



# Additional Help Topics

Help Documentation

## Additional Help Topics

### Automating LogIn to SmarterMail

The HTML code below demonstrates how you can make a text link (e.g. "Log into your mail") that automatically logs a user in to the SmarterMail application. By putting a hidden form on a simple web page, you can fill in the "Email Address", and "Password" information either via hard coding the data or through a scripting language like ASP, ASP.Net, or ColdFusion.

For the example code listed below, we have the form values set to generic text (e.g. "Actual\_Email\_Address\_Here") to show where you would hard code values that are submitted to the login.aspx page. You could also dynamically generate these values using a scripting language like ASP or ColdFusion (a sample ASP script would substitute value="Actual\_Email\_Address\_Here" with value=<% =email %>). The form action shown (http://127.0.0.1:9998/smartermail/login.aspx) uses the default location of the Smartermail Web Interface. If you have created a separate web site for Smartermail, or assign a different IP address for Smartermail within IIS, this action would have to be altered to reflect this change. This example demonstrates how easy and powerful the Smartermail application is in allowing companies to automate entry into the mail application.

```
<html>
```

```
<head> <meta http-equiv= "Content-Language" content= "en-us" > <meta http-equiv= "Content-  
Type" content= "text/html; charset=windows-1252 "> <title>Smartermail Login</title> </head>
```

```
<SCRIPT LANGUAGE= "JavaScript" > function GoToMail() { document.mailform.submit(); }  
</SCRIPT>
```

```
<body>
```

```
<form name= "mailform" action= "http://127.0.0.1:9998/Login.aspx" method= "post" > <input type=  
"hidden" name= "shortcutLink" value= "autologin" id= "shortcutLink" > <input type= "hidden"  
name= "email" id= "email" value= "Actual_Email_Address_Here" > <input type= "hidden" name=  
"password" id= "password" value= "Actual_Password_Here" > </form>
```

```
<p><a href= "JavaScript:GoToMail()" > Log into your mail </a></p>
```

```
</body>
```

```
</html>
```

## Gateways and Other Server Roles

Please note that SmarterMail was designed to support one server in several of these roles. For instance, one server could act as an Incoming Gateway, Outgoing Gateway, or Backup MX.

SmarterMail can also take on one of these roles when placed together with a competing mail server product. For example, using SmarterMail as an outgoing gateway on a server other than your primary mail server may help to resolve problems with stability of other mail server software products.

### **Primary mail server**

- Use for storing email for defined users.
- Accessible through POP, SMTP, IMAP, and over the web.
- To configure:
- Follow instructions in online help

### **Backup MX Server**

- Use as a backup for mail delivery in case of short amounts of downtime or delivery problems on your primary mail server.
- To configure:
- Add a placeholder domain (called "example.com") to open up the port to listen on.
- Configure SmartHosting by adding the IP addresses to which delivery should be allowed.
- In general settings, change the delivery retry times to 10, 10, 10, and 1440.
- In DNS, add secondary MX records pointing to the new server's IP. Set the preference value higher than the main MX record.

### **Incoming Gateway server**

The FREE, one-domain version will suffice for virtually all environments.

- Use to host third party anti-virus and/or anti-spam software products in order to reduce load on primary server.
- Reduces load on primary server by managing all incoming sessions and performing

abuse/intrusion detection.

- To configure:
- Enable domain forwarding and add all destination IPs and domain names that will be forwarded.
- Add a placeholder domain (called "example.com") to open up the port to listen on.
- In DNS, change the MX records of your domains to reference the new gateway server.
- Install and configure any third-party anti-virus or anti-spam products, such as Declude JunkMail or Declude Virus.

### **Outgoing Gateway server**

The FREE, one-domain version will suffice for virtually all environments.

- Use as a delivery mechanism to reduce load on your primary servers.
- Also use as a method to combat blacklisting. If the server gets blacklisted, rotate the primary IP on the network card to a different one to send out on the new IP.
- To configure:
- Add a placeholder domain (called "example.com") to open up the port to listen on.
- Set relay option in General Settings to "nobody".
- Add the primary mail server's IP addresses to the IP Whitelist for SMTP.
- In your primary mail server's General Settings page, set the IP address of the gateway server and enable gatewaying.

### **SmartGateway server**

The FREE, one-domain version will suffice for virtually all environments.

- Use as a delivery mechanism to balance the load on your gateway servers.
- To configure:
- Add a placeholder domain (called "example.com") to open up the port to listen on.
- Set relay option in General Settings to "nobody".
- Add the primary mail server's IP addresses to the IP Whitelist for SMTP.
- In your primary mail server's General Settings page, set the IP address of the gateway server and enable gatewaying.

## **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 a Backup MX Server

- Add a placeholder domain (called "example.com") to open up the port to listen on.
- Configure SmartHosting by adding the IP addresses to which delivery should be allowed.
- In general settings, change the delivery retry times to 10, 10, 10, and 1440.
- In DNS, add secondary MX records pointing to the new server's IP. 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
- Encourage the adoption of SPF

### 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.

To receive notifications of every update that SmarterTools releases for SmarterMail, go to the SmarterTools Customer Portal , login, select Account Management, then select Mailing Lists, and choose the "Updates.SmarterMail" subscription. Whenever a new update for SmarterMail is released, an email is sent to that mailing list. The list is not used for any other purpose.

## 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 mis-delivered 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 email accounts 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-all accounts 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.
- Go to the General Settings page under the Settings menu.
- Click on the Security tab.
- Change Catch-Alls to Disabled.
- Click on Save icon.

## Restrict Bounces and Auto-Responders

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 auto-responders that reply back to spoofed spam email.

SmarterMail allows you to restrict bounces and auto-responders 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 auto-responders, do the following:

- Alert your users of the new policies being put into place.
- Go to the General Settings page under the Settings menu.
- Click on the Security tab.
- Change Auto-Responders to either Disabled or Require SPF.
- Change Bouncing to either Disabled or Require SPF.
- Click on Save icon.

## 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 accounts 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 account 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 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.
- Go to Manage Domains.
- Click on the Actions menu next to the domain and choose Edit Domain.
- Go to the Technical tab.
- Check the Require SMTP Authentication box.
- Click on Save icon.

It is also recommended that you update this setting in 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 sender match authenticated address" is set for all domains. This means that a sender's "From" address must match the SMTP authentication address, making it more difficult for users to spoof addresses. This can be done under Protocol Settings -> SMTP In .



To apply this setting to all domains on your server at once, use the Default Domain Settings Propagation page in the Settings menu.

## Encourage the Adoption of SPF

SPF is an excellent method of preventing email spoofing, protecting your users from having their domain show up on spam throughout the world. SPF, however, is only as effective as you make it, as it requires changes to your DNS servers for each domain you host email for.

It is in the best interest of all email users everywhere that domain administrators add SPF records to their domain that indicate what servers are authorized to send email for their domain. Encouraging your domain administrators to adopt SPF protects them from being the victims of spoofing, and reduces the spam threat on not only your server, but others throughout the world as well.

More information can be found at: <http://www.openspf.net/>

## Proper DNS Settings for Email

There are several major things to set up on your DNS server for each site you add to SmarterMail. How you set these up is dependent upon both who hosts your DNS and what DNS software is used. Check your DNS server documentation for instructions on how to set up the following records (replace example.com with the proper domain name).

Also, please bear in mind that your DNS may need to be set up differently. This is only a guideline that is recommended for most installations.

- WebMail URL - Add an A or CNAME record for mail.example.com that points to the IP address of the webmail interface. This will allow users of that domain to access the webmail by typing in <http://mail.example.com> or <http://mail.example.com:9998> in their web browser (depending on whether you use the included web server or IIS).
- Mail Pointer (MX) - Add an MX record for the domain that points to mail.example.com. This will allow other email servers to locate your mail server.
- Reverse DNS Record - Add a reverse DNS record for IP addresses assigned on the server to provide extra assurance to other mail servers. Also, it is recommended that the primary IP address of the server also have a reverse DNS record.
- Sender Policy Framework - Some large email providers like Hotmail and AOL are starting to require specially formatted TXT records to be added to your DNS. This special format is known as SPF (Sender Policy Framework). Information about how these records should be formatted can be found at <http://spf.pobox.com> . Please keep in mind that the owners of the domains may have significant input on what goes into these records.

## Changing the System Administrator Login

By default, the login for the system administrator for SmarterMail is admin/admin . While this is easy to remember, it is also fairly easy to guess. When installing SmarterMail for the first time, you will be required to change this password during the setup wizard. Here are instructions in the manner you would want to change the system administrator password again.

### Instructions

- Login as the administrator with the current login.
- Click the Settings icon.
- Choose General Settings in the left tree view.
- Click on the Administrator tab.
- Enter the current password for verification.
- Enter a new username and password (avoid using an email address for the username).
- Click on Save icon.

### 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

There are times when you will need to access domain specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator. This can be a useful method to examine domain settings or configure settings.

To impersonate a domain, click the manage icon . Then select the desired domain in the content pane and click Manage in the content pane toolbar. A new window will pop up, and you will be logged in as the domain administrator. From there, you may edit user accounts, content filters, or whatever other part of the domain that needs to be changed.

For instructions on troubleshooting specific user accounts on a domain, please see the topic [Troubleshooting an Email Account](#) .

## Modifying Scoring for the SpamAssassin-based Pattern Matching Engine

System administrators can modify the scoring for the SpamAssassin-based pattern matching engine

using the local.cf file. However, this feature is only recommended for experienced system administrators.

The local.cf file is placed in the service's SAData folder. It is used to override existing tests or to create new tests supported by SmarterMail. Note: Any modifications to the local.cf file will not be overwritten when installing a new version.

## Overriding an Existing Test's Score

The most common modification to the local.cf file will be to override an existing test's score. For example, if a system administrator notices a lot of spam messages getting into his users' mailboxes that are failing a particular test, he may want to override that test's score.

To do so, the server administrator would add something like:

```
score TEST_I_WANT_TO_OVERRIDE 1.3
```

Here score is the keyword used by the engine, TEST\_I\_WANT\_TO\_OVERRIDE corresponds to the existing test they want to override and 1.3 is the new score.

## Creating a New Test

If a system administrator notices a new pattern appearing in spam messages that isn't covered by the default files, he may want to create a new test. This would look something like this:

```
body NEW_TEST /test/ #look for the word test in the body of the email score NEW_TEST 10.3
```

Here body is the keyword for determining the type of test, NEW\_TEST is the name of the new test, /test/ is the perl style regular expression that will be used while scanning the email, and everything after the pound-sign is a comment.

The system administrator will also need to score the new rule so that it has some effect on the final weight.