addresses — should listen, assign protocols to those ports or assign a hostname for each IP address. All ports being used should be assigned to at least one IP address on the server. However, SmarterMail provides system administrators with some flexibility when configuring bindings. This means, for example, that the system administrator can allow POP (port 110) on the IP 111.111.111.11 but not allow it on 222.222.222.22. In addition, some servers may have other programs installed that need to listen on mail ports. To accommodate this, the system administrator can configure SmarterMail to listen on a subset of IP addresses, leaving the remaining IP addresses available for other programs.

Another benefit to binding IPs to your mail server is that you can limit the possibility of your entire mail server being blacklisted by assigning IPs on a per-domain basis. That means that spammers sending messages on your mail server will only get their domain and their specific IP blacklisted rather than getting the entire mail server blocked.

When accessing Bindings , the following tabs will be available, and each tab will display the number of items configured for each:

IP Addresses

Every IP address stored on the server's Network Interface Card (NIC) will be displayed in this section. As a result, it's not possible to add an IP address for bindings from this page: it must be available from the Network Interface Card (NIC). Information is displayed about each IP address, including its hostname, a description (if one is added), and the number of ports the IP address is assigned to.

Clicking on an IP address opens its configuration options. The following setting will be available:

• IP Address - The IP address from the server. This field cannot be edited.

• Hostname - The hostname that should be assigned to the IP address (e.g., mail.example.com). A hostname can be assigned to each IP address on the server. This is beneficial because it

allows every domain on the server to be assigned its own IP address, thereby limiting the chances of the entire mail server becoming blacklisted should a user on one domain send out unwanted emails.

• Description - A friendly explanation of the binding's purpose.

• Ports - Select each port on which this IP address should listen. All ports being used should be assigned to at least one IP address on the server.

As mentioned, the IP Addresses listed in this section are pulled from the server and can only be removed from SmarterMail by removing the IP Address from the NIC. (If an IP address continues to show in the IP Addresses section or cannot be deleted, it is possible the IP address is still contained in the server registry. After removing an IP address from the NIC, be sure it is removed from the registry as well.) Occasionally, however, an IP address that is NOT stored in the server's NIC may appear in this list. These IP addresses can be removed using the Delete button, if desired.

Ports

Use this section to assign specific protocols to ports or to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules to any ports and protocols. When viewing this tab, each port added will be listed, and some information about each is avaialble, including its name, the type of port, and the number of IP addresses assigned to the port.

To add a new port, click the New button. To edit an existing port, simply click on it. Regardless of whether you're adding a new port or editing an existing one, a modal opens and the following settings will be available:

• Protocol - The type of communications protocol that should be used (IMAP, LDAP, POP, SMTP, XMPP, or Submission Port).

• Port - The port number on which to listen for the selected protocol.

• Name - The friendly name for the port.

• Encryption - If the port requires SSL or TLS encryption, select the appropriate option. SSL always assumes the connection will be secure and sends the encryption immediately. TLS connects normally and then looks to see if the connection is secure before sending the encryption.

• Certificate Path / Password - If SSL or TLS encryption is selected, enter the complete path to the security certificate and its corresponding password.

• IP Addresses - Every IP address on the server will be listed here. Select the IP address(es) on which this port should listen.

<u>Regarding SSL Certificates</u>

When adding or modifying ports, one thing asked for is an Encryption type. If SSL or TLS is selected, SmarterMail asks for a Certificate Path and Password . Even when using SmarterMail to manage SSL Certificates, those fields are still required. This is because some clients do NOT support SNI. For this reason an administrator will need to add a certificate to act as a fallback for each SSL/TLS Port binding in order for SmarterMail to listen for TLS connections. It can be the same certificate for each port and administrators should verify all secure port bindings are configured to use a certificate file that includes the private key.

Delivery Limits

Below are the features available when viewing the Delivery Limits section of SmarterMail. Delivery limits allow a system administrator to manage how email is routed through the SmarterMail server. Handling routing helps prevent the server from possible blacklists for mishandling spam, from sending mail it shouldn't send, and more. There are three (3) main ways system administrators can handle routing mail. These include:

Do Not Forward

The Do Not Forward list is a useful tool for preventing issues with companies that have extremely strict spam policies. For example, AOL and Comcast do not differentiate between the sending server and the server that forwarded a spam message. As such, they commonly blacklist legitimate domains for forwarding spam. Because it's impossible to prevent ALL spam messages from being forwarded when a user has automated forwarding enabled, system administrators may prefer to completely prevent email forwarding to those strict domains. Note: Do Not Forward only prevents the automated forwarding of email, which is configured in the user's general settings. Any messages that are manually forwarded by Users are not impacted by the Do Not Forward list.

To add a new Do Not Forward domain, click the New button. To Edit an existing domain, click on it and you can change it. To Delete an existing entry, select the entry (or multiple entries) and click Delete . When adding or editing an entry, the following option will be available:

• Domain Name - Enter the name of the domain that should be blocked from automated email forwarding. When a domain is included in this list, users will see the following notification when they attempt to save a forwarding address with that domain: "Forwards to the following address(es) are not allowed: _____." Note: Users will still be able to manually forward emails to users on that domain.

Sender Priority

Sender Priority allows the system administrator to assign priority levels to specific email addresses. For example, a company may want the mail server to send emails from its support team (support@@example.com) before sending emails to mailing lists.

To create a new sender priority override, click the New button. To edit an existing entry, click on it. To Delete an existing entry, or multiple entries, select it and then click the Delete button. When adding or editing an entry, the following settings will be available:

- Email Address - The email address of the user or group.
- Message Delivery Priority - The priority level assigned to this user's messages.
- Description - A brief summary why the sender priority override was created.

Reserved Domains

System administrators can prevent certain domains names from being added to SmarterMail. For example, domains that are already used for free email services, like gmail.com or yahoo.com, are ideal additions to the reserve list as allowing administrators to add such domains to SmarterMail could affect message delivery. Similarly, domains that are traditionally reserved for testing and documentation, such as test.com or example.com are also ideal candidates for the reserve list.

To add new Do Reserved Domains, click the New button. To Edit an existing domain, click on it and you can change it. To Delete an existing entry, select the entry (or multiple entries) and click Delete . When adding or editing an entry, the following option will be available:

- Reserved Domain Name - Enter the domain name. It's also possible to add multiple domains, and each should be on its own line.

System Events

This settings page is only available to administrators of the SmarterMail installation.

The Event system in SmarterMail is an incredibly powerful and flexible tool that allows administrators to automatically perform actions based on specific criteria and remain up-to-date with what is going on with the SmarterMail server, domains and user accounts. SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to users that need the information. For example, a system administrator can create an event that will automatically notify a domain's administrator(s) when a domain's disk space has met a certain threshold.

Another example can be a situation where, for business or legal reasons, a company wants all of the emails sent to and from their users to be "journaled", or sent offsite for backup purposes. While SmarterMail includes a robust Archiving feature, journaling is a little different. In many cases, a

company wants messages copied to another address, at another service, to serve as a backup, or archive, of their communications. The Events system in SmarterMail makes this very easy. Events can be created — one for messages sent and one for messages received — that add a recipient to each type of message. This recipient can be an external address that collects all of a domain's emails for offiste backup. The senders, and recipients, won't even be aware that their messages are being journaled.

By default, SmarterMail is installed with several pre-defined system events. These are available to help system administrators keep track of important information, such as the impending expiration of any paid add-ons, when a new version is available to be downloaded and installed, when the overall disk space usage on the server is getting to a critical point, when a user's disk space is getting to a critical point and more. Any "built-in" Events are labeled as such — these Events can not be deleted, though they can be edited. Other pre-defined events can be edited and changed to match the needs of the system and system administrator, or deleted entirely.

Creating New Events

To create a new event, click New . The following options will be available:

General

- Event Name - The friendly name of the event.
- Event Status - New events default to a status of Enabled. However, to temporarily stop an event from triggering, you can change the status to Disabled.
- Event Category - The feature to which the event pertains: User, Mailing List, Alias, Throttling, Email or Collaboration.
- Event Type - The occurence that triggers the event. Each category has several specific event types that can trigger the action.

Conditions

Each event type has its own corresponding conditions. The global conditions that are seen across all event types are listed below.

- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Service - The service impacted that would fire the event: SMTP, POP, IMAP, Delivery, POP Retrieval.

Actions

Each event type has its own corresponding actions. The global actions that are seen across all event types are listed below.

• Send a notification - This option will send a notification to the Notifications window. It can also send a popup browser notification and an email.

• Send an email - This option will send an email to the specified address.

• Command Line Action - Execute a specified command line. A note about Maximum Frequency: Generally, this is used to set how frequently the action is performed. For example, if you set a maximum frequency of 15 minutes for an event that means the event will only fire once in that 15-minute period regardless of how many times the event conditions are met. In some cases, however, SmarterMail uses a default frequency, regardless of what is set for the Event Action. This is used in place of the Maximum Frequency setting as NOT doing this would cause undue stress on the server. A perfect example of this is the Send Email Action for sending an email notification when a user is throttled. By default, SmarterMail uses a Maximum Frequency of 30 minutes for this type of event.

Event Variables

Below is a list of variables available for any and all system events. Note: This list may change as variables may be added at any time.

- Alias Addresses — #aliasaddresses#
- Alias Name — #aliasname#
- All Domain Admins — #alldomainadmins#
- Check Name — #checkname#
- ClamAV IP — #clamip#
- ClamAV Port — #clamport#
- Consecutive Failures — #consecutivefailures#
- Days Left — #daysleft#
- Day of Week - #daysofweek#
- Description — #description#
- Detected By — #detectedby#
- Disk Drive — #diskdrive#
- Free Disk Space (GB) — #diskspacefree#
- Free Disk Space (%) — #diskspacefreepercent#
- Disk Drive — "#diskdrive#
- Disk Usage (GB) — #diskspaceused#
- Disk Usage (%) — #diskspaceusedpercent#
- Domain — #domain#
- Domains Used - #domaincount#

- Domains User (%) — #domainpercent#

- Domain Usage (MB) — #domainusagemb#

- Domain Usage (%) — #domainusagepercent#

- File Name — #filename#

- File Size (KB) — #filesize#

- Forwarding Address - #forwardingaddresses#

- From Address — #emailfrom#

- From Domain — #fromdomain#

- Full Name — #fullname#

- Gateway Address — #gatewayip#

- Hard Reject — #hardreject#

- Intra Domain — #intradomain#

- IP Address — #ipaddress#

- Add-on Name — #licensefor#

- List Name — #listname#

- Location — #location#

- Mailbox Allowed Size (MB) — #mailboxsizemax#

- Mailbox Usage (MB) — #mailboxusagemb#

- Mailbox Usage (%) — #mailboxusagepercent#

- Mailing List Address — #mailinglistaddress#

- Max Disk Size (GB) — #diskspacegbmax#

- Max Domain Size — #domainsizemax#

- Memory Used (MB) — #memoryusedmb#

- Memory Used (%) — #memoryusedpercent#

- Messages an Hour — #amtinhour#

- Password — #password#

- Percent Complete — #percentcomplete#

- Primary Domain Admin — #primarydomainadmin#

- Priority — #priority#

- Rule Name — #rulename#

- Rule Type — #ruletype#

- Server Name — #servername#

- Service — #service#

- Size (KB) — #sizekb#

- SpamAssassin IP — #spamassassinip#

- (SpamAssassin) Name — #spamassassinname#

- SpamAssassin Port — #spamassassinport#

- Spam Level — #spamlevel#

- Spam Weight — #weight#

- Spool Count — #spoolcount#

- Status — #status#

- Subject — #emailsubject#

- Subscribe Method — #subscribemethod#

- Thread Count — #threads#

- Throttle Limit Type — #throttlelimittype#

- To Address — #toaddress#

- To Domain — #todomain#

- Unsubscribe Method — #unsubscribemethod#

- Uptime (Days) — #uptimedays#

- Username — #username#

- Version — #version#

- Virus Name — #virusname#

Gateways / Failover

Gateway Setup in SmarterMail

Gateways perform a crucial function when running mail servers, especially in very busy environments. Their primary mission is to handle the flow of inbound or outbound traffic, ensuring timely and proper delivery of messages. As such, they handle the majority of the traffic, easing the sending and delivery of email to its intended recipient.

SmarterMail simplifies the ability to set up and configure gateways. Here, you select the Gateway mode, which dictates the type of gateway being set up.

If any gateways have already been created, they will be displayed here. Otherwise, this page will be blank.

Types of Gateway

Outbound gateways allow you to reduce the load on your primary server by using a secondary server to process outbound mail. Gateway servers can also be used to combat blacklisting. If the gateway server gets blacklisted, simply rotate the primary IP on the network card to a different one to send out on the new IP.

There are two types of Outbound Gateway: Round Robin or Specific Domains.

"Round Robin", means that when multiple gateways are configured, domains will use one then use the next to send mail, cycling through each gateway.

"Specific Domains" allows administrators to select a specific gateway for specific domains when those domains are being set up. (Or, it's possible to set the gateway for a domain after it's been set up.)

To add a new outbound gateway, click the New button. When adding or editing an entry, the following settings will be available:

- • Gateway Mode - The type of gateway to add. For an outbound gateway, select either Round Robin or Specific Domains, depending on the type of outbound gateway you want to add.
- • Server Address - The IP address or hostname of the gateway server.
- • Port - The port used to connect to the gateway server.
- • Encryption - Select the type of encryption from the list.
- • Status - The status of the outbound gateway. To temporarily turn off the outbound gateway, select Disable from the list.
- • Enable Authentication - Enable this setting if your outbound gateway server requires authentication. Then enter the Auth Username and Password below.
- • Auth Username - The authorized username of the gateway server.
- • Auth Password - The corresponding password for the authorized username.
- • Verify Connection before Save - Enabling this means SmarterMail will test the connection to the Server Address and Port prior to actually connecting to the gateway.

The purpose of gateways labeled "Backup MX" or "Domain Forward" are to reduce server load by pre-processing incoming messages prior to the messages being handed off for delivery to the primary SmarterMail server. For example, spam checks and antivirus scans should be performed by these types of gateway, especially in larger environments, as they are standalone servers that simply process incoming messages, so they don't act as primary mail servers. This frees up the primary server so all it has to do is deliver messages to individual users.

A "Backup MX" will only receive messages when your primary server is down.

A "Domain Forward" allows you to easily send mail through one server to another and permit you to have a single point of entry for inbound SMTP traffic. When messages come in for a forwarded domain, they are handled just like any other incoming message, which includes being handled based on the Spool settings for the server. (I.e., Settings > General > Spool.) For example, if a delivery delay has been established for the server, messages are also delayed accordingly. In addition, an inbound server can run external virus or spam scanners, which can reduce the load on your existing network servers.

To set the server as either a Backup MX or Domain Forward, click the New button and select your option. When adding or editing an entry, the following settings will be available:

- Gateway Mode - The function that the inbound gateway will perform: Backup MX or Domain Forward.
- IP Addresses (single, range or CIDR block) - The IP address, or range of IP addresses, of the primary mail server.
- Status - New gateways default to a status of Enabled. To temporarily stop an inbound gateway, you can change the status to Disabled.
- Description - A friendly name for the inbound gateway.
- SMTP User Verification - Available when setting up a Domain Forward, this setting makes SmarterMail verify that a recipient exists when accepting mail from the gateway.

Domains Note: This card is only available if the gateway mode is set to Domain Forward, so it's used to specify which domains the gateway will accept mail for:

- Domain Verification - The method used by the inbound gateway to determine if a domain is valid or not: Specified Domains or All But Specified Domains. List the domain(s) below (one entry per field).

SmarterMail Gateway

This allows you to specify whether the gateway being set up will be used for another SmarterMail server. If you're seeing slowness in mail deliveries, and the gateway is set up as a Backup MX or Domain Forward AND SmarterMail Gateway, and the spool count is high, it's possible something is tying up the transfer of mail from the gateway to the SmarterMail server.

- Enable SmarterMail Gateway Mode - Select this option to indicate that the gateway is being created for a separate SmarterMail server that is actually hosting the email.
- SmarterMail URL - The webmail URL for the SmarterMail server the gateway is being set up for. For example, you have one SmarterMail server being set up as a Domain Forward "inbound" gateway (e.g., gateway1.example.com), and it's forwarding mail to a domain (or to domains) on a separate SmarterMail server (e.g., mail1.example.com). The information input as the "SmarterMail URL" will be the primary URL for the SmarterMail server the gateway will forward email to, or https://mail1.example.com. Use of a SmarterMail gateway allows administrators the abiltiy to use web services to verify the users and domains, if needed. Note: SmarterMail uses a cache of the domains and users on a server, so if there are any changes (e.g., additions, modifications like enabling/disabling users or domains, or deletions) these changes may not be reflected for up to 10 minutes until the cache is refreshed.
- SmarterMail Username - The identifier used to log in to the SmarterMail server.

• SmarterMail Password - The corresponding password used to log in to the SmarterMail server.

• User Verification - The method used by the inbound gateway to determine if a user is valid or not. Note: If none is selected, the inbound gateway server will accept all email addresses for the domain. If Web service is selected, the inbound gateway will check with the primary mail server for a list of valid email addresses.

Spam Note: This card is only available if the gateway mode is set to Domain Forward or Backup MX.

As Backup MX or Domain Forward gateways act on mail coming into the server, it's possible to specify the actions taken for the messages that are classified as spam Low, Medium, or High. If a message is processed that is NOT marked with a spam level, actions can still be taken as well.

Configuring SmarterMail for Failover (Windows Only)

This feature is only available in SmarterMail Enterprise for Windows.

Who Should Use This

This document is intended for use by administrators deploying SmarterMail in high-volume environments and/or for organizations that want to ensure maximum uptime. It provides minimal system requirements and considerations for deploying SmarterMail in a failover environment. Note: Failover requires activation of SmarterMail Enterprise. For licensing information for this product, contact the SmarterTools Sales Department .

Failover Overview

SmarterMail Enterprise allows organizations to decrease the likelihood of service interruptions and virtually eliminate downtime by installing SmarterMail on a standby server that is available should the primary mail server suffer a service interruption. For businesses that use their mail server as a mission-critical part of their operations, failover functionality ensures that the business continues to communicate and that productivity remains at the highest levels possible, even if there is a primary server failure.

Understanding How Failover Works

The main components of failover functionality are; a primary server that acts as the default
SmarterMail server and manages the licensing of the server cluster, and a secondary server that
remains connected and available in a "hot standby" mode until the primary server experiences
problems with network access or system hardware. It's considered a "hot standby" because the server
is "hot", in that it's powered on, but the SmarterMail service (and possibly the web server) are
inactive/disabled.

If the primary server fails, SmarterMail can be configured to automatically enable services on the secondary server. When this occurs, the secondary server then takes over responsibility for processing background threads and supporting all email functionality. This server will remain in active status until another failure occurs or the primary mail server comes back online.

The initial set up of SmarterMail's failover functionality entails system administrators manually disabling both the node and SmarterMail service on the primary server and then starting the node and SmarterMail service on the standby. However, system administrators can easily use third-party monitoring systems and script an automated failover and recovery strategy as needed. An example of this is provided at the end of this document.

Minimal System Requirements

• A minimum of two servers running Microsoft Windows Server 2019 64-bit. (Windows Server Core is not currently supported).

• Three IP addresses

• Both servers must have their server times synchronized

• A domain account or local system User or Group account with bidirectional authentication. Note: SmarterMail can NOT be run using Local System, Local Service or Network Service in a failover configuration.

• NFS/SMB share for mail and system files. We recommend that the share is running on a NAS/SAN that is configured as RAID 10

Adding Network Load Balancing to Your Servers Note: This needs to be performed on each server that will be used in the failover environment.

• Open the server manager console

• Right click on Features in the tree view and select Add Features

• Check the box next to Network Load Balancing and select Next

• Click Install

• Once the installation finishes, click Close

Configuring the Load Balanced Cluster for Use with Failover

• Navigate to Start → Administrative Tools → Network Load Balancing Manager

• Click the Cluster menu item and select New

• In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New

• When the Interface Name and Interface IP appear, select the Interface Name and click Next

• Since this is the primary node, ensure the host Priority is set to 1

• In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are

correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines. Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.

• Click Next

• In the New Cluster: Cluster IP Addresses window, click Add and enter in your cluster IP address and the same subnet mask as in Step 6

• Select Next

• In the New Cluster: Cluster Parameters window, confirm the IP address and subnet mask, then enter a Full Internet Name , though this is optional

• Ensure the cluster operation mode is set to Multicast

• Click Next

• In the New Cluster: Port Rules window, click Edit

• If you want you can restrict the cluster IP to work on an individual port or across a port range. You can also simply allow the cluster IP to work across all ports on the server

• Ensure your port rules are set to Single Host in the Filtering Mode section

• Click OK

• Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

• From the secondary server navigate to Start → Administrative Tools → Network Load Balancing Manager

• Click the Cluster menu item and select Connect to Existing . Note: the existing cluster will need to be running before a secondary node can be added

• In the Connect to Existing: Connect window, enter the IP address of your existing cluster as the Host and click Connect

• Select the existing cluster that appears in the Clusters section and click Finish

• In the main Network Load Balancing Manager , expand Network Load Balancing Clusters and right-click on your Cluster (it may be the IP address of your cluster) and select Add Host to Cluster

• In the Add Host to Cluster: Connect window, enter the IP address of the secondary server in the Host: section and click Connect

• When the Interface Name and Interface IP appear, select the Interface Name and click Next

• In the Add Host to Cluster: Host Parameters window, confirm the IP address and subnet mask and ensure the Initial Host State is set to Stopped . As this is the second node you're adding to

your cluster, the Priority should be set at 2

• Click Next

• Just as with the primary node, in the Add Host to Cluster: Port Rules window you have the ability to set this node to respond via specific ports or a port range. If you wish to set these rules, click Edit . Otherwise, click Finish to complete the setup

• Wait for the nodes to converge and, if necessary, stop the secondary sever by right-clicking the second server's name, select Control Host → Stop

Configure a Shared Service Directory

• Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. Note: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.

• Inside that new SmarterMail folder, create a Settings folder

• Configure your permissions accordingly. The SmarterMail service needs to run as a domain account or a local account with bidirectional authentication. You can configure this within the Windows Services console. When running SmarterMail with failover, Local System, Local Service and Network Service users are not allowed. Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

• Manually install and configure a primary SmarterMail server using the .MSI file available from the SmarterMail downloads page . Then, stop the service on this primary installation.

• Manually install another SmarterMail Enterprise instance on a second server. This new installation will be your standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.

• Stop the SmarterMail service on the standby

• Edit the failover.json file in the primary server's Settings folder as follows.

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer

• IsEnabled - Set this to True

• SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this (this example is for a Windows server):

```
{ "NodeId": "a51eba87-c8c6-49e3-812f-84e46ab617e7", "FailoverIPAddress":
"122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath":
"\\\\serverName\\SmarterMail\\Service\\Settings" } The code should look
like the above: casing, proper escaping of paths, etc. in order for the
JSON to be read properly.
```

• Save this file, then copy it to the standby's Settings folder, replacing the existing failover.json
• Copy over all folders and files from SmarterMail's Settings folder to the Settings folder in the shared service directory you created.
• Start the service on the standby server and verify that the paths are pointing to the network shared paths
• Activate your Enterprise key on the standby by logging into SmarterMail's management interface as the system administrator and going to the activation section. Then stop the SmarterMail service on the server
• Start the service on the primary server, then reactivate your Enterprise license key in the SmarterMail management interface
• After re-activating the license, go to IP Addresses and bind all the ports to the load balancer's IP address and make sure no other IPs have any ports bound to them
• Both servers are now set up for failover. To verify this, log into the primary server as the system administrator and go to Gateways / Failover . The servers that are part of the failover cluster will be displayed on the Failover Servers tab.

Adding Failover to an Existing Installation of SmarterMail Note: You will need to configure both servers for Network Load Balancing and set up a shared service directory. See the steps outlined in the Adding Network Load Balancing to Your Servers , Configuring the Load Balanced Cluster for Use with Failover , Joining Additional Nodes to the Cluster and Configure a Shared Service Directory sections earlier in this document for more information.

• Ensure the primary server is running the latest version of SmarterMail and that it is also configured as an IIS site. Ensure the IIS binding is pointing to your cluster IP address

• Install SmarterMail on a standby and configure it as an IIS site. Ensure the cluster node is stopped on the standby and ensure the IIS binding is also pointing to the cluster IP

• Stop the SmarterMail service on the standby

• Copy all of your mail data (located in C:\SmarterMail\ by default) to your shared service directory. If possible, use robocopy to do this because it will not result in any downtime for the mail service

• Once robocopy finishes, run it one more time. This second pass will only copy any new data

• Stop the SmarterMail service on the primary server

• Edit the failover.json file in the primary server's Settings folder as follows:

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer

• IsEnabled - Set this to True

• SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this:

{ "NodeId": "a51eba87-c8c6-49e3-812f-84e46ab617e7", "FailoverIPAddress": "122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath": "\\\\serverName\\SmarterMail\\Service\\Settings" } The code should look like the above: casing, proper escaping of paths, etc. in order for the JSON to be read properly. Also, due to size limitations, in the sample above the SharedSystemFilesPath is split across 2 lines -- that should be ONE line.

• Copy that failover.json file, after you've edited it, and move it to the same location on the standby. You should replace the file on the standby, if it already exists.

• Run the robocopy one more time to copy over any modified files and remaining spool emails

• Copy over all folders and files from the SmarterMail service's Settings folder to the Settings folder in the shared service directory you created.

• Edit the domains.json file in the shared Settings folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)

• Edit the settings.json file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on E:\SmarterMail, you would then perform a find and replace for all instances of E:\SmarterMail to \\NAS01\SmarterMail).

• On the primary server, go to Start → Administrative Tools → Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node

• Start the SmarterMail service on the standby

• Access SmarterMail's web interface at the cluster IP and sign in as the system administrator

• Activate your Enterprise key on the standby by logging into SmarterMail's management interface as the system administrator and going to the Licensing section.

• Verify that the data and settings are being picked up from the shared Service directory

• Stop the SmarterMail service on the standby and stop the secondary cluster node

• Start the cluster node and the SmarterMail service on the primary server

• Sign into the web interface on the primary server and re-activate the Enterprise license key by going to the Licensing section.

• Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

Below is an example of a PowerShell script that can be created to automate the SmarterMail failover process. You can utilize a third party monitoring product such as PRTG or SolarWinds (though there are many others) to execute this script when a failure is detected.

Prepping PowerShell on the Servers

The servers will need to be configured to run remote scripts and accept remote PowerShell sessions. Therefore, on each server, run the following commands within an elevated PowerShell console:

- Set-ExecutionPolicy RemoteSigned - Press Y to accept
- Enable-PSRemoting -force

Sample Script - Stop a Primary Server and Start the Hot Standby

In the scripts below, replace the "WAN" variable called in the –hostname parameter with the name of your interface. This can be obtained by opening a PowerShell console on the server and typing Get-NlbClusterNodeNetworkInterface . Also replace Server01 and Server02 with the NetBIOS names of your servers.

```
$StopPrimary = New-PSSession -ComputerName Server01 Invoke-Command -Session
$StopPrimary -ScriptBlock { Import-Module NetworkLoadBalancingClusters ;
Stop-nlbclusternode -HostName Server01 -InterfaceName "WAN" ; import-module
WebAdministration ; stop-webapppool SmarterMail; set-service -computerName
Server01 -name mailservice -status stopped ; remove-pssession Server01}

$StartSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StartSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; set-service -computerName Server02 -name mailservice
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-pssession Server02 }
```

Sample Script - Stop the Hot Standby and Re-start the Primary Server

These scripts can be used to bring the primary server back online and stop the standby after your monitoring software issues an all-clear.

```
$StopSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StopSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool
SmarterMail; set-service -computerName Server02 -name mailservice -status
stopped ; remove-pssession Server02}
```

```
$StartPrimary = New-PSSession -ComputerName Server01 Invoke-Command -
Session $StartPrimary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server01 -
InterfaceName "WAN" ; set-service -computerName Server01 -name mailservice
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-pssession Server01 }
```

General System Settings

Below are the configuration options available when viewing the General Settings section of
SmarterMail.

- Server Info
- Paths
- Webmail Login
- Webmail
- Reports
- Folder Auto-Clean
- Calendar Auto-Clean
- Notification Auto-Clean
- File Storage
- Cloud Storage
- Attachments
- External Senders
- Spool
- Message Archiving
- Footer
- Block Authentication by Country

Server Info

- Hostname - The hostname of the server.

Note: Hostnames should be in the format computername.domain.com.
• DNS IP Address #1 - The IP address of the primary DNS server. If left blank, the DNS server
information will be pulled from the Windows Networking settings. (Recommended.)
• DNS IP #2 - Enter the IP address of the secondary DNS server. If left blank, the DNS server
information will be pulled from the Windows Networking settings. (Recommended.)

Paths

By default, SmarterMail stores certain information in pre-defined paths. However, there may be times when system administrators want certain things stored in separate locations. A perfect example of this is the SmarterMail Spool: for many servers, having the Spool process on a separate drive on the server can increase performance and server reliability, not to mention save disk i/o. That's because the Spool for any mail server can tax a drive due to all the file reads and writes. Having the Spool on a separate drive — we recommend putting it on an SSD drive — can help the overall lifetime of a mail server.

In this section, system administrators can specify which drive paths to use for the following:

• Spool Path - Having the Spool on a separate drive is recommended for any mail server due to the i/o required. If you are using a real-time virus scanner, this is the path that must be scanned in order to properly handle viruses.

• Log Files - Storing SmarterMail log files on a separate drive means that more space is available for users. Depending on how log files are set up — the level of detail stored for each — having a separate, large hard drive specifically for log files means less potential for disk space issues for users. Note: Changing the log path will not take effect until you restart the SmarterMail service.

• Quarantine Path - This is the directory used for files caught by SmarterMail's antivirus and antispam integrations. Having quarantined items stored on a separate drive can further protect a mail server from issues caused by viruses.

Webmail Login

Small businesses using SmarterMail on their own servers, or even companies using SmarterMail from their hosting provider, will benefit from the ability to customize the SmarterMail login page to add a company logo, provide additional branding text, or simply adjust the default 'Login to SmarterMail' text to be more in line with an overall brand message. Note: System administrators can allow domain administrators to override the custom login screen by editing the Domain and enabling Webmail Login Customization in the Features section.

• Logo Image - Upload an image, like a company logo, by dragging and dropping a file in the highlighted area or clicking to browse for a file (max file size of 3mb). Uploading an image using this upload control will host the image publicly on the server and enter the tag in the HTML section. Note: Uploading an image here alone will NOT display the image on the login screen. The HTML must remain in the Login Page HTML section. This upload control can be used by those who don't have their logo publicly hosted or who wish the image source to point back to their mail server. Furthermore, regardless of the image uploaded, the image's source URL will remain the same; only one image may be hosted at a time.

• Custom Login Text - Use this setting to customize the login page header to something more in line with an overall brand message. If Custom Login Text is left blank, SmarterMail's login page will show the default text "Welcome to SmarterMail".

• Custom Title Text - Use this setting to customize the title of the login page to something more in line with an overall brand message. If Custom Title Text is left blank, SmarterMail's login page will show the default text of "SmarterMail" in the browser tab title. Note: When a system administrator is logged in, the custom title text will appear on all pages. If the login display for a domain is not set to default or overridden, users will see this text on the login page only, with their email address displayed as the browser title for all other pages.

• Login Background - Use this option to select the background image(s) that displays on your login screen. Use the default images that come with SmarterMail, point to your own path on the server or select a solid color background. For custom images, the following image formats are supported: SVG, PNG, JPEG/JPG and GIF. Minimum size is dependent upon the image type being used. However, you can use 1920 x 1280 as a general guideline.

• Enable custom login page HTML - Check this box to enable the ability to use HTML to further modify the login screen to add additional text or adjust the layout.

• Login Page HTML - Enter the custom HTML that will be used to further modify the login screen (in-line custom CSS can be used as well). Note: To include white space around the Image on Login Screen, the div id "companyinfo" must be included.

Webmail

• Logout URL - By default, users are presented with the login page for their mail server when they log out of webmail. Entering a full URL here means the added URL will open in the user's window once they log out instead of the login page.

• Replace online help with custom URL - When enabling custom help, whatever is entered as the Custom Help Text, and the URL that text redirects to, will replace the standard, default Online Help link that is displayed. That means you'll be redirecting users of the SmarterMail server to your OWN help documentation and away from the documentation created by SmarterTools.

• Hide external email avatars - This allows system administrators the ability to block email avatars from services like Gravatar or other external image sources.

Reports

Use this tab to specify the following settings:

• Delete Server Stats After (Months) - The length of time server stats should be kept before being deleted. By default, server stats are deleted after 13 months.

• Delete Domain Stats After (Months) - The length of time domain stats should be kept before

being deleted. By default, the domain stats are deleted after 13 months.

• Delete User Stats After (Months) - The length of time user stats should be kept before being deleted. By default, the user stats are deleted after 13 months.

Folder Auto-Clean

Folder Auto-clean is a method for limiting how much of a user's disk space is used by the Junk EMail, Sent Items, and Deleted Items folders. By placing limits on the size of these folders, system administrators can help ensure that user accounts do not fill up unnecessarily. Messages are deleted from the folders in the order that they were received so that older messages get deleted first.

• Allow domains to override auto-clean settings - Enable this setting to allow domain administrators to create their own auto-clean policies for their domain.

• Allow users to auto-clean Inbox - Enable this setting to allow users to create auto-clean policies on the Inbox folder.

Any existing auto-clean rules will be listed. To add a new folder auto-clean rule that will apply to all users across all domains, click on the New Rule button.

If the Rule Type is set to Size, the following options will be available:

• Folder - The folder that will be auto-cleaned: Deleted Items, Junk Email or Sent Items.

• When size greater than (MB) - The maximum size of the folder, in megabytes. Once the folder reaches this size, the auto-clean process is started and older messages (messages that were received the longest time ago) are deleted.

• Reduce to (MB) - The size the folder should be after the auto-clean process has completed, in megabytes. When auto-cleaning, SmarterMail will delete older messages first until the folder reaches this size. Note: This number should always be lower than the previous field.

If the Rule Type is set to Age, the following options will be available:

• Folder - The folder that will be auto-cleaned: Deleted Items, Junk Email or Sent Items.

• Days - The maximum number of days mail will stay in the selected folder before deletion.

Auto-Clean Timings

Size-based auto-clean rules are run whenever an action is performed on a particular folder. For example, moving a message into the folder. Once that action occurs, the auto-clean rule is run, and it runs each time an action is performed. Age-based rules, however, run once per day, on the FIRST folder action for that day. For example, deleting an email first thing in the morning. When you delete an email, it's moved to the Deleted Items folder, which is a folder action. At that point, if there's an age-based auto-clean rule for the Deleted Items folder, the rule is run and then is silent until an action

is performed on the next day. If no action is performed on a folder with an age-based rule, the rule still runs automatically shortly after midnight, server time.

Calendar Auto-Clean

Having a system-wide setting for all domains that limits past calendar appointments is another way to help prevent disk drives from filling up. Just as with messages, calendar appointments are deleted in the order they were created or accepted.

> • Calendar Auto-Clean Months - The max age of a calendar appointment before it is permanently deleted. By default, this is set to 12 Months.
> • Allow domains to override auto-clean settings - Enable this setting to allow domain administrators to create their own auto-clean policies for their domain.

Notification Auto-Clean

One other way to help limit disk space is by automatically cleaning out old notifications for a user's account. When notifications are dismissed, they're still logged by SmarterMail. Therefore, unless old notifications are actually deleted, that log file can grow rapidly, especially if a user has a number of notifications. When notifications are automatically cleaned, they're cleaned in the order they were created or dismissed.

> • Notification Auto-Clean Days - The max age of a notification before it is permanently deleted. By default, this is set to 30 Days.

File Storage

SmarterMail's file storage feature allows users to upload files to the server and share them via public links. One benefit of using file storage is that it reduces the stress on the server by keeping large files out of the spool. Note: Files uploaded to the server are counted toward the user's disk space allocation, so system administrators should encourage users to delete any unused files whenever possible.

> • Max File Size (KB) - The maximum size a file can be in order to be uploaded to the File Storage area. This has a relationship to the file size limits for attachments, and any files uploaded to Online Meetings and/or Chats as all of those items are stored in a user's File Storage area.
> • Root Webmail URL - The base URL of any file stored and shared in file storage. By default, the base URL corresponds to the domain the mail server is set up on (i.e., http://mail.example.com). If SmarterMail is configured on an external IP that allows a network address translation (NAT) to an external IP, the system administrator may need to modify the root URL.

Cloud Storage

SmarterMail's cloud file storage feature enables users to upload files to the server and share them via public links. By storing large files separately, this feature helps reduce server load and keeps the spool optimized. System Administrators can integrate various add-ons with SmarterMail to enhance file storage capabilities.

Visit the Marketplace to explore available Cloud File Storage add-ons.

Attachments

- Inbound Extension Blacklist - This list allows you to limit the file types that are allowed INTO the mail server. For example, many email administrators won't allow executable files (EXE) as they can cause issues on the mail server, and possibly across an entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .exe or EXE)
- Outbound Extension Blacklist - This list allows you to limit the file types that are users are allowed to send OUT OF the mail server. For example, many email administrators won't allow batch files (.BAT) as they can cause issues on the recipients' mail server, and possibly across their entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .bat or BAT) IF a user attempts to send an email or create a calendar appointment invitation that contains a blacklisted file extension, the outbound delivery of that message or invite is blocked.
- Extension Blacklist for Uploads - Use this section to select and list any file types that cannot be uploaded to the server across any area. This includes files uploaded to File Storage, attachments to calendar appointments, contacts, contact groups, tasks, and notes, as well as files added to signatures or uploaded via chat or in Online Meetings. Essentially, any area that allows a file upload. System administrators may want to limit the capabilities of users to upload certain file types, such as executables (.exe) or other file types that can possibly be used to cause problems on the server.

External Senders

SmarterMail has the ability to notify users when an email they receive has originated from an account outside of their organization and/or their domain. For example, financial institutions like to be notified if an email comes from someone outside of their own company, and that's where the External Sender text comes in handy.

That said, some organizations like for their users to be able to manage the accounts this text appears on, without disabling it entirely. For those organizations, SmarterMail allows system administrators to give domains the ability to overrid this setting. In addition, system administrators can select where to add external sender text: It can be appended to the body of the message or the subject line.

• Allow domains to override external sender settings - When enabled, domain administrators can modify the settings made by system administrators, customizing them for their own users.

• Add text to body - When enabled, this will add a text box to the body of the message that cautions the recipient that the email originated outside their own domain, and to take caution when clicking links or opening attachments.

• Add text to subject - When enabled, this adds the text "[EXTERNAL SENDER]" to the subject line of the message.

Spool

• SubSpools - SubSpools are within the spool path and allow SmarterMail to work around the NTFS limitation of 30,000 objects in an individual folder. SmarterMail will utilize subspools by evenly distributing mail among the subspools, allocating up to 10,000 messages per subspool. If the subspool count is set to 1, the Spool folder will be used. Note: If the subspool count is lowered, the old subspool folders will not be automatically deleted; however, you may manually delete the unused subspool folders if you wish. This design is to accommodate for situations where the subspool count is lowered while mail is still processing in those folders. (Default value is 10)

• Delivery Delay (Seconds) - This number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message. By default, the delivery delay is 1 second.

• Retry Intervals (Minutes separated by commas) - When the mail server is unable to contact the receiving server, the email attempting to be sent is held for a period of time before the mail server attempts to resend it. This is the time between retries. Users can specify multiple retry attempts to resend emails before it is bounced. By default, this is set to 16 attempts - at 1, 5, 5, 15, 30, 30, 30, 30, 60, 90, 120, 240, 480, 960, 1440, 2880.

• DNS Errors Before Bounce - The maximum number of attempts SmarterMail should make before the message is bounced due to a DNS error. The most common cause of a DNS error is a misspelled domain. Limiting the number of attempts before DNS errors are bounced is beneficial because messages will not sit in the queue for long periods of time taking up processing on the mail server and possibly slowing the system down. This will be helpful to users because messages will be bounced sooner and will give users the opportunity to fix any mistakes and get a message resent. By default, the server will make 2 attempts. Note: Setting this at 1 retry can be dangerous if the DNS server fails or if there is a loss of Internet connectivity. To disable this feature, set the number of bounces equal to the number of retry intervals.

• Notify Senders of Delay After (Attempts) - Sets the number of delivery attempts before the

sender is notified that the email delivery is delayed. This can be beneficial as it lets the sender know that the mail server is still attempting to deliver the message but that the recipient has not received it yet. (Default value is 0.)

• Max Local Delivery Threads - Enter the maximum number of messages that can be sent at one time to email addresses that are on the local server. If a message cannot be sent, the server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. (Default is 50)

• Command Line File - Move the slider to the right to enable this option. Then enter the full path to an executable you wish to use to process incoming messages. Use %filepath as an argument to pass the path of the email file to the executable. It is allowable for the executable to delete the message to prevent delivery. Example: If you set this field to "c:\program files\myexe.exe %filepath" on Windows, the program myexe.exe will be launched with the full path to the spool file as its first argument.

• Command-Line Timeout (Seconds) - The number of seconds that the server will wait for information from the remote server. By default, the timeout is set to 5 seconds.

Message Archiving

By default, SmarterMail does not archive messages for new installations. System administrators need to set up rules for archiving domains — either all domains or for individual domains, depending on need. To specify which domains on the SmarterMail are archived, the system administrator will need to create archiving rules on each domain's Configuration card when the domain is added to the server. (Or edit each domain individually if it's already been added to the server.)

Alternatively, a rule can be created that will archive messages for all domains on the server. To create a rule for archiving all domains, use the Settings button.

By default, SmarterMail will set an archive path, which will match the default data path set up when SmarterMail was installed. (This is generally c:\SmarterMail\Archive.) However, that path can be edited as needed. Then, it's possible to select which messages are archived: all messages, inbound messages, or outbound messages. Finally, set the Archive Auto-Clean rules.

Regarding auto-clean rules, this is purely dependent on need and business rules. Administrators can elect to purge messages in yearly increments, from 1 to 10 years. They also have the opportunity to disable auto-clean rules by selecting "Never". Realize, however, that never cleaning out the archive can take up quite a bit of space, so plans should be made accordingly.

Creating Message Archiving Rules

When adding or editing a message archive settings, the following settings will be available:

• Archive Path - The directory on the hard drive in which archived messages are saved.

• Direction - Set the direction of the messages you want added to the Archive. The following Rules are available:

• Save All Messages

• Save Inbound Messages

• Save Outbound Messages

• Archive Auto-Clean - How long to store messages in the archive before they're automatically deleted from the server.

Once email archiving is set up, both system administrators and domain administrators can search the archives. Note: Please note that domain administrator search requires individual domain archiving rules to be set up, as noted above. It is also important to know that archives are not deleted by SmarterMail and, as a result, they can get very large. Be sure to check your archive folders regularly to see if they should be backed up and removed from the hard drive.

Archive Autoclean

Message archiving has an automated autoclean feature to help preserve mail server disk space. By default, on new installations, this is set to five (5) years. However, when setting up archiving rules, this can be adjusted to Never, or in one (1) year increments between one (1) and ten (10) years, as needed. For upgrades, autoclean defaults to "Never".

Footer

System administrators can configure server-wide message footers that SmarterMail will append on all incoming and outgoing messages. Messages that a SmarterMail user forwards that already has a footer will not have the system footer appended as well. Although similar to signatures, message footers are typically used to convey disclaimers or provide additional information. For example, a system administrator may want every message to include a notice that the message was scanned for viruses or the text "Sent by SmarterMail."

• Enable footer for all messages - Move the slider to the right to turn on the message footer for all incoming and outgoing messages. This setting does not need to be enabled to allow domain administrators to override. If domain admins do override this setting and it's enabled for all messages, emails will have the domain footer on outgoing messages but still have the system footer on incoming messages.

• Apply to mailing lists - Move to slider to the right to enable this setting and append the message footer to mailing list messages. Note: Mailing lists have their own configurable footers. If a custom mailing list footer is already configured, enabling this option will append a second footer at the end of each message posted to the mailing list subscribers. Because this may be

confusing for mailing list moderators and recipients, most administrators will choose to keep this option disabled.

• Allow domains to override footer - Move the slider to the right to enable this setting and allow domain administrators to configure a unique message footer for their domain.

• Footer - Use this section to create the message footer text. Clicking the edit icon will open a modal that includes an HTML-based editor, allowing admins to create footers that seamlessly fit into any email message. Note: The message footer does not support the use of variables.

Block Authentication by Country

Part of a system administrator's job is making sure bad actors can't attempt to brute force logins to user accounts. Blocking authentication attempts from specific countries, or ONLY ALLOWING authentication from specific countries, is one way of doing this. Adding a country to the setting will just block authentication attempts, it won't impact sending or receiving messages from the country. It will simply prevent anyone from the country(-ies) logging into the server, regardless of protocol. However, system administrators won't be able to add their "home" country, which will prevent them from accidentally locking out users. Use this card to specify the following:

It's worth noting that if an entire country is blocked, but an IP within that country is added to the server's Whitelist, that IP will NOT be blocked as the Whitelist takes priority. For example, if you blocked the entirety of Albania, but added a single IP address that falls within Albania's block, only that IP will be able to authenticate to the server. No other Albanian IPs will be able to authenticate. (No offense meant to Albania — it simply appears towards the top of the list of countries.)

• Countries to Block - Use this dropdown to select "Specified Countries" or "All But Specified Countries". When selecting "Specified Countries", authentication attempts attempted from the country(-ies) that are selected will be blocked. When selecting "All But Specified Countries", only authentication attempts from the selected country(-ies) will be allowed. Attempts from any other country will be blocked.

• Country - Use this dropdown to select one or more countries, based on the block type selected.

Licensing and Activation

During the installation process for SmarterMail, you're asked to input a license key, which defines the Edition and mailbox count that is activated once the installation completes. If you so desire, you can install SmarterMail as the Free Edition, which is good for use with 1 domain and up to 10 mailboxes.

To upgrade to a paid version and unlock additional mailboxes and/or gain access to use purchased SmarterMail Add-ons , a license key must be activated. Furthermore, if the SmarterMail installation is moved to another server or upgraded to a different version or product level, the product will need to be

activated again. System administrators can use the Licensing section to activate SmarterMail or view current licensing information and limits. Note: Activation of a license key requires the server to contact SmarterTools over port 443 (HTTPS). Please ensure that any firewall or internet security software you have installed allows an outgoing TCP port 443 request. If the server cannot connect for security reasons or due to internet connectivity, please contact sales@@smartertools.com to request steps for a manual activation. A manual activation requires the server's hostname, which can be found by entering 'hostname' into the server's command prompt.

When accessing Licensing , the current licensing details for SmarterMail and its add-ons will be displayed, including the license key, license level information, status of the license or subscriptions, the number of items used out of the total limit, and an indication of whether an add-on trial is available. A license's current Maintenance and Support status is listed as well as it's expiration date. (This includes the status of any add-ons as well as SmarterTools' licenses.)

The following actions can be taken:

• Activate - Select this option to activate a new SmarterMail license key. Activating a paid license requires authentication by verifying the SmarterTools account login credentials. Trial

license keys do not require authentication to be activated.

• Reactivate - Select this option to refresh the limits of the SmarterMail installation. This will cause SmarterMail to call back to the SmarterTools servers to refresh the limits of the license key and should be used after purchasing an add-on, upgrading to the Enterprise edition or increasing the mailbox limit. Reactivating is immediate and does not require authentication with the SmarterTools account credentials.

• Purchase - Select this option to be taken to the SmarterTools website where you can purchase a new license key or add-on.

• Start Trial - If an add-on trial is available, a Start Trial button will appear on its card. This allows the system administrator to test the functionality for up to 30 days. A trial can only be activated one time. To continue using the service after the trial, the add-on must be purchased. In addition, trials are not available on Free Editions of SmarterMail. Note: The ActiveSync trial is limited to 25 Mailboxes. Note: If you are running a trial version of SmarterMail, it will automatically revert to SmarterMail Free when the trial expires.

Volume Mounts

To system administrators, a "volume" is an accessible storage area within a file system. These are typically locations on a hard disk or other storage that are assigned drive letters. In order to use these volumes they need to be "mounted". For example, if you plug a USB drive into a Windows laptop that USB drive is automatically assigned a letter, allowing it to be used immediately. This is "mounting" that new "volume" on that laptop. While this is normally done on a server directly via command line or using a drive utility, with SmarterMail, system administrators can also mount Windows or Linux volumes directly from the web interface.

Virtually any area that has a specific path or location, from mail data to logs, can, and probably should, have its own volume mount. This allows administrators to easily scale servers without the usual hardware hassles and without touching core volumes. Best of all, adding a volume is straightforward: set the path, configure your mount and unmount commands, and SmarterMail handles the rest. Your settings stay centralized, your data remains secure, and you stay fully in control.

Uses for Volume Mounts

Be default, SmarterMail sets some default paths for various things: the Spool, logs files, and virus quarantine. In addition, each domain that's added has a Primary Path for its data, and system administrators can add Secondary Paths for domains as well. All of these paths require some type of attached storage location. This is where Volume Mounts can come in handy.

Let's say there's a particularly busy domain -- busydomain.com. The amount of message data that this domain generates grows, and grows quickly. Using a Volume Mount, it's possible to mount a new

drive and assign it a drive letter: Z:\ (in Windows). The system administrator can then go to busydomain.com and set up a Secondary Path that points to Z:\SmarterMail\Domains\BusyDomain and moves messages and SmarterMail File Storage files that are older than 90 days over to this new location on the newly mounted volume. This data is moved, in the background, but remains indexed and searchable. And each day, new data is moved once it hits whatever age the system administrator designates. The system administrator can then go in and do that for other domains so that older message data moves off of the Primary Path over to the Secondary, saving space on the primary drive.

As demonstrated, using Volume Mounts, an administrator can mount additional storage locations for SmarterMail, then set various paths to use that newly attached storage. Log files can go on one Volume, virus quarantine can go to another Volume. The efficiency of Volume Mounts within SmarterMail, then, is that you don't need to use a Disk Manager or command line to add these Mounts -- it's all handled directly from the SmarterMail interface.

Adding New Volume Mounts

To add a new Volume Mount, click the New button. When adding a Volume Mount, the following settings will be available:

- Volume Mount Path - REQUIRED. This is the location on the volume that will eventually hold the data. For example, "/var/local/folder1" in Linux, or "z:\" in Windows.
- Volume Mount Command - REQUIRED. Here, you essentially put all of the commands you'd need to mount the drive in your particular operating system. In Linux, that could be multiple commands strung together with "&&" between them. In Windows, this is simplified.
- Volume Unmount Command - This is the command necessary to unmount the volume. In Linux, that is generally "umount [Volume Mount Path]" and in Windows it is generally "net use [Volume Mount Path] /delete".

Simple Examples

Below are a couple of examples of using Volume Mounts. In both examples we'll mount volumes as simple guest shares, without the need for any credentials. However, this page is extremely flexible and can accommodate virtually any type of mount.

Linux

- Volume Mount Path: /mnt/everyone
- Volume Mount Command: mkdir -p /mnt/everyone && echo -e "//it-drive/everyone /mnt/everyone cifs guest,iocharset=utf8,uid=$(id -u),gid=$(id -g),file_mode=0775,dir_mode=0775,nofail 0 0" | tee -a /etc/fstab && mount -a
- Volume Unmount Command: umount /mnt/everyone

Windows

- Volume Mount Path: T:\
- Volume Mount Command: net use T:\\it-drive\shared
- Volume Unmount Command: net use T: /delete

Notes

- Prior to actually adding a mounted volume, SmarterMail will attempt to write/delete a file to the new mount to verify it and check things like permissions. The result of this test is displayed via toast notification.
- Only Volume Mounts added within SmarterMail will appear on this page. If a volume is mounted on the SmarterMail server directly, it is not displayed.
- There is no need to mount existing volumes that are already on the server. (You can on Windows, but not in Linux.)

Protocols

The Protocols page allows system administrators to configure various settings for every protocol used by a mail server: POP, IMAP, SMTP, LDAP and XMPP, as well as the security settings available. (I.e., TLS/SSL versions allowed.) Basically, these settings dictate how SmarterMail handles messages sent or delivered by these protocols.

- POP
- IMAP
- SMTP In
- SMTP Out
- EWS
- LDAP (Enterprise Only)
- XMPP (Enterprise Only)
- Security Protocols
- Mailbox Migration

POP

Use this card to specify the following POP settings:

- POP Banner - The text that is displayed when initially connecting to the port.
- Command Timeout (Minutes) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 5 minutes.
- Max Bad Commands - After this many unrecognized or improper commands, a connection

will be automatically terminated. By default, the maximum number of bad commands is 8.

• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 500.

• Max POP Retrieval Threads - SmarterMail is multithreaded, meaning it can do more than one thing at a time. This setting is for the maximum number of threads you want SmarterMail to work on concurrently for retrieving mail using the POP protocol. By default, the maximum number of POP retrieval threads is 10.

• POP Retrieval Interval (Minutes) - The frequency by which SmarterMail checks for new POP messages. By default, the POP retrieval interval is 1 minute.

• Disable insecure auth methods for non-SSL authentication - Enabling this will block any insecure authentication types over non-SSL connections.

IMAP

Use this card to specify the following IMAP settings:

• IMAP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:

• #HostName# : The hostname grabbed from the URL connected to by the client.

• #ConnectedIP# : The IP address of the client connecting to the mail account.

• #Time# : The current time in the server's timezone. (E.g., Thu, 06 Jan 2022 10:07:54 -07:00)

• #UnixTime# : The current server time translated to a Unix timestamp. (E.g., 1641488874)

• #TimeUTC# : The current server time translated to UTC. (E.g., Thu 06 Jan 2022 17:07:54 +0000)

• Command Timeout (Minutes) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 15 minutes.

• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.

• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• Max IMAP Retrieval Threads - The maximum number of threads you want SmarterMail to work on concurrently. By default, the maximum number of POP retrieval threads is 10.

• IMAP Retrieval Interval (Minutes) - The frequency by which SmarterMail checks for new IMAP messages. By default, the IMAP retrieval interval is 10 minutes.

• Enable IDLE Command - IMAP idle is an extension of the IMAP protocol that allows a mail server to send status updates in real time. Through IMAP IDLE, users can maintain a connection with the mail server via any mail client that supports IMAP IDLE, allowing them to be instantly aware of any changes or updates. When enabled, SmarterMail will inform any connecting IMAP client that it accepts the IDLE command. Note: IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually hinders performance.

• Disable insecure auth methods for non-SSL authentication - Enabling this will block any insecure authentication types over non-SSL connections.

SMTP In

Use this card to specify the following inbound SMTP settings:

• SMTP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:

• #HostName# - The hostname of the IP address to which the connection is made.

• #ConnectedIP# - The IP address of the remote computer.

• #Time# - The system's local time.

• #TimeUTC# - The time in UTC.

• #UnixTime# - The number of seconds since January 1, 1970.

• Allow Relay - If you are concerned about spammers using the relay function to send mail through your server, or do not want any other mail server to use your SMTP server as a gateway, set this to Nobody. Note: This is strongly recommended.

• Nobody - Restricts sent mail to only work via SMTP authentication and with accounts on the local SmarterMail Server (except for IPs on the White List).

• Only Local Users - Limits relay access to users (email accounts) for a valid domain on your SmarterMail Server.

• Only Local Domains - Limits relay access only to mail hosts (domains) on your SmarterMail Server.

• Anyone - Allows any other mail server to pass messages through your mail server, increasing the chances of your mail server being used for sending large volumes of messages with domains not associated with your local mail server. Selecting this option turns off statistics for all domains, due to the high amount of messages that are passed through the mail server with an open relay.

• Session Timeout (Minutes) - After a connection fails to respond or issue new commands for this number of minutes, the connection will be closed. By default, the session times out after 15 minutes.

• Enabled - Select this checkbox to enable the session timeout setting.

• Command Timeout (Seconds) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.

• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.

• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• Max Hop Count - After a message gets delivered through this many mail servers, it is aborted by the software. This prevents looping due to DNS problems or misconfigurations. By default, the max hop count is 20.

• Max Message Size (KB) - This controls incoming messages, and outbound messages sent via email clients configured with IMAP or POP. As such, this setting should match, if not exceed, the Max Message Size set for domains. This will help prevent email client users from having their outbound messages rejected due to the message size. By default, the max message size is 512000 KB and this number includes text, HTML, images and attachments. Note: Base64 encoding of attachments increases their size by approximately 35%. Knowing this, and in order to provide a better user experience, SmarterMail allows messages to be sent that are technically over the limit set for Max Message Size. For example, a 10MB message with a 490MB attachment will still be sent even though the actual message size, after base64 encoding, would far exceed the 500MB max limit.

• Max Bad Recipients (0 = Unlimited) - At times, spammers will hammer a domain with a dictionary harvesting attack. This means that software is used to send messages to many of the most common mailbox addresses (e.g., admin, user, contact, etc.) or username variations (e.g., alan@@, alana@@, alanb@@, etc.) in order to find valid email addresses. Setting the max bad recipients means that after this many bad recipients (those that don't exist for the domain), the SMTP session will be terminated. This setting allows you to better protect yourself against email harvesting attacks. A value of 20 is recommended in most cases.

• Append Received Line - Select the option for appending the received line for All Inbound Messages, Non-authenticated messages or for no messages at all. Note: If a message has no Received headers, SmarterMail will add one to prevent issues with some mail clients.

• Require Auth Match - Select this to force a user's From: address to match their SMTP

authenticated address, either by matching the entire email address or by matching just the domain - or not requiring it at all. This setting helps keep senders from spoofing email addresses through email clients.

• Max Messages Per Session (0 = Unlimited) - The maximum number of messages that can be sent in one session. This is useful in handling cases where spammers will make one connection and then send a large amount of messages with that connection.

• Enable VRFY command - Enable this setting to allow others (including other mail servers) to verify an email address on the server. Note: Some people believe enabling VRFY commands is a security risk, so be sure to research the possible ramifications before enabling this feature.

• Enable EXPN command - Enable this setting to allow others to list all users associated with an alias or list. Note: Some people believe enabling EXPN commands is a security risk, so be sure to research the possible ramifications before enabling this feature.

• Enable Delivery Status Notifications (DSN) - Delivery status notifications are automated messages notifying a sender about the delivery status of a message: if it bounces, if it was delayed or if delivery was successful.

• Allow relay for authenticated users - This setting enables the "Allow Relay" setting when users are required to use SMTP Authentication for sending messages.

• Enable Domain's SMTP auth setting for local deliveries - Enable this setting to enforce SMTP authentication for all local deliveries. For example, mail from user1@@example.com to user2@@example.com must be authenticated even though the message is bound for local delivery.

• Disable AUTH PLAIN method for non-SSL SMTP authentication - This setting disables plain authentication.

• Disable AUTH LOGIN method for non-SSL SMTP authentication - This setting disables plain text authentication.

• Disable CAUTH CRAM-MD5 methods for non-SSL SMTP authentication - Enabling this will block any insecure authentication types over non-SSL connections.

• Continue delivery if session is disconnected by client - When enabled, this setting allows your mail server to receive deliveries from legacy mailers, such as PHP Mailer, which do not wait for any feedback from the receiving server before disconnecting a session. This setting is disabled, by default. Note: If this setting is enabled, it is very possible the mail server will receive duplicate emails from legitimate servers that may have disconnected early as the sending server sees that as a failure, so it will continue to retry delivering its messages.

SMTP Out

Use this card to specify the following outgoing SMTP settings:

• Outbound IPv4 - The IPv4 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown along with the following:

• Use Primary IP on NIC - This will use the IP address that's assigned to the Network Interface Card (NIC) on the SmarterMail server.

• Use the Domain's IP - When a domain is set up by a system administrator, they can assign a specific IP address from the server as the "Outbound IPv4" address for that domain.

• Rotate IP List - Allows system administrators to select a number of different IP addresses that will be used, and the order in which they'll be used, to send email should connection failures or time-outs occur.

• Order - The numerical position for the specified IP address.

• IP Address - The IP address associated to the specified position.

• Rotate List Fail Ratio - The percentage of successes to failures before the IP is rotated. (In decimal format, so .5 would be 50%)

• Rotate List Fail Threshold - The total number of successes and failures before the IP is rotated. Note: Both conditions have to be true for the IPs to be rotated. So if you have a Fail List Ratio of .5 AND a List Fail Threshold of 50 successes and failures, and BOTH of those conditions are met, the IP is rotated. Otherwise, mail will continue to flow.

• Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown along with the following:

• Use Primary IP on NIC - This will use the IP address that's assigned to the Network Interface Card (NIC) on the SmarterMail server.

• Use the Domain's IP - When a domain is set up by a system administrator, they can assign a specific IP address from the server as the "Outbound IPv6" address for that domain.

• Rotate IP List - Allows system administrators to select a number of different IP addresses that will be used, and the order in which they'll be used, to send email should connection failures or time-outs occur.

• Order - The numerical position for the specified IP address.

• IP Address - The IP address associated to the specified position.

• Rotate List Fail Ratio - The percentage of successes to failures before the IP is rotated. (In decimal format, so .5 would be 50%)

• Rotate List Fail Threshold - The total number of successes and failures before the IP is rotated. Note: Both conditions have to be true for the IPs to be rotated. So if you have a Fail List Ratio of .5 AND a List Fail Threshold of 50 successes and failures, and BOTH of those conditions are

met, the IP is rotated. Otherwise, mail will continue to flow.

• Disable - This disables the use of IPv6 on the server.

• Use Primary IP if selections are unavailable - Enable this setting to have SmarterMail automatically fall back to the primary IP when a failure has occurred. SmarterMail will only attempt to connect once if this option is enabled.

• Command Timeout (Seconds) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 60 seconds.

• Max Delivery Threads - The maximum number of messages that can be sent at one time to email addresses that are not on the local server. If a message cannot be sent, the SmarterMail server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. By default, the max delivery threads is 50.

• Max Recipients Per SMTP Session - The maximum number of recipients that can be included in one SMTP session. For example, with the limit set to the default of 500, an email containing 600 recipients would utilize two SMTP sessions for delivery - one with 500 recipients and the other with 100. This setting can useful if a receiving server rejects sessions that exceed their allotted recipient limit. Note: Setting this limit to Unlimited is not recommended unless there is a specific case for doing so.

• Enable DNS Caching - Enable this setting to cache the results of DNS calls in SmarterMail. When enabled, all DNS query results are stored for a period of time determined in the configuration (time-to-live) of domain name records. This decreases the query load placed on the authoritative servers and ensures that answers to these queries are stored locally for rapid querying, thereby speeding up the delivery of messages.

• Append X-Smartermail-Authenticated-As Header - Toggling the slider to the right means that outgoing messages will have a new line item in the message header called "x-smartermail-authenticated-as" that demonstrates that the message sender was verified using SMTP authentication. This header can then be used by antispam services for validation.

• Disable Remote Bounces - This setting disables bounce messages for messages that fail to reach remote recipients. That means that when a SmarterMail user emails an external recipient (any user not on their domain) and their email fails to deliver, they will NOT receive a bounce message from the recipient's server. Note: This setting disables bounce messages for remote/external deliveries only. A SmarterMail user who sends an email to a user on the same domain will still receive a bounce message if that local delivery fails.

• Enforce strict certificate validation - This setting prevents the server from connecting to servers over SSL/TLS that have an invalid certificate For example, this prevents SSL/TLS

connections to servers with out-of-date certs or domain name mismatches on their certificate. Note: Disabling this is not recommended because it may allow a third party to setup a rogue certificate and intercept communications.

• Relaxed certificate name validation - Dependent on the enforcement of strict certificate validation, when this setting is enabled, communciation with domains that have expired certificates, self-signed certificates, or other certificates with certifying authority issues will continue to be rejected. However, issues with certificate naming will be ignored as long as the root top level domain is on the certificate. For example, when using a wildcard certificate issued for "*.domain.com", communication with domains such as "mail.domain.com", "www.mail.domain.com", "www.mail17.email.domain.com", etc. would all be allowed as long as the root certificate was NOT expired and was issued for "domain.com".

EWS

Use this card to specify the following EWS settings:

• Max EWS Retrieval Threads - The total number of threads used to process EWS requests.
• EWS Retrieval Interval (Minutes) - How often EWS requests are processed by SmarterMail.

LDAP (Enterprise Only)

This feature is only available to administrators using SmarterMail Enterprise.

Use this card to specify the following LDAP settings:

• Session Timeout (Seconds) - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 300 seconds.
• Command Timeout (Seconds) - If the server receives a command that sends large amounts of data and the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.

XMPP (Enterprise Only)

This feature is only available to administrators using SmarterMail Enterprise.

Use this card to specify the following XMPP settings:

• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

Security Protocols

SSL and TLS are security protocols that encrypt the transmission of data, allowing users to access their email without the fear that someone has intercepted their data during transit. Use this card to modify the security protocols that are allowed to connect to your mail server. Note: Prior to modifying these settings, SmarterMail must be configured for SSL or TLS connections which requires the installation of a security certificate on the server where SmarterMail is installed and the SmarterMail port(s) to be bound to the corresponding protocol(s). Please review the article, Configure SSL/TLS to Secure SmarterMail, in the SmarterTools Knowledge Base for more information.

- System Defaults - Use System Defaults to allow the operating system to choose the best protocol to use, and to block protocols that are not secure.
- SSL 3.0 - Enable this setting to allow inbound and outbound connections to your mail server over SSL 3.0. Note: Allowing connections over SSL 3.0 is not recommended. This protocol has been deprecated by the IETF and is considered to be highly insecure.
- TLS 1.0 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.0. Note: Allowing connections over TLS 1.0 is not recommended. This protocol has been deprecated by the IETF and is considered to be highly insecure.
- TLS 1.1 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.1.
- TLS 1.2 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.2. It is recommended that TLS 1.2, at the very least, is enabled.
- TLS 1.3 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.3. Allowing connections via TLS 1.3 ONLY is strongly encouraged.

Mailbox Migration

The ability to set the number of threads used when migrating a mailbox can help speed up that migration (more threads = faster processing), but it can also impact the performance of the mail server if too many threads are dedicated to migrations. This setting allows the system administrator to manage the number of threads used for migrating accounts over to SmarterMail.

Security

IDS Rules

Through the use of SmarterMail's intrusion detection system (IDS), there are several methods for preventing abuse and denial of service (DoS) attacks on your mail server. For example, IDS rules (also known as abuse detection rules) can be configured to monitor a variety of activity on the mail server,

including the number of connections coming from a single IP address, the number of messages sent within a specific timeframe, the number of login attempts and more. These rules allow SmarterMail to alert system administrators of suspicious behavior or take action to prevent the attack. Note: IDS Rules will not block local IPs. If the IP address is in one of the following formats, it will not be blocked:

- 10.*.*.*
- 172.16.*.* - 172.31.*.*
- 192.168.*.*

IDS Rules Overview

By default, SmarterMail offers several rules that are pre-configured upon installation and cover every protocol available. These rules cover the most common types of attacks against a mail server and include a Denial of Service rule, password brute force protection by email address and by IP, and password retrieval brute force protection. The following details can be seen for each entry in the list:

- Type - The type of Abuse Detection rule configured: Denial of Service (DoS), Bad SMTP Sessions (Harvesting), Internal Spammer, Password Brute Force by Protocol or Bounces Indicate Spammer.
- Action - The action to be taken when the rule is triggered.
- Time Frame - The period of time, in minutes, that is examined to determine if the rule's action should be triggered.
- Threshold - The threshold that is examined to determine if the rule's action should be triggered. For example, the number of messages sent, the number of connections made from an IP address, the number of bounce messages received, etc.
- Block Time - The time frame, in minutes, in which the IP address will be blocked. Note: If a notification email is sent, then this setting is ignored as a Block does not occur.
- Description - A friendly name or brief description of the rule.

IDS Rules

To create a new Abuse Detection rule, click the New button. When adding or editing an entry, the following configuration settings will be available, based on the Detection Type chosen:

Denial of Service (DoS)

Too many connections from a single IP address can indicate a Denial of Service (DoS) attack. Enable this option to block IPs that are connecting too often to the server. Note: It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists or make many connections if you enable this option.

• Time Frame (Minutes) - The period of time, in minutes, that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.

• Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.

• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.

• Description - A friendly name or brief description of the rule.

Password Brute Force by IP

Many times, hackers will attempt to "guess" a users' passwords by sending different variations of common passwords, to one or more users, in an attempt to log in to an account. This is considered a "brute force" attack. These requests can come from one IP address, or many.

• Time Frame (Minutes) - The period of time, in minutes, that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.

• Logins Before Block by IP - The number of login attempts before a block is placed. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.

• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.

• Description - A friendly name or brief description of the rule.

Password Brute Force by Email

A common ploy by spammers and hackers is attempting to guess passwords for a particular user, especially a "generic" account like contact@@, though it could be for an often-used public account for a particular user, like a company CEO or other executive. Many times this entails continual log in attempts to that account using different passwords, each a bit different from the one before it, thereby attempting to "brute force" the password.

• Time Frame - The period of time, in minutes, that is examined to determine if a login attempt is a brute force attempt. Too many connections in this period of time, and a block will be initiated.

• Logins Before Block by Email - The number of failed login attempts before the IP is blocked.

• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.

• Description - A friendly name or brief description of the rule.

Password Retrieval Brute Force

Another common type of attack is by spamming a "Forgot Password" link. Oftentimes, these types of password resets don't have proper security techniques in place to disallow generic email addresses from being used as a recovery address. SmarterMail, however, is "smarter", after all, so this type of attack is prone to failure. That doesn't keep spammers from trying, however. System administrators can also avoid this type of attack by either not allowing users to reset their own passwords or by using Active Directory authentication whenever possible.

- Time Frame - The period of time, in minutes, that is examined to determine if a password retrieval is a brute force attempt. Too many connections in this period of time, and a block will be initiated.
- Password Recoveries Before Block - The number of failed password recovery attempts before the IP is blocked.
- Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Bad SMTP Sessions (Harvesting)

A bad session is any connection that ends without successfully sending a message. Many bad sessions usually indicate spamming or email harvesting. Leaving all of these options set to 0 (zero) will disable this type of abuse detection. Note: It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists if you enable this option.

- Time Frame - The period of time, in minutes, that is examined to determine if an IP address should be blocked. Too many bad sessions in this period of time, and a block will be initiated.
- Bad Sessions Before Block - The number of bad sessions before a block is placed. A few bad sessions happen once in a while, for instance when a person sends an email to a user that does not exist. It is not these people that you are targeting, but rather those that are attempting to compromise or harass your customers.
- Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Internal Spammer

Enabling this rule in SmarterMail will block or quarantine a user from sending mail, as well as alert an administrator, whenever multiple emails from a single sender are delivered externally from the server during a specified time frame.

• Action - Choose whether to have a notification appear in the interface, block messages from the sender, or quarantine messages from the sender. Note: If system administrators prefer to have an email sent, a System Event should be created (Security category → IDS Rule Triggered event type.

• Time Frame - The period of time, in minutes, that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.

• Messages Before Notify - After this many messages are delivered within the time period specified, the email notification is sent and the Action chosen is performed.

• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold. Note: If a notification email is sent, then this setting is ignored as a Block does not occur.

• Notify Email - The email address of the administrator to which the notification will be sent.

• Description - A friendly name or brief description of the rule.

Bounces Indicate Spammer

Enabling this rule in SmarterMail will block or quarantine a user from sending out mail, as well as alert an administrator, after receiving a certain number of bounce messages in the specified time frame.

• Action - Choose whether to have a notification appear in the interface, block messages from the sender, or quarantine messages from the sender. Note: If system administrators prefer to have an email sent, a System Event should be created (Security category → IDS Rule Triggered event type.

• Time Frame - The period of time, in minutes, that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.

• Bounce Threshold - After this many bounce messages are received within the time period specified, the email notification is sent and the Action chosen is performed.

• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold. Note: If a notification email is sent, then this setting is ignored as a Block does not occur.

• Notify Email - The email address of the administrator to which the notification will be sent.

• Description - A friendly name or brief description of the rule.

Resetting IDS Rules to Their Defaults

If, for whatever reason, your rules get out of whack or you feel they need to be re-configured, it's easy to reset them back to their "factory defaults". Simply select Reset IDS Rules from the Actions (□)

dropdown. When you do, all existing rules are replaced with the default configuration that's available upon fresh installation of SmarterMail. It's then possible to start re-configuring as needed.

Importing/Exporting Settings

One of the primary reasons SmarterMail is so popular is that it's very easy for a system administrator to manage. Not only is SmarterMail's administration all web-based, many of the functions available for administrators can be exported from one machine and imported into another SmarterMail installation. This makes it easy for administrators to have a consistent set of security settings, antispam settings, and more across all of the SmarterMail servers in use. The options for importing or exporting IDS rules are available from the Actions (□) dropdown.

When exporting your rules, the settings are saved as a JSON file to the location specified in File Explorer. When importing files, a modal window opens and the corresponding JSON file can be dragged-and-dropped right in the modal or the file can be selected using File Explorer.

Blacklist / Whitelist

System administrators are able to control the IP addresses that are blacklisted from accessing, or whitelisted for access to, mail services. Blacklisting an IP address prevents it from making inbound connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed, including spam filtering, greylisting and IDS rules. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own. Note: Internal IP addresses are whitelisted by default. If this is a concern, system administrators can edit these whitelist entries to disable whitelisting for one or more protocols or bypasses. However, internal IP addresses cannot be deleted.

By default, both of these tabs will be empty as SmarterMail has no way of knowing the IPs or IP Ranges that need to be blocked or granted access to its various services. However, once entries are added, the following details can be seen on both tabs:

- Source - The domain name or IP address that's black/whitelisted.
- Country - The country associated with the IP address.
- Description - The friendly name giving to the Source or reason for the blacklist.
- Webmail - Whether the black/whitelist is enabled for this protocol.
- EAS - Whether the black/whitelist is enabled for this protocol.
- IMAP - Whether the black/whitelist is enabled for this protocol.
- LDAP - Whether the black/whitelist is enabled for this protocol.
- MAPI & EWS - Whether the black/whitelist is enabled for this protocol.
- POP - Whether the black/whitelist is enabled for this protocol.

- SMTP - Whether the black/whitelist is enabled for this protocol.
- WebDAV - Whether the black/whitelist is enabled for this protocol.
- XMPP - Whether the black/whitelist is enabled for this protocol.

However, the following columns are only seen on the Whitelist tab.

• IP Bypass - For whitelists only, allows a system administrator to prevent spam checks and greylisting on email delivered from specific IP addresses.

• SMTP Auth Bypass - For whitelists only, whether SMTP Authentication is bypassed for the entry.

• IDS Brute Force - For whitelists only, whether the IDS Brute Force rules (including Password Brute Force by IP, Password Brute Force by Email, and Password Retrieval Brute Force) are bypassed for this entry.

• Bypass Spam Checks - For whitelists only, whether SMTP spam checks are bypassed for the entry.

• Bypass Greylisting

Adding a new Blacklist

To create a new entry in the blacklist, click New . When adding or editing an entry, the following options will be available:

- IP Addresses (single, range or CIDR block) - When listing an IP address, enter a single IP address or an IP range in dotted quad notation. (E.g., 123.45.678.90, or 12.345.67.0/24). If an IP range is entered, all IP addresses within that range will be contained in the list.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"
- Protocol(s) - Enable the protocol(s) you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP.

Be sure to click Save to add the entry.

Adding new Whitelist

To create a new entry in the blacklist or whitelist, click New . When adding or editing an entry, the following options will be available:

- Source - Whether the whitelist will be for a domain or an IP address or range.
- Domain Name - When Domain Name is the Source, this is the domain name to whitelist.
- IP Addresses (single, range or CIDR block) - When listing an IP address, enter a single IP address or an IP range in dotted quad notation. (E.g., 123.45.678.90, or 12.345.67.0/24). If an IP range is entered, all IP addresses within that range will be contained in the list.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"

    • Bypass IP for Spam Checks - When using a gateway, this will bypass spam checks for messages passed through the gateway.

    • Bypass SMTP Authentication - Used for whitelists only, enabling this bypasses the need for SMTP authentication for whitelisted IPs or domains.

    • Bypass IDS Brute Force - Used for whitelists only, enabling this bypasses IDS Brute Force checks for whitelisted IPs.

    • Bypass Spam Checks Important Note: If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses and IP bypasses. Because anyone can write any return path that they want when sending a message, this extra check helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender.

    • Bypass Greylisting - Used for whitelists only, enabling this bypasses greylisting for whitelisted IPs.

    • Protocol(s) - Enable the protocol(s) you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP. Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the system administrator may want to review the settings prior to adding the IP range.

SMTP Auth Bypass

Whitelisted IP addresses can bypass SMTP authentication, which is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server. Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are websites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's Whitelist and enable SMTP Authentication Bypass. Whitelist entries with SMTP Auth Bypass enabled will not be asked to provide an SMTP Authentication login.

Importing/Exporting Settings

One of the primary reasons SmarterMail is so popular is that it's very easy for a system administrator to manage. Not only is SmarterMail's administration all web-based, many of the functions available for administrators can be exported from one machine and imported into another SmarterMail installation. This makes it easy for administrators to have a consistent set of security settings, antispam settings and more across all of the SmarterMail servers in use.

To import or export settings, simply click the Actions (☐) button and select either option. When exporting, the settings are saved as a JSON file to the location specified in File Explorer. When importing files, a modal window opens and the corresponding JSON file can be dragged-and-dropped right in the modal or the file can be selected using File Explorer.

Blacklist / Whitelist

System administrators are able to control the IP addresses that are blacklisted from accessing, or whitelisted for access to, mail services. Blacklisting an IP address prevents it from making inbound connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed, including spam filtering, greylisting and IDS rules. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own. Note: Internal IP addresses are whitelisted by default. If this is a concern, system administrators can edit these whitelist entries to disable whitelisting for one or more protocols or bypasses. However, internal IP addresses cannot be deleted.

By default, both of these tabs will be empty as SmarterMail has no way of knowing the IPs or IP Ranges that need to be blocked or granted access to its various services. However, once entries are added, the following details can be seen on both tabs:

> • Source - The domain name or IP address that's black/whitelisted.
> • Country - The country associated with the IP address.
> • Description - The friendly name giving to the Source or reason for the blacklist.
> • Webmail - Whether the black/whitelist is enabled for this protocol.
> • EAS - Whether the black/whitelist is enabled for this protocol.
> • IMAP - Whether the black/whitelist is enabled for this protocol.
> • LDAP - Whether the black/whitelist is enabled for this protocol.
> • MAPI & EWS - Whether the black/whitelist is enabled for this protocol.
> • POP - Whether the black/whitelist is enabled for this protocol.
> • SMTP - Whether the black/whitelist is enabled for this protocol.
> • WebDAV - Whether the black/whitelist is enabled for this protocol.
> • XMPP - Whether the black/whitelist is enabled for this protocol.

However, the following columns are only seen on the Whitelist tab.

• IP Bypass - For whitelists only, allows a system administrator to prevent spam checks and greylisting on email delivered from specific IP addresses.

• SMTP Auth Bypass - For whitelists only, whether SMTP Authentication is bypassed for the entry.

• IDS Brute Force - For whitelists only, whether the IDS Brute Force rules (including Password Brute Force by IP, Password Brute Force by Email, and Password Retrieval Brute Force) are bypassed for

this entry.

• Bypass Spam Checks - For whitelists only, whether SMTP spam checks are bypassed for the entry.

• Bypass Greylisting

Adding a new Blacklist

To create a new entry in the blacklist, click New . When adding or editing an entry, the following options will be available:

    • IP Addresses (single, range or CIDR block) - When listing an IP address, enter a single IP address or an IP range in dotted quad notation. (E.g., 123.45.678.90, or 12.345.67.0/24). If an IP range is entered, all IP addresses within that range will be contained in the list.

    • Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"

    • Protocol(s) - Enable the protocol(s) you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP.

Be sure to click Save to add the entry.

Adding new Whitelist

To create a new entry in the blacklist or whitelist, click New . When adding or editing an entry, the following options will be available:

    • Source - Whether the whitelist will be for a domain or an IP address or range.

    • Domain Name - When Domain Name is the Source, this is the domain name to whitelist.

    • IP Addresses (single, range or CIDR block) - When listing an IP address, enter a single IP address or an IP range in dotted quad notation. (E.g., 123.45.678.90, or 12.345.67.0/24). If an IP range is entered, all IP addresses within that range will be contained in the list.

    • Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"

    • Bypass IP for Spam Checks - When using a gateway, this will bypass spam checks for messages passed through the gateway.

    • Bypass SMTP Authentication - Used for whitelists only, enabling this bypasses the need for SMTP authentication for whitelisted IPs or domains.

    • Bypass IDS Brute Force - Used for whitelists only, enabling this bypasses IDS Brute Force checks for whitelisted IPs.

    • Bypass Spam Checks Important Note: If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses and IP bypasses. Because anyone can write any return path that they want when sending a message, this extra check helps prevent spammers from flooding users

with hundreds of messages that aren't truly from a trusted sender.

• Bypass Greylisting - Used for whitelists only, enabling this bypasses greylisting for whitelisted IPs.

• Protocol(s) - Enable the protocol(s) you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP. Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the system administrator may want to review the settings prior to adding the IP range.

SMTP Auth Bypass

Whitelisted IP addresses can bypass SMTP authentication, which is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server. Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are websites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's Whitelist and enable SMTP Authentication Bypass. Whitelist entries with SMTP Auth Bypass enabled will not be asked to provide an SMTP Authentication login.

Importing/Exporting Settings

One of the primary reasons SmarterMail is so popular is that it's very easy for a system administrator to manage. Not only is SmarterMail's administration all web-based, many of the functions available for administrators can be exported from one machine and imported into another SmarterMail installation. This makes it easy for administrators to have a consistent set of security settings, antispam settings and more across all of the SmarterMail servers in use.

To import or export settings, simply click the Actions (□) button and select either option. When exporting, the settings are saved as a JSON file to the location specified in File Explorer. When importing files, a modal window opens and the corresponding JSON file can be dragged-and-dropped right in the modal or the file can be selected using File Explorer.

SMTP Blocks

SMTP Blocks are an effective method for temporarily preventing a domain or individual user from sending email from the server. For example, if a particular user is sending an abnormal amount of email, you can add their address to the SMTP Blocks list and they will be unable to send email until

you remove them. Users and/or domains can be left on the list for whatever time you deem appropriate. This action can be an effective stop-gap versus actually deleting the user and/or domain from the server, giving users or domain administrators the ability to clean up their act before having their mail server privileges revoked. Note: SMTP Blocks are enabled against a message's Return Path versus using the FROM address because the Return Path is generally more difficult to spoof than simply the FROM: address.

By default, this tab will be empty. However, once entries are added, the following details can be seen for each:

- Address - The email address being blocked.
- Type - The type of block: Email Address / Domain or EHLO Domain.
- Direction - Whether the block is for inbound, outbound, or all messages.
- Description - The description given to the block.

EHLO Domain vs Email Address / Domain Block Types

An "EHLO domain" is the return value given when a mail server sends the EHLO/HELO command. (SmarterMail treats both equally.) A standard EHLO domain is the fully qualified domain name set up for the mail server. (E.g., "mail.your_domain.com".) However, it IS possible that it will be something different based on whether the command is sent through the mail server's web interface or an email client. For example, it may be the local IP address of the sending machine. Therefore, there is no well-established rule for what should be entered for an EHLO block until some testing is done by the system administrator. An email address / domain block is just that: a flat block on the address or domain that's listed. Note: SMTP blocking does NOT occur immediately when the EHLO command is given. Instead, a "soft" block is used and SmarterMail will fail any authentication attempts or RCPT TO commands. This is because if the failure occurs right after the EHLO command, any person attempting to spam from a mail server could figure out what the problem is and change the domain given with the command on each send. A "soft" failure should, instead, make the spammer believe he is using an incorrect password.

Adding a New Block

To create a new block, click on New . When adding or editing an entry, the following configuration settings will be available, based on the Block Type chosen:

- Block Type - Whether the block affects an email address or an entire domain, or an EHLO domain.
- Blocked Address - The complete email address of the user, the domain name or the value used for the EHLO domain.
- Direction - For user/domain (non-EHLO domain) blocks, this refers to the types of messages

that should be blocked from sending: Inbound, Outbound or All Messages.

• Description - A friendly name or brief description of the block.

Importing/Exporting Settings

One of the primary reasons SmarterMail is so popular is that it's very easy for a system administrator to manage. Not only is SmarterMail's administration all web-based, many of the functions available for administrators can be exported from one machine and imported into another SmarterMail installation. This makes it easy for administrators to have a consistent set of security settings, antispam settings and more across all of the SmarterMail servers in use.

To import or export settings, simply click the Actions (□) button and select either option. When exporting, the settings are saved as a JSON file to the location specified in File Explorer. When importing files, a modal window opens and the corresponding JSON file can be dragged-and-dropped right in the modal or the file can be selected using File Explorer.

SSL Certificates

SmarterMail gives system administrators the ability to manage the SSL certs assigned to various domains that are being hosted by SmarterMail by navigating to Settings → SSL Certificates .

Certificates can be acquired from any qualified Certifying Authority (e.g., Digicert) then manually added to a SmarterMail domain. In cases like this, where administrators acquire SSL certs outside of SmarterMail, those certificates are displayed on the Certificates tab.

Certificates can also be automatically generated by SmarterMail using the included Certifying Authority(-ies), such as Let's Encrypt. This is, by far, the simplest way to manage SSL for SmarterMail domains as it's all contained within SmarterMail. Automated certificates can be found on the Automatic Certificates tab.

Note: In order to use SmarterMail's automatic certificates, a few things need to be understood:

• Hostnames must be pointed at the SmarterMail server using an A record in DNS.

• Hostnames must be routable, top level domains. (I.e., not local domains, etc.)

• HTTP binding must be present in IIS and configured to land on the SmarterMail web interface.

• nothing can intercept HTTP requests on any hostname. This includes having something like Ceritfy the Web/Let's Encrypt installation or proxy. If these are installed or proxied, they must be removed prior to using SmarterMail's automatic certificates.

When accessing SSL Certificates, the following tabs are available, and each tab has its own cards/details:

- Options
- Certificates
- Automatic Certificates

Regarding Port Bindings

When adding or modifying ports (on the Ports tab over at Settings > Bindings), one thing asked for is an Encryption type. If SSL or TLS is selected, SmarterMail asks for a Certificate Path and Password . Even when using this page to manage SSL Certificates, those fields are still required. This is because some clients do NOT support SNI. For this reason an administrator will need to add a certificate to act as a fallback to each SSL/TLS Port binding in order for SmarterMail to listen for TLS connections. It can be the same certificate for each port, however.

Options

The Options area contains the following cards:

Options

This card consists of basic options for SSL Certificates. These include:

- Certificate Folder Path - This is the path on the server where SmarterMail SSL certificates are stored. By default, this is c:\SmarterMail\Certificates.
- Certificate Password (if any) - The password used to encrypt the certificate store folder to add additional at-rest security, or the password associated to any existing certificates that are added to the certificates folder that the system administrator wants SmarterMail to read. Note: This password should match the one configured in the centralized certificate store in IIS. If a password is not necessary, this can be left blank.
- Enable Automatic Certificates - This toggle will enable SmarterMail to generate SSL certificates automatically for domains that are added. Enabling this will display the cards detailed below.

Automatic Certificates

When automatic certificates are enabled, it's up to the system administrator to not only select the certificate provider, but also make/edit some existing settings to ensure certificates are issued properly.

- Certificate Authority - The company issuing the SSL certificate.
- Email Address for Certificate Notifications - Most certifying authorities require an email address for any notifications regarding certificates. This can be a generic address.
- Hostname prefixes (one per line) - These are the prefixes covered by the issued SSL certificate. By default, "autodiscover", "mail" and "webmail" are provided. If other prefixes are

used, such as "POP" or "SMTP", they will need to be added manually. Note: If a prefix is listed, but is not used, it will not be sent to the Certifying Authority.

• Terms of Service - A link is provided to the terms of service of the Certificate Authority that's selected.

Certificate CSR

When certificates are issued, they're issued to a particular organization. This section lists the organizational information requested for the Certifying Authority. We default some information, but it can be edited as needed.

• Organization - The name of the organization requesting the certificate.

• Organization Unit - The particular unit/department within the Organization requesting the certificate. (This can match the Organization.)

• City - The city that corresponds to the Organization.

• State / Province - The state or province that corresponds to the Organization.

• Country - The country that corresponds to the Organization.

Certificates

This tab lists any certificates that reside in SmarterMail's Certificates Folder that were NOT automatically generated by SmarterMail. These are generally pre-existing certs that were already in the cerfiicates folder or that were placed there after being manually generated or generated outside of SmarterMail. Each certificate is displayed with the following information:

• File Name - The actual file name of the certificate.

• Hostnames - The hostname(s) associated to the certificate.

• Expires - The expiration date of the certificate.

• Renews - The renewal date of the certificate, which is generally 30 days prior to the Expires date.

• Status - Generally, this will display Active if the SSL certificate is being read successfully by SmarterMail. However, another status may be listed. For example, the certificate is invalid due to an incorrect password or if one or more hostname(s) associated to the certificate aren't able to be reached via the internet. Note: Any certificate added or uploaded to the Certificates Folder MUST be a .PFX file type.

Uploading Certificates

On the Certificates tab, it's possible to add new certificates to SmarterMail simply using the Upload button. Note: Only .PFX files can be uploaded.

- Click the Upload button, and a modal will open.
- Use the Choose File button to find, and select, the .PFX file you want to upload.
- Add the password associated to the file, if one was added. If you get an error, you can try leaving this field blank.
- Click the Next button. Ideally, you'll get the message that "Your certificate has been verified. The certificate can be used for the hostnames below:" and you'll see your hostname and the expiration date of your certificate. If errors occur, they will be displayed instead, so you can troubleshoot the issue.

Alternatively, you can manually drop .PFX files into SmarterMail's Certificates folder and they will appear on the Certificates tab. If you have your own cert generation app (certbot, certifytheweb, etc.), you can configure it to export to SmarterMail's Certificates folder and SmarterMail should immediately pick up the new certs as long as you use a consistent (or no) password on them.

Removing Certificates

In order to remove a certificate (either custom certificates or automated certificates), once the domain(s) served by the certificate are handled as necessary, a system administrator simply needs to remove the associated .PFX file from the Certificates folder. (By default, C:\SmarterMail\Certificates) Once that's done, SmarterMail will update the certificates list and that certificate will no longer be present.

Automatic Certificates

This tab lists the certificates that have been automatically generated by SmarterMail using the Certifying Authority selected on the Options tab. Similar to the Certificates tab, some information is available on the page, including:

- Hostnames - The hostname(s) associated to the certificate.
- Expires - The expiration date of the certificate.
- Renews - The renewal date of the certificate, which is generally 30 days prior to the Expires date.
- Status - Generally, this will display Active if the SSL certificate is being read successfully by SmarterMail. However, another status may be listed. For example, the certificate is invalid due to an incorrect password or if one or more hostname(s) associated to the certificate aren't able to be reached via the internet.

Status Codes

The status of various certificates can be varied, depending on whether the cert is Active or if there are

issues. SmarterTools makes the status codes as verbose as possible so you know exactly what an issue is. Below are the various short and long descriptions (where applicable) for each:

- Disabled — The certificate was disabled by a system administrator.
- Active — Certificate was generated and is working properly.
- Certificate was generated but has binding errors — Certificate was generated but could not be bound to the web interface.
- Certificate has been deactivated — Certificate has been deactivated. Please generate a new one.
- Certificate has expired — Certificate has expired. Please generate a new one.
- Domain validation has failed — Domain validation has failed. Please ensure that the hostname is accessible through HTTP from the internet.
- Inaccessible through HTTP — The hostname for this site is not bound to this SmarterMail instance when navigating to it through HTTP. This is necessary to verify ownership for the certificate.
- Domain validation is pending — Domain validation is pending. This may take a few minutes.
- Certificate has been revoked — Certificate has been revoked. Please generate a new one.
- Generating certificate — Domain validation has completed and your certificate will be generated shortly.
- Certificate has no private key
- Invalid Password — Certificate cannot be loaded with password provided
- Certificate file cannot be loaded

If there are issues binding the cert to IIS, the following status is displayed:

- Another site is already bound to the same hostname, so SmarterMail cannot automatically add the binding.
- Automatic binding is not supported on this server operating system.
- An error occurred applying the website binding. Refer to the administrative log file for more information.
- Cannot find the website that is bound to your MRS folder.
- Cannot find the MRS folder in your installation path.

System Messages

SmarterMail sends a variety of automated email messages for certain actions within SmarterMail. For example, system messages are sent to users when their password has expired or is in violation of the password policies set up for their domain. Administrators can modify certain messages sent out from the server to make them match a company's voice and style, add extra information or add a standard

From address. If a system message does not have a From address, the system message will appear to come from "noreply@@" the SmarterMail domain that made the request. For example, if a password reset request is made for a user on example.com, and there's no From address set for the system password reset request message, the user will receive that reset email from "noreply@@example.com". Note: if the domain already has a "noreply@@" account, alias or mailing list set up, they are not affected by this functionality.

When accessing System Messages , a list of the current system messages will be displayed along with the following:

- Message - This is the message's title/type.
- Language - The language used for the message.
- Subject - The messages subject. This is what appears in the Subject line of the sent message.

Click on a message's row to edit the text. The following settings will be available:

- Message Title - This is not editable, but it displays the message's title and language. (E.g., Delivery Status Failure - English)
- Subject - The subject of the email. In some cases, the subject will contain system variables. It's a good idea to leave these variables "as-is" in the subject.
- Message Body - The message body of the email.
- From Address - Administrators can add a From address to allow users to respond to system messages or to decrease the likelihood a message will be caught by spam filters. If no address is entered, messages are sent from "noreply@@" the SmarterMail domain that made the request.
- Display Name - The friendly name or description of the sender that will appear in conjunction with the From address (if included) in the From field of the email.

Creating a System Message in a New Language

System administrators have the ability to create new versions of the default system messages in a different language. How those messages get used is as follows:

For Delivery Status messages, the language used is determined as follows:

- Try to find a matching message based on the language in the default user settings for the domain of the recipient of the original message. For example, if user1@@domain1.com sent a message to user2@@domain2.com, a Delivery Status message sent back to user1@@domain1.com would use the language configured for user2@@domain2.com.
- If no message has been found matching the recipient's language, SmarterMail will try to find a matching message in English.

For all other messages, the language is determined by these criteria:

- Try to find a matching message based on the user's language.
- If no message has been found, try to find a matching message based on the language for the domain's default user settings.
- If no message has been found, try to find a matching message in English.

To create a new, default system message in another language, do the following:

- Click the New button in the content pane. A modal opens.
- Select the Message Type . That is, select a default system message you want to recreate in a new language.
- Select the Language for the new system message.
- Click the Save button. The new message window appears in the content pane. Here, you add in your Subject the message contents and set the From Address and Friendly Name .
- Once all has been filled out, click the Save button to save the new message.

Deleting System Messages

Any new system messages that are created in other languages can be deleted as needed. Simply click on the box next to the message, then click the Delete button. Multiple messages can be deleted by selecting multiple boxes. Note: To ensure that there is always a defined message for each message type, English messages cannot be deleted.

Additional Help Topics

Automating Login to SmarterMail

Companies using SmarterMail can easily automate user entry into the mail application by configuring auto-login functionality and the SmarterMail API. The code samples (Python and PHP) shown below demonstrate how you can make a text link or button on a website (e.g. "Log into your mail") that automatically logs a user in to the SmarterMail site. This implementation of auto-login works seamlessly across domains, so the two applications do not have to be hosted on the same server. (Though the code should run on the SmarterMail server.)

Some notes about the example code listed below: Important: Code provided is for informational purposes only. It is not guaranteed to work, especially without input by a seasoned or knowledgeable programmer. In addition, if other languages are required, the provided code can be used as a guideline. However, SmarterTools will not generate sample code in other languages. Finally, autoLoginTokens are one-time use and only last 10 minutes.

We have the form values set to generic text (e.g. "domain@example.com") to show where you would hard coded values that are submitted to the login page. You could also dynamically generate these values using a scripting language like .NET, PHP, or any other. You'd simply substitute hard coded values using variables generated by your code.

The serverEndpoint, https://mail.example.com , uses the default hostname of the SmarterMail web interface. If you have created a separate website for SmarterMail or if you assign a different IP address for SmarterMail within IIS, this action would have to be altered to reflect this change. In addition, this code assumes that your SmarterMail site is secured with SSL/TLS, which it should be.

Auto-Login Sample Python Code

```
import requests # run 'pip install requests' to get this # All the code
here should be happening SERVER SIDE # Once you have 'autoLoginUrl' you can
render an html page with a button or redirect the user to this URL. #
Python requires proper formatting in order to run without error. This code
sample may not be formatted properly. serverEndpoint =
"https://mail.example.com" userEmail = "domain@example.com" systemAdminUser
= "admin" systemAdminPass = "admin" def handle_response_error"("prefix,
response): # Checks if the response indicates success; prints message and
exits if not. if not response.status_code == 200: print(f"Error: [{prefix}]
Received status code {response.status_code}") return True data =
response.json() if not data.get('success', True): # Assuming 'success' key
indicates success status print(f"Error: [{prefix}] {data.get('message',
```

```
'Unknown error')}") return True return False # STEP 1: Login to System
Admin login_response =
requests.post(f"{serverEndpoint}/api/v1/auth/authenticate-user", json={
"username": systemAdminUser, "password": systemAdminPass },
headers={'Content-Type': 'application/json'}) if
handle_response_error("SystemAdminLogin", login_response): exit(1) # Exits
if there was an error login_response_data = login_response.json()
accessToken = login_response_data['accessToken'] # Splitting user and
domain from email user, domain = userEmail.split("@") # STEP 2: Make a
login token login_token_response =
requests.post(f"{serverEndpoint}/api/v1/auth/retrieve-login-token", json={
"username": user, "domain": domain }, headers={ 'Content-Type':
'application/json', 'Authorization': f'Bearer {accessToken}' }) if
handle_response_error("RetrieveLoginToken", login_token_response): exit(1)
# Exits if there was an error login_token_data =
login_token_response.json() autoLoginUrl = login_token_data['autoLoginUrl']
# For demonstration purposes, printing the auto login URL print("Auto Login
URL:", autoLoginUrl)
```

Auto-Login Sample PHP Code

```
<?php $serverEndpoint = "https://mail.example.com"; $userEmail =
"domain@example.com"; $systemAdminUser = "admin"; $systemAdminPass =
"admin"; function handle_response_error($prefix, $response) { if
($response['statusCode'] != 200) { echo "Error: [$prefix] Received status
code " . $response['statusCode'] . "\n"; return true; } $data =
$response['data']; if (isset($data->success) && !$data->success) { //
Assuming 'success' key indicates success status echo "Error: [$prefix] " .
($data->message ?? 'Unknown error') . "\n"; return true; } return false; }
function make_request($url, $payload, $headers) { $ch = curl_init($url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true); curl_setopt($ch,
CURLOPT_HTTPHEADER, $headers); curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($payload)); $response =
curl_exec($ch); $statusCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
curl_close($ch); return [ 'data' => json_decode($response), 'statusCode' =>
$statusCode ]; } // STEP 1: Login to System Admin $loginResponse =
make_request("$serverEndpoint/api/v1/auth/authenticate-user", [ "username"
=> $systemAdminUser, "password" => $systemAdminPass ], ['Content-Type:
application/json']); if (handle_response_error("SystemAdminLogin",
$loginResponse)) { exit(1); // Exits if there was an error } $accessToken =
$loginResponse['data']->accessToken; // Splitting user and domain from
email list($user, $domain) = explode("@", $userEmail); // STEP 2: Make a
```

```
login token $loginTokenResponse =
make_request("$serverEndpoint/api/v1/auth/retrieve-login-token", [
"username" => $user, "domain" => $domain ], [ 'Content-Type:
application/json', 'Authorization: Bearer ' . $accessToken ]); if
(handle_response_error("RetrieveLoginToken", $loginTokenResponse)) {
exit(1); // Exits if there was an error } $autoLoginUrl =
$loginTokenResponse['data']->autoLoginUrl; // For demonstration purposes,
printing the auto login URL echo "Auto Login URL: " . $autoLoginUrl . "\n";
?>
```

Backup MX Servers

A Backup MX Server is a mail server that will store (spool) your incoming email if your primary mail server becomes unavailable. A mail server can become unavailable to receive incoming mail for a number of reasons.

For example:

- Hardware or software failure
- Very busy and unable to receive new incoming connections, or emails
- Network connection is down or saturated
- Network routing issues can also cause your mail server to become unavailable

Case 1 - No Backup MX

If you do not have a Backup MX Server, the following conditions may occur:

- Email will be bounced (Returned to Sender).
- Your (inbound) email will cause a backup in the originating mail server's spool.
- Service Timeout. Depending on the Retry attempts by the originating mail server, your mailboxes may never receive their incoming email.
- Users do not understand bounce messages. To most users, bounce messages are unreadable, so when they can't send an email, they do not try to resend.

Case 2 - With a Backup MX

How Email works when a Backup MX Server is involved:

- User sends an email to 'user@@example.com' (a mailbox hosted by your SmarterMail Server)
- Their mail server looks up the MX Records for 'example.com' and finds two:

- IP: x.x.x.x Weight: 10
- IP: y.y.y.y Weight: 20

• Their mail server first attempts to connect to: x.x.x.x

• Connection fails, which could be caused by any of the above conditions

• They try to connect to the secondary MX record: y.y.y.y

• They successfully connect to this server.

• Email transmission begins, and the Backup MX Server receives the email into its spool.

• Since there are no existing local domains on this server, SmarterMail stores this email in its spool.

• Based off of the Retry Attempts, SmarterMail will continue to try and make connections to your Primary Mail Server.

• SmarterMail will only make 4 retry attempts. It is recommended that you set the last attempt to a longer timeframe, i.e., 24 hours (1440 minutes)

• This way SmarterMail does not send a Bounce Message to the originator saying that it could not deliver the message, before your Primary Server is back online.

• If your Primary Mail Server comes back online before the final Retry Attempt, you can reset the Retry Counts on all messages in the spool. This will force the Backup MX Server to try forwarding all existing mail in the spool back to your Primary Mail Server.

Configuring SmarterMail as a Backup MX Server

In the event that the primary mail server goes down, system administrators can set up SmarterMail to function as a backup MX server to ensure users continue to receive incoming email messages. When the primary mail server cannot be contacted, email servers on the web will attempt delivery to the backup MX server. When the primary server comes back online, the backup MX server will deliver all held email.

Set up of the primary mail server

Follow these steps on the primary email server to ensure that it's listening on the appropriate IP address(es):

• Go to Bindings .

• Click on the Ports tab. A list of ports will load in the content pane. By default, ports 110, 143 and 25 are already set up. If necessary, add any alternative ports you may need SmarterMail to listen on by clicking the New button.

• Click on the IP Addresses tab. A list of IP addresses will load in the content pane.

• Click into each IP address you wish to listen on, and place a check in the box for the appropriate port. Click Save . Your server is now set up to listen on the selected ports for the IPs they have been added to. Note: You can only edit one IP address at a time.

• Click on Security from the navigation pane on the left.

- Click on the Whitelist tab.

- Click New .

- Enter the IP address of your backup MX server.

- Adjust the Gateway and Security options as necessary. Note: If "Bypass IP for Spam Checks"" AND "Bypass Spam Checks"" are both enabled, Bypass Spam Checks will take priority, preventing any spam checks from happening at all.

- Click Save .

Set up the Backup MX server

On the SmarterMail installation that will be configured as your backup MX server, follow these steps to get the backup MX set up:

- Go to Gateways / Failover .
- Click on the Incoming tab.
- Click New .
- In the Gateway Mode field, select Backup MX from the list.
- Type the IP address or IP range in the appropriate field for the mail server you're creating the backup MX for. (Typically, this is your primary mail server IP or IP range, which was set up above.)
- Adjust the SmarterMail Gateway and Spam settings as necessary. (Enable the SmarterMail gateway mode if the primary mail server is a SmarterMail installation, as this setting is what allows you to enable User Verification, which will ensure the user exists before the backup MX server attempts to deliver mail for that user back to the primary.)
- Click Save .
- Click on General in the navigation pane to the left.
- On the Spool card and change the Retry Intervals setting to 10, 10, 10, 1440.
- Click Save .
- In your primary DNS configuration — whether it's managed locally or via your web host or DNS provider — add secondary MX records that point to the new server's IP address. Be sure to set the preference value higher than the main MX record.

Locking Down Your Server

Security is an ever-growing concern to business small and large. Because email servers are constantly under attack, SmarterMail has many features built into it to protect you. This topic explains steps you can take to protect yourself, your users, and your investment.

What is Security for a Mail Server?

The word security has many meanings. SmarterTools' opinion is that mail server security is comprised of several types of protection:

- Protecting your data
- Protecting your users
- Protecting your service availability
- Protecting others on the internet

Below are some "Best Practices" for maintaining a locked-down server, one that can withstand the constant abuse that mail servers are subject to.

- Update SmarterMail regularly
- Disable catch-all accounts
- Restrict bounces and auto-responders
- Require SMTP authentication Enable abuse detection
- Avoid unnecessary whitelists
- Enable SMTP blocking -->

Update SmarterMail Regularly

SmarterTools is constantly working to improve SmarterMail and make it even more resistant to attacks. It is recommended that you keep your copy of SmarterMail up to date in order to stay protected.

Releases are announced via a system event that displays a notification within SmarterMail when a new version is available. In addition, we occasionally update customers via our social media pages and/or via email.

Disable Catch-All Accounts

Catch-all accounts were popular in the past because of the flexibility they offer to a domain administrator. All an administrator had to do was add a catch-all account, and any mail that was misdelivered would drop right into his mailbox. When catch-alls were most popular, spamming methods were not as sophisticated, and email harvesting attacks were not so prevalent.

Today, however, mail servers get attacked every minute of every day. Spammers assault email domains with thousands of spam messages sent to different users in the hope that they will strike a hit to verify that the email account exists and to deliver another spam email.

In addition, if the catch-all user has an auto-responder enabled, the problem can be doubly harmful. Spammers rarely use their real email address, so if your user auto-responds to each of the thousands of

messages above, and they happen to go to a large email provider, you will likely end up getting blacklisted as a spammer yourself.

As you can see, allowing the use of catch-alls exposes you to many types of abuse. SmarterMail allows catch-alls because it is expected in a mail server, but to lock down your server, we recommend the following procedure that will disable catch-alls:

- Alert your users that catch-alls are being disabled.
- Select the domain you want to edit.
- Click on the Configuration tab.
- Disable Catch-All Alias on the domain's Features card.
- Click Save .

Restrict Bounces and Autoresponders

Email Bouncing occurs when delivery failures occur or a mailbox is full. A brief explanation of the error is sent back to the original sender of the message. Before spam became such a problem, this was usually not an issue. Today, however, spammers will sometimes spoof known spam trap accounts at places like SpamCop as the sender of the message. Thus, when your mail server bounces the message, the bounce ends up in the spam trap. Enough of these, and you'll be blacklisted.

The exact same is true for autoresponders that reply back to spoofed spam email.

SmarterMail allows you to restrict bounces and autoresponders to only those accounts that pass SPF checks, or to disable them entirely. SPF verifies that an email is not spoofed, and most of the serious spam trap accounts out there have SPF set up. To require SPF for bounces and autoresponders, do the following:

- First, alert your users of the new policies being put into place. Then you can make the necessary changes.
- Go to Antispam in the navigation pane and then the Options tab.
- Change Autoresponders to either Disabled or Require message pass SPF .
- Change Content Filter Bouncing to either Disabled or Require message pass SPF .
- Click Save in the content pane toolbar.

Require SMTP Authentication

SMTP Authentication is an unspoken requirement of domains on modern mail servers. Any domain that does not have Authentication enabled is at a serious risk of being a relay for spam. Spammers will try thousands of email addresses until they find one to send through, and if Authentication is not enabled, they will be able to use up your bandwidth and system resources to send mail.

Enabling SMTP Authentication ensures that users must supply credentials to send email from your server. This requires a change in their email clients so that the user's information gets passed in SMTP, so there is often a bit of a learning curve. This process is necessary and important to protect your server, however, and without it you are open for abuse.

To require SMTP Authentication for a domain, do the following:

- Alert your users of the change they will need to make to their email client. Due to the nature of this change, it is wise to give them a fair amount of warning.
- Select the domain you want to edit.
- Click on the Configuration tab.
- On the Security card , enable Require SMTP Authentication .
- Click Save .

It is also recommended that you update this setting in the default domain settings so that all new domains will require SMTP Authentication. In addition, to further secure the use of SMTP Authentication, you should ensure that "Require Auth Match" is set to Domain or Email Address for all domains. This means that a sender's "From" address much match the SMTP authentication address or domain, making it more difficult for users to spoof addresses. This can be done under the SMTP In tab of the Protocol Settings.

To apply this setting to all domains on your server at once, use the Domain Propagation page in the Settings menu.

Changing the System Administrator Login

When installing SmarterMail for the first time, you will be required to create a system administrator password during the setup wizard. However, there may be times when you need or want to change this. Here's how to do this.

Instructions

- Go to Administrators .
- Select the administrator you want to edit.
- Use the Change Password button.
- Enter the current (old) password for verification.
- Enter a new and password (If changing the username as well, avoid using an email address for the username).
- Click on Save .

Resetting an Unknown Login

For instructions on how to reset an administrator login when the current login is unknown, please see the KB article How To Reset an Administrator Username and Password .

Troubleshooting a Domain or User

There are times when you will need to access domain specific information or review the settings/configuration of a particular user. SmarterMail offers system administrators the ability to impersonate users or domain administrators to accomplish these goals.

First things first: as a system administrator, as long as "Allow domain management" and "Allow impersonation" permissions were granted to your administrative account, you'll be able to assist with any domain or user management duties that come up. In addition, the need to impersonate a domain administrator is mitigated by having domain settings available to system administrators with "Allow domain management" permissions. When managing a domain, system administrators will have tabs available when managing a domain that mirror the same settings seen by domain administrators. Therefore, while it's not necessary to impersonate a domain administrator, it is definitely possible.

Using a Domain's Accounts Tab

If a system administrator has the proper permissions, when they manage a domain they'll see tabs that represent all of the settings that domain's administrator has access to. One of these tabs is the Accounts tab. Here, a list of all that domain's users is displayed along with columns that display certain pieces of information about each user. One of those columns is labeled Type . If you need to impersonate a domain administrator, look for a user with the "Domain Administrator" type. Simply select that user then select Impersonate User from the Actions (□) button. A new browser tab will open up, and you'll be taken to that user's settings. From here, you can go to Domain Settings and see that all of that domain's settings.

Alternatively, you can right-click on a username on the Accounts tab and select "Impersonate User" from the context menu. Both methods have the same result.

Translation Guide

Upon installation, SmarterMail offers translations for over 15 different languages. While the majority of the most popular languages are covered, there may be instances where a specific regional language or other language isn't represented with our default installation. That's where the SmarterMail translation files come into play.

SmarterMail includes an English language file that contains each word, phrase and sentence used in

SmarterMail. For every translation key, there is an associated text value, and each value would need to be translated.

System administrators, therefore, have the ability to either edit existing translation files to correct errors or change the way something is referenced, or create entirely new translations using the English language file that's provided. These new translations can account for dialects or colloquialisms, making translation more friendly and usable for specific customers. Ideally, any changes, updates or new translations that are created should be shared with SmarterTools. That's because with each update we role out, the previous (unchanged) files will be used in the update process, overwriting any changes made to the installed files. If we have current, updated translations, we can provide those along with any updated Builds we release.

Creating a New Translation

To begin, navigate to the translations folder and save a copy of the English language file found there. Then, title the copy according to your locale abbreviation. (E.g., Zh-TW.json for Taiwanese.) A list of the different locale abbreviations can be found here: http://msdn.microsoft.com/en-us/goglobal/bb896001.aspx .

As you edit each language string in the new file, once you've saved your changes you can see the changes immediately in your browser when you switch the interface language to your specific translation.

Styling Notes for JSON Files

Note that some characters require special encoding to preserve the integrity of the JSON file. If you're unfamiliar with this programming language, you can use an JSON editor to modify and validate the file. If at any point your language stops showing up, there is likely a problem with JSON formatting. Look at the items you just changed to ensure they don't have any invalid characters, missing commas or mismatched tags. There are two important things to remember when editing the JSON file:

- Avoid using double quotes when editing a line that already uses double quotes.
- Avoid translating any variable names, as these are used by the SmarterMail backend in order to properly display information.

Here are some examples:

- If a string value includes quotation marks, use single quotes, not double quotes. For example, these formats are acceptable:

```
TRANSLATION_KEY: "This is the translated text, and this is how 'quoted
text' should appear.", TRANSLATION_KEY: "This is more translated text, and
```

```
\"quoted text\" can also be formatted like so.", But this format will break
the file:
```

```
TRANSLATION_KEY: "This is translated text, and this is NOT how "quoted
text" should appear.",
```
• Any words within curly brackets {} should not be translated, unless those words are encompassed by apostrophes. Here are 3 examples of how to properly translate the variables:

   • The following string should remain as is , since each word in this string is within the curly brackets without accompanying apostrophes.

```
DISK_SPACE_WITH_PERCENT: "{{used | bytes}} {{percent ? ('(' +
(percent|number:0) + '%)') : ''}}"
```
• In the following string, each word is contained in the curly brackets. However, because Alias and Aliases are encompassed by apostrophes, you would need to translate only those words .

```
DOMAIN_MANAGEMENT_ALIASES: "{{count}} {{count == 1 ? 'Alias' : 'Aliases'}}"
```

• In the following string, both of and Used should be translated.

```
DISK_SPACE_USED_OF: "{{used | bytes}} {{total ? ('of ' + (total | bytes)) :
''}} Used"
```

When the Translation is Complete

Once you've completed your translation, you can validate the JSON formatting here: https://jsonlint.com . Once it validates, PLEASE contact sales@@@smartertools.com and let us know. We'd be happy to include your translation along with our installation files.

Glossary

Below is an alphabetized list of the various terms and phrases used in the SmarterMail Product.

Account - An account consists of an email address and a password, used to log into a mail server to retrieve or send mail.

Administrator - The person or company that purchased and installed SmarterMail Professional Edition on a server with abilities to set global configurations and create and delete email domains and end users.

Alias - An email address representing another address that only forwards received mail to another address or group of addresses. For example, if your email address is you@@example.com and you wanted to make an account for purchases without actually having separate inboxes to check, simply create the email Alias purchases@@example.com and the mail for purchases will be redirected to your original mailbox.

APOP - APOP stands for Authenticated Post Office Protocol. Every mail connection made sends your username and password across the network in clear text (no encryption). With APOP, your password is encrypted while being transmitted over the Internet.

Auto Responder - A preconfigured message immediately sent back to anyone you receive an email from.

Blacklist - Block email from email addresses and domains added to this list.

Content Filtering - Content Filtering allows a user to search incoming messages for certain words or string of words. Messages containing the filtered items can be acted upon, for example deleting them so it never reaches its final destination, or moving them to a separate folder away from the main inbox.

DNS Server - A DNS Server is a computer designated to holding a list of domain names and their corresponding IP addresses. For the purposes of SmarterMail, some Domain Name Servers hold a list of domain names and IP addresses associated with mass spam mail outs. SmarterMail makes it possible for administrators to enter the URL and take advantage of these Domain Name Servers to filter out mail from known spammers.

Domain - A domain is the name associated with the last half of an email address, it resides after the @@ symbol (e.g. in support@@example.com, example.com is the domain).

Domain Administrator - The owner of a particular domain responsible for adding and deleting email accounts and setting configurations associated with that domain. The domain administrator account also functions like a standard user account in that it can send and receive mail, manage contacts, etc.

Domain Alias - An additional domain that forwards received mail to another address or group of addresses. For example, you may have two email addresses with different domain names, to combine their inboxes, add one email address to the Domain Alias List.

End User - A person who uses SmarterMail to send and receive mail, manage contacts and calendar events, etc. whether using the webmail client, a desktop client or mobile device.

Folder Auto-Clean - Automatic deletion of older messages when a folder reaches a certain size. Used to keep folders like Junk Email under control.

Forward - To redirect a received email to another email address.

IMAP / IMAP4 - Internet Message Access Protocol (IMAP) is a standard protocol for accessing email from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which email is received and held for you by your Internet server. IMAP requires continual access to the server during the time that you are working with your mail.

IP Address - Internet Protocol address is the numeric physical address of any computer. Therefore, you can access a computer by entering either the domain name or the IP address for the domain (e.g. 127.0.0.1).

IP Bypass - Pardon IP addresses from SMTP authentication enabled on any domain. This is often used to allow clients who have applications that do not support SMTP authentication to bypass this check.

IP4R / RBL List - A DNS lookup that attempts to determine if a mail server is likely to be sending spam. You take the IP address of the mail server, turn it around, and query a "DNS zone", to come up with something like "2.0.0.127.relays.example.com". If the mail server is listed in the spam database you queried, it will return an answer indicating that the mail server is listed.

LDAP - Lightweight Directory Access Protocol (LDAP) is a communication protocol for accessing online directory services. Programs like Outlook and Thunderbird use LDAP to retrieve contact lists from SmarterMail.

List Server - A list server (mailing list server) is a program, or a feature in a program, that handles subscription requests for a mailing list and distributes new messages, newsletters, or other postings from the list's members to the entire list of subscribers as they occur or are scheduled. Note: A list server should not be confused with a mail server, which handles incoming and outgoing email for Internet users.

Mailbox - A folder that contains messages.

Mailing List - A mailing list is a list of people who subscribe to a periodic mailing distribution on a particular topic. Mailing lists include each person's email address. Mailing lists have become a popular

way for Internet users to keep up with topics they're interested in. Many software producers and other vendors are now using them as a way to keep in touch with customers.

POP / POP3 - With Post Office Protocol version 3 (POP3) your mail is saved for you in your mailbox on the mail server. When you read your mail, all of it is immediately downloaded to your computer and no longer maintained on the mail server.

Postmaster - A required default email account for a domain. In order to receive email from the postmaster account, it has to be forwarded to another email address.

Relay - Allows an SMTP server to accept any email destined for other hosts and re-deliver that mail to the proper host, much like a track and field relay race where the SMTP servers are the runners and the email message is the baton.

SMTP - Simple Mail Transfer Protocol is a TCP/IP (Internet) protocol used in sending and receiving email. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending email and either POP3 or IMAP for receiving messages that have been received for them at their local server.

SMTP Authentication - When the mail server requires an email address and password that matches an account in order to send mail, as opposed to requiring just an email address.

Spam Check - A resource used for checking the validity of an email sender.

Spam List - Some Domain Name Servers (DNS) on the Internet contain a list of addresses from mail servers that are solely used for email spam. Therefore, the Spam List is an editable list of DNS' so you can compare your incoming mail to those known spam email servers and filter them out accordingly (An example of an "antispam" DNS is opm.blitzed.org).

Spam Weight - The weight is a value assigned to a spam check according to its validity and competency. Generally, the higher the weight, the more likely an email message is spam.

Spool - A directory on the mail server that holds emails before they are viewed or downloaded from a client.

Stats - The overall calculations about email from a domain including total messages and bandwidth.

URL - The Uniform Resource Locator is an address that links to a web page or web server that is usually entered into the top of a browser.

User - A client with an email account.

Web Interface - The point of access for administrators and end users to the Mail Server via browser.

Webmail - An interface for sending and receiving email through the use of a browser instead of an email program (e.g. Outlook). SmarterMail's webmail client is as powerful and feature-rich as any desktop or mobile email client.

Web Service - A Web Service is a remote application interface that a program can connect to in order to obtain information or execute commands through standard internet ports (typically port 80, the same port used by a typical web browser)

Whitelist - Add an email address to this list to accept all mail from the sender, regardless of Black List restrictions.

SMARTERTOOLS END USER LICENSE AGREEMENT

This End User License Agreement ("EULA") is between SmarterTools, Inc. ("SmarterTools") and the License holder ("You" or "Your") of the product this EULA accompanies ("Software"), whether the License was acquired individually, or on behalf of a company, organization, or other entity. It is important to read and understand all the terms, limitations, and conditions contained in this EULA prior to installing and using the Software because they affect how You may use the Software and Your rights under this License. By explicitly accepting this EULA by installing, copying, downloading, accessing, or otherwise using the Software, You agree to be bound by the terms of this EULA. If, prior to using or installing the Software, You decide that You are unable or unwilling to agree to the terms of this EULA, promptly and completely uninstall and destroy any electronic copies of the Software and accompanying items in your possession.

This EULA shall apply to this Software, future versions of this Software, updates, add-ons, and plug-ins to this Software, features selection(s), including, but not limited to, "Professional," "Enterprise" and "Free" editions of the Software, and maximum allowed numbers of users, profiles, devices, email addresses, domains, web sites, or agents ("level"), in addition to any services, technical support, advice, and recommendations related to this Software that may be made available by SmarterTools on the internet, on websites, in the Software documentation, via email or by telephone.

DEFINITIONS

The following definitions shall apply for the purposes of this EULA:

"Confidential Information" shall mean any information or material provided by SmarterTools to You, regardless of how it is provided, that is labeled "Confidential" or has any similar designation, or is information logically understood to be confidential by any reasonable person. This information also includes, but is not limited to, license keys, information related to SmarterTools pricing, any product roadmap, any marketing plans, any Software improvements, or any other information not made available to the public.

"Dedicated Hosting" shall refer to an individual, group, or organization ("Dedicated Host") that maintains a physical server device that is wholly or, in the case of Virtual Private Servers ("VPS"), a dedicated portion of a physical server device that is sold, leased, or otherwise made available to a third party; whether or not a fee or other compensation is exchanged; and in which the third party has authorization and/or access to the activation areas of the software and/or to system administration functions.

"Effective Date" shall be the date upon which this EULA was accepted by You.

"Guest Operating System" shall mean any operating system for which You are officially licensed that runs as a guest, or instance, on top of another operating system, such as in the use of one or more VPS that are used to run the Software.

"License" shall refer to the revocable, non-exclusive, non-transferable license to use the Software in accordance with the terms and conditions of this EULA. The term License applies to purchased and non-purchased Licenses, including but not limited to the object code, source code, and any accompanying alphanumeric combinations used to enable and/or activate the software or certain Features Selection(s) in the Software (collectively, "License Keys")

"License Key" shall apply to the alphanumeric combination entered/applied upon installation and used to access Feature Selections. License Keys are delivered to the owners of purchased (paid for) Licenses and to those who may receive authorized promotional or trial Licenses, if applicable (pursuant to this EULA). This EULA remains in full force and effect for the Software whether a License Key is required or provided by SmarterTools.

"Maintenance and Support" shall mean a yearly, optional licensing subscription that provides You with the ability to download and install any software updates released by SmarterTools and submit support requests as outlined on the Technical Support page of the SmarterTools website. Maintenance and Support is required for the continued use of any Third-Party add-on based on the agreements in place with Third-Party vendors.

"Periodic License" shall be a License with a defined start and end date whether such License is subject to renewal, automatically renews, effectively terminates, or is extended (e.g., Monthly/Lease Licenses, Trial Licenses, Development Licenses). Periodic Licenses may be governed by additional terms and conditions in a separate written agreement.

"Shared Hosting" shall refer to an individual, group, or organization ("Shared Host") that maintains a physical server device upon which software and/or tools are owned and installed by the Shared Host and made available to third parties for access or use; whether or not a fee or other compensation is exchanged; and in which the third parties do not have authorization or access to the activation areas of the Software and/or do not have authorization or access to system administration functions.

"Software" or "Product" shall mean any products developed by SmarterTools, and any third-party products and/or services provided as part of those products and installed by end users and/or system administrators, regardless of where that installation occurs.

"Third Party Providers" shall be any other software, application, plug-in, add-on, utility, tool, device, or methodology by any individual, group, organization, affiliation, company, or other entity that connects, modifies, links, and/or integrates to/with the Software for any purpose whatsoever.

1. License.

A. Grant of License.

Subject to the terms and conditions of this EULA, SmarterTools hereby grants You a revocable, non-exclusive, non-transferable, non-assignable, limited license to use the Software ("License"). This License shall commence on the purchase date of the Software and shall remain in effect until terminated in accordance with the terms of this EULA or superseded by another end user license agreement pursuant to installation of an Update or changes in Features Selection. SmarterTools, together with any third-party content providers whose software code is incorporated in the Software or distributed with it, retains all right, title, and interest to the Software, including, but not limited to, copyrights, trademarks, proprietary methods, and trade secrets ("Intellectual Property") incorporated into the Software.

This License to use the Software is conditioned upon You paying all related charges and fees imposed by SmarterTools for purchase of the Software, monthly license of the Software, or for the authorized delivery of the Software as a service (SaaS). SmarterTools may, in its sole discretion, disable this License if You fail to pay such charges or fees within the time allowed by SmarterTools or otherwise violate any terms in this EULA.

B. Use of the Software.

You shall use the Software for Your own personal or internal business purposes. Personal or internal business purposes shall include the installation of the Software and activation of only one License on any single instance (i.e., personal computer, server, virtual private server (VPS), Cloud instance, etc.) by You or Your Customer(s) pursuant to the terms of section 1.C. below.

C. Sublicense, Resale, Lease, Sub-lease, or Transfer

You may sublicense this License to a third party(ies) ("Customer") only pursuant to a Shared or Dedicated Hosting agreement and the terms and conditions of this EULA, if applicable. You represent and warrant that each Customer has accepted this EULA prior to allowing the Customer access to or utilization of the Software and You shall promptly provide confirmation of each Customer(s) s acceptance of the EULA upon request by SmarterTools. You shall indemnify, defend, and hold SmarterTools harmless against any claims asserted by or against You by any of Your Customer(s) or by any third party related to Your Customer(s) s use of the Software, including but not limited to claims of infringement of the intellectual property rights of any third party and the additional warrantee, liability, and indemnification provisions found in Sections 3 and 5.

Certain authorized parties ("SmarterTools Partner") may Resell, Lease, or Transfer this License (collectively, "Transfer") to any third-party subject and pursuant to a separate authorizing agreement

with SmarterTools. For the purposes of this EULA, Transfer shall refer to any transaction whereby sole use, management, ownership, and/or control of the software is assigned to any third-party for that party's benefit, pursuant to the terms and conditions of this EULA, whether a fee or other compensation is charged and whether such Transfer is permanent or temporary. Transfers by or between any party(ies) other than SmarterTools or a SmarterTools partner must be approved by SmarterTools in advance and in writing.

You may install and maintain the Software on behalf of a third party; however, all SmarterTools Licenses in such circumstances must be purchased by the third party directly through SmarterTools or through a SmarterTools Partner and the Software must be activated under the name of the related third party; thereby, the related third party assumes full ownership of the License subject to the terms and conditions of this EULA.

D. Limitations on Use of the Software and License Keys

You shall not modify, reverse engineer, reverse assemble, decompile, disassemble, decrypt, reflect, or use reflection on the Software, or otherwise attempt to discover or obtain the source code or structure, sequence, or organization of the software in whole or in part, except as provided in Section 9 of this EULA. You may distribute copies of the software code in the same format that you received it, pursuant to the terms of this EULA, so long as You do not modify the Software in any way and so long as all copyright, trademark, and other notices contained in the Software remain intact.

You shall not attempt to bypass, circumvent, disable, design around, or obviate the License Keys for any reason, including but not limited to attempts to access features, capacity, or capabilities in the Software not included in your Features Selection. Further, other than pursuant to Section 1.C. of this EULA, You shall not disclose or disseminate any License Keys associated or distributed with the Software, publicly or to any third party, nor shall You allow anyone else to use any such License Keys.

You may reassign/migrate this Software to a different device owned, leased, or rented by You subject to SmarterTools' approval in its sole discretion, if You completely uninstall or delete the Software from any personal computer, server, Virtual Private Server, or other device on which the Software was previously installed. SmarterTools reserves the right to require, in its sole discretion, reauthorization, re-registration, or another form of authentication at no additional charge to enable reassignment of the Software and may disable the related License Key and/or access to the Software at any time if it determines, in its sole discretion, that such reassignment is prohibited by the terms of this EULA or constitutes fraud.

You shall not use the Software to harm third parties, disseminate unsolicited communications (emails, etc.), requests, or harmful data or programs including but not limited to malicious scripts and viruses.

You shall not use the Software to disseminate pornography, child pornography, or other harmful or illegal materials, or in any way that may disparage or bring disrepute to SmarterTools.

E. Beta Services

SmarterTools may, from time to time, offer certain Software or Services as closed or open beta services ("Betas", "Beta Software", "Beta Service(s)") for the purpose of testing and evaluation by You. You agree that SmarterTools has the sole authority to determine the period for this testing and evaluation. In addition, You agree that SmarterTools will be the sole judge as to the success of such testing and evaluation and the decision, if any, to include or otherwise offer the Software or Services tested. You further agree that SmarterTools will not be liable to you or to any third part for any harm related to, or arising out of our caused by, any Betas.

2. Term and Termination.

This EULA is effective as of the date You install or use the Software, or as of the date You accept this EULA, whichever is sooner. You may terminate this EULA by completely deleting and wholly destroying any copies of the Software and documentation in Your possession or control. SmarterTools may terminate and/or disable the License or EULA if, in its sole discretion, SmarterTools determines that You have breached any of the terms and conditions of this EULA, with or without notice to You of such termination. Sections 1.B., 1.C., 1.D., 3, 5, 6, 7, 8, 9, 10, 11, 12, and 13 shall survive termination of this EULA.

3. Limited Warranty and Limitation of Liability.

A. No Warranties

SmarterTools does not warrant that the Software will meet Your requirements, that the operation of the Software will be uninterrupted or error-free; that any data supplied by the Software will be accurate; or that the Software will work with any 3rd-party or supplemental software or hardware furnished with or accompanying the Software. Further, SmarterTools does not warrant the efficacy, functionality, or operation of such Accompanying Software or Hardware. ALL HARDWARE, SOFTWARE, OR OTHER PRODUCTS OR SERVICES PROVIDED BY SMARTERTOOLS UNDER THIS EULA ARE PROVIDE AS-IS, AND SMARTERTOOLS EXPRESSLY DISCLAIMS ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

B. No Liability for Damages

SmarterTools shall not be liable for any damages under this EULA, including but not limited to consequential, statutory, punitive, incidental, or indirect damages, including but not limited to any loss of data, loss of profits, loss of savings, loss of time or convenience, or additional cost arising out of the

use of or inability to use the Software, documentation, support, or any 3rd-party or accompanying software or hardware; even if SmarterTools has been advised of the possibility of such damages.

SmarterTools only provides the Software; it does not, and cannot, provide any additional products, policies, or services that should be included as part of an organization's use of the Software. Examples of these products, policies, or services include networking appliances, network configurations, firewalls, backup software or services, backup policies, backup retention policies, data protection policies, data protection services, or any other product or service that should be used to mitigate the potential for issues that may cause loss of data, loss of profits, loss of savings, loss of time, or any additional costs arising out of the use of, or inability to use, the Software.

It is Your responsibility to verify whether the Software or service matches the level of risk, security considerations, compliance regulations, or other mitigating circumstances based on your particular use case for the Software, your industry, laws, rules, and guidelines, or any other factor. SmarterTools documentation should not be the sole factor referenced or reviewed for you to make this judgement/verification. Product installation and testing should be performed in addition to communicating with SmarterTools, reviewing documentation, and other exploratory research and analysis as part of your due diligence.

You undertake to keep SmarterTools indemnified from and against all claims and demands of any third party relating to an unauthorized access to or exposure of sensitive or confidential information and/or relating to a data breach, including any exposure of sensitive or confidential information as defined by article 33 GDPR, in Your infrastructure and/or Software and against all charges, costs and expenses incurred in defending, contesting or settling such claims or demands, unless the same can be shown to be attributable solely to the acts or default of SmarterTools.

Further, SmarterTools shall not be liable for nor bound by any claims, representations, promises, assertions, or other statements made by anyone other than SmarterTools employees or officers, including but not limited to resellers and sales representatives.

SmarterTools shall not be liable for any damages or inconvenience resulting from errant data or misreporting of data, nor failures to relay information that may be deemed important by the user, any errant or substantial mistranslation of language or information, and/or for any damages arising from events listed in Section 5 of this EULA.

C. Third Party Providers and Web Services

The Software is designed to integrate and/or to be used in conjunction with Third Party Providers through web services. SmarterTools assumes no liability and makes no warranty or guarantee regarding the applicability or effectiveness of this Software when used in conjunction with these products or whether such integration or use might interfere with the operation therein. You agree to

hold SmarterTools harmless in all matters resulting from the integration or use with Third Party Providers.

D. Limitation of Liability

Your sole remedy under this Agreement shall be limited to replacement of the Software.

4. Technical Support

Currently, SmarterTools provides technical support for the Software via SmarterTools personnel, documentation, and internet resources. For a period after initial purchase of a License, and for subsequent periods when Maintenance and Support is active for a License, technical support from SmarterTools personnel is provided at no charge. If Maintenance and Support is no longer active on a License or if the License is for a product that is no longer in development by SmarterTools, technical support is only available via documentation and internet resources. SmarterTools also provides fee-based tickets for emergencies related to SmarterTools products, as well as training and installation of SmarterTools products. These fees may vary from time to time. Technical support is provided AS-IS, and the provisions of section 3.A., 3.B., 3.C, and 3.D. apply to technical support.

SmarterTools provides no guarantee, expressed or implied, regarding the efficacy or continuation of technical or other support for this Software or version of this Software for any length of time and SmarterTools may choose to discontinue such support at any time and for any reason.

5. Indemnification.

SmarterTools shall defend you against any third-party claim that Your use of the Software, as authorized under this EULA, infringes any patent, copyright, or trademark of a third party, and indemnify you from the resulting costs and damages awarded against You to the third party making the infringement claim. This is dependent upon you (a) notifying SmarterTools, in writing, of any Infringement Claim within thirty (30) days of notice of the claim; (b) giving SmarterTools sole control of the defense of any Infringement Claim and any related negotiations or settlement; and (c) giving SmarterTools all information and assistance necessary to settle or defend the Infringement Claim.

Exclusions to the above include for any Infringement Claim arising out of Your, or any party's other than SmarterTools, modification(s) to the Software, the use of other than the most current version of the Software if the infringement would have been avoided by use of the most current version, the use of Open Source Software in conjunction with the Software, the use of the Software with materials not furnished by SmarterTools or not in accordance with this EULA, or use of the software outside the scope of this EULA.

You shall defend, indemnify, and hold harmless SmarterTools and its suppliers, licensors, successors, affiliates, agents, employees, executives, and assigns (hereafter "SmarterTools Indemnified Parties")

from any claims, damages, losses, or expenses (including without limitation attorney fees and costs) incurred in connection with any and all damages, losses, claims, suits, judgments, or causes of action asserted against SmarterTools Indemnified Parties by third parties or Your Customers related to:

Damages arising from Your breach or Your Customer's breach of this EULA; Any loss, misdirection, or inaccuracy of any and all data, message, and/or information (partial or complete) by, or directed to, You, Your Affiliates, Your Customers, Your vendors, Your assignees, or any related third party and from any action, inaction, or consequence arising out of such loss, misdirection, or inaccuracy of any data, message, or information; Any misuse, abuse, hostile transmission, fraud, or unlawful action arising from or related to the use of the Software or any portion thereof by, or directed at, You, Your affiliates, Your Customers, Your vendors, Your assignees, and/or any related third party; Any claim, damage, loss, or expense related to the installation, quality, use, operation, functionality, transfer, or de-installation of the Software by You, Your Customer(s), or third parties; Any charges imposed by You or third parties on You or Your Customers related to Your or Your Customer(s) s use of the Software, including but not limited to charges for data transmission and bandwidth, regardless of whether you have followed any recommendations provided with the Software or Software documentation.

6. Transfers

The rights under the License may be sublicensed under the terms of Section 1.C. or transferred to any of Your successors, heirs, or assigns. Any other attempt to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is void unless You have a separate written agreement with SmarterTools allowing for such transfer(s).

7. Jurisdiction.

This Agreement shall be governed in all respects by the laws of the United States and the State of Arizona, except for conflict of law's provisions. The parties agree that for any dispute, controversy, or claim arising out of or in connection with this Agreement, venue and personal jurisdiction shall be in the federal, state, or local court with competent jurisdiction located in Maricopa County, Arizona. The prevailing party will be entitled to an award of reasonable attorney's fees.

In the case that You are an agency or entity of the United States Government, the following additional terms apply:

* The Software qualifies as Restricted Computer Software, as defined in the Rights in Data-General clause at Federal Acquisition Regulations 52.227-14.

* Use, duplication, or disclosure by the Government is subject to restrictions as set forth in

subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

8. Payments and Pricing.

You shall pay the total fee(s) for the Software imposed by SmarterTools at the time of purchase. You shall pay all invoices rendered by SmarterTools within thirty (30) calendar days after the invoice date, or within another time frame set forth by SmarterTools in writing in a separate agreement. All payments shall be made in United States Dollars ($).

Pricing for the Software and any associated products is available on the SmarterTools website. Additional fees may apply when upgrading to a version of the Software significantly enhanced with features previously not existing in Your License. In addition, SmarterTools may update pricing of the Software and any associated products, to reflect current exchange rates, inflation, material, workforce and suppliers' costs, additional fees imposed by Third Parties, or other reasons.

A. Effect of Non-Payment

If You fail to pay any amount due within the above timeframe, SmarterTools may impose late charges equal to the lesser of 1.5% per month or the highest interest rate allowable by applicable law, together with all related expenses and collection costs, including reasonable attorneys' fees, incurred by SmarterTools collecting any amounts owed under this EULA. Further, You shall reimburse SmarterTools for any out-of-pocket expenses incurred in connection with duties performed by SmarterTools hereunder. Upon request by You, SmarterTools shall provide You with reasonable documentation evidencing the out-of-pocket expenses incurred by SmarterTools.

9. Limitations to Customization.

Altering the appearance and/or user interface of the Software can only be achieved, and is only supported, by using the tools and options provided within the Software itself. (E.g., using the tools within the software to customize login pages and/or providing custom links to help documentation.) Any changes to any files installed with the Software that are made outside of the Software's interface is done at your own risk and will not be supported, retained, or otherwise preserved during any upgrade, downgrade, or other installation of the Software.

All applicable copyright and trademark information shall not be removed in any way, shall remain visible to the naked eye and free from any clutter or similar color scheme. In addition, any proprietary notices in the Software shall be maintained and neither removed nor obscured in any way.

10. Transmission of Information and Communication.

At purchase of the Software and at other times during the term of this EULA You will be required to supply certain information including, but not limited to, email address(es), password(s), street addresses, personal and/or company information, payment information (e.g., credit card information), and/or other personally identifiable and potentially valuable information. Acceptance of this Agreement indicates Your willingness to provide this information, to keep Your information up to date and current, and to have it transmitted to SmarterTools via internet, phone, facsimile, verbally, or otherwise and Your assumption of the incumbent risks associated with such transfers. SmarterTools takes the privacy and security of data very seriously and will make efforts to protect data in accordance with our privacy policy. A copy of the SmarterTools privacy policy is available by request and incorporated herein by reference. In any event, SmarterTools and its suppliers, licensors, successors, affiliates, agents, employees, executives, and assigns shall not be liable for any stolen, misdirected, or otherwise mishandled information pursuant to this EULA.

From time-to-time SmarterTools may contact You at any address, including any email address(es), You have provided to SmarterTools regarding the Software, available Updates or Features Selection for the Software, or for promotional purposes. You hereby expressly consent to such communications. If you do not wish to receive further notices, you may notify SmarterTools of your preferences via your account on the SmarterTools website.

From time to time the Software may use the internet or other means to exchange data with computers, servers, or other electronic devices owned by SmarterTools to maintain licenses, communicate updates or instructions, provide utilization metrics, gauge performance, enforce SmarterTools' rights with regard to licensing and this EULA, or other information as is needed. Acceptance of this Agreement indicates Your acceptance of this communication and Your assumption of the incumbent risks associated with such communication. Any attempt to prevent, preclude, disrupt, or modify this communication is not allowed under this EULA and may result in the disabling of the Software and license key.

SmarterTools may, at its discretion, offer products and/or services related to the software directly to any user and/or administrator of its Software. The ability of such users and/or administrators to purchase, subscribe or otherwise make use of such products/services is done at their request and any transaction will occur between such users and/or administrators and SmarterTools directly.

11. Third-party Correspondence, Interaction, Purchase, Service, or Promotion

During use of the Software, You may enter into correspondence with, purchase goods and/or services from, or participate in promotions of third party advertisers or sponsors displaying goods and/or services through the Software, and you recognize, however, that certain third-party providers of ancillary software, hardware, or services may require Your agreement to additional or different licenses agreements or other terms prior to Your use of or access to such software, hardware, or

services.. Any such activity, and any terms, conditions, warranties, or representations associated with such activity, is solely between You and the applicable third party. SmarterTools shall have no liability, obligation, or responsibility for any such correspondence, interaction, purchase, service, or promotion between You and any such third-party including, but not limited to, translations, mapping, sharing, or any other service or transfer, even if such third-party correspondence, interaction, purchase, service, or promotion is listed as a benefit or feature of the Software. SmarterTools explicitly disclaims any liability, obligation or responsibility for the continuation, viability, quality, reliability, or availability of any such third party provided correspondence, interaction, purchase, service, or promotion.

In all events, conditions, and circumstances the provisions and limitations of Sections 3, 5, and 7 shall apply.

12. Severability.

The provisions of this Agreement will be deemed severable, and the invalidity or unenforceability of any provision(s) will not affect the validity or enforceability of any other provision(s) herein.

13. Disabling of License Keys

SmarterTools may disable License Keys at any time at its sole discretion. Examples of instances where License Keys may be disabled include, but are not limited to the following: for invoices that are not paid within a reasonable timeframe as determined by SmarterTools payment terms; License Key purchases that are made fraudulently and/or deceptively; License Key purchases that result in a charge-back or disputed charge; Instances where License Key owners threaten legal action against SmarterTools; Instances where License Key owners are deemed by SmarterTools to be abusive towards SmarterTools and/or SmarterTools employees, or otherwise refuse to work collectively with SmarterTools to resolve issues with our software whether through phone conversation, email, live chat, online message boards or community posts, or other means.

14. Dispute Resolution

Any disputes, claims or controversies arising out of, relating to, concerning, or pertaining to the terms of this Agreement, or to either Party's performance or failure of performance under this Agreement ("Disputes"), which Disputes the Parties have been unable to resolve by informal methods, will first be submitted to mediation.

Either Party may initiate mediation by providing Notice to the other Party of a written request for mediation, setting forth a description of the Dispute and the relief requested. Unless otherwise agreed to by the Parties, the mediation will not be scheduled for a date that is greater than 60 days from the date of Notice of the request for mediation.

The Parties will cooperate with one another in selecting the mediator ("Mediator") and in scheduling the time and place of the mediation, per Section 7. Such selection and scheduling will be completed within 30 days after Notice of the request for mediation.

The Parties covenant that they will participate in the mediation, and that they will share equally in its costs (other than each Party's individual attorneys' fees and costs related to the Party's participation in the mediation, which fees and costs will be borne by such Party).

Results of the mediation will not be subject to discovery and will be confidential, privileged, and inadmissible for any purpose, including impeachment, in any arbitration or other proceeding between or involving the Parties, or either of them; provided, however, that evidence that is otherwise admissible or discoverable will not be rendered inadmissible or non-discoverable because of its use in the mediation.

15. Export Control and Regulation

You may not use, export, import, or transfer the Software except as authorized by U.S. law, the laws of the jurisdiction in which you obtained the Software, and any other applicable laws. In particular, but without limitation, the Software may not be exported or re-exported (a) into any United States embargoed countries, or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce's Denied Person's List or Entity List. By using the Software, you represent and warrant that (i) you are not located in a country that is subject to a U.S. Government embargo, or that has been designated by the U.S. Government as a "terrorist supporting" country and (ii) you are not listed on any U.S. Government list of prohibited or restricted parties. You also will not use the Software for any purpose prohibited by U.S. law, including the development, design, manufacture, or production of missiles, nuclear, chemical, or biological weapons. You acknowledge and agree that products, services, or technology provided by SmarterTools are subject to the export control laws and regulations of the United States. You will comply with these laws and regulations and will not, without prior U.S. government authorization, export, re-export, or transfer SmarterTools products, services, or technology, either directly or indirectly, to any country in violation of such laws and regulations.

16. Entire Agreement.

This EULA constitutes and expresses the entire agreement and understanding between the parties hereto with respect to the subject matter, all revisions discussions, promises, representation, and understanding relative thereto, if any, being herein merged. This Agreement replaces and supersedes any prior agreement entered between the parties hereto with respect to the subject matter herein. This EULA may change, from time to time, and when changes are made, the "Revision Date" at the bottom of this document will change to note when the EULA was last updated.

Rev. 20240422