



# Additional Topics

Help Documentation

## Additional Topics

### Automating Log In to SmarterMail

The HTML code below demonstrates how you can make a text link (e.g. "Log into your mail") that automatically log a person 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>
```

## 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 several different web services. These web services allow 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, test servers added to the Web Interface, and more.

To view the web services and the corresponding functions available to you, go to your default Web Interface install location and append "services/SERVICENAME.asmx". Your particular SmarterMail location can be the specific IP address of the Web Interface (e.g. if you installed SmarterMail with the default installation you would use <http://127.0.0.1:9998/services/SiteAdmin.asmx>, etc. or a specific IP address you assigned for the Web Interface if you custom-installed SmarterMail or moved SmarterMail to a new web server) or a specific site name if you configured SmarterMail as an actual website within IIS (e.g. [mail.example.com](http://mail.example.com)). Below you will find a brief explanation of the web services available to you, along with the default installation paths to the specific web services details page.

### User Alias Administration

<http://127.0.0.1:9998/Services/svcAliasAdmin.asmx>

There are six (6) functions of this service available for customization. These services allow developers and/or System Administrators to dynamically create email aliases using SOAP, an HTTP GET command, or an HTTP POST command.. The functions, and their corresponding functions, are:

- DeleteAlias - will delete a specified email alias.
- UpdateAlias - will update a specified email alias.
- GetAlias - will return information on a specified email alias.
- AddAlias - will created an email alias and add it to the specified domain.
- GetAliases - will return all aliases that belong to a specified domain.
- SetCatchAll - sets the specified alias to be the catch-all, or clears the catch-all if a blank alias name is provided.

## Domain Administration

<http://127.0.0.1:9998/Services/svcDomainAdmin.asmx>

There are twelve (12) functions of this service available for customization. These services allow developers and/or System Administrators to dynamically add or delete domains, return domain defaults, set a primary domain, and more using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well). The functions, and their corresponding properties, are:

- RenameDomain - renames the specified domain.
- GetDomainSettings - returns the default domain settings in a DomainSettingsResult object.
- GetDomainInfo - returns the default domain settings in a DomainSettingsResult object.
- AddDomain - creates a new domain in the specified folder.
- UpdateDomain - updates the settings for the specified domain.
- GetAllDomains - returns a list of all domain names.
- GetDomainDefaults - returns the default domain settings in a DomainSettingsResult object.
- UpdateDomainNameAndPath - changes the specified domain's name and/or path.
- DeleteDomain - deletes the specified domain.
- GetDomainStatistics - returns the statistics for the specified domain over the specified period of time.
- ReloadDomain - reloads the specified domain's settings.
- SetPrimaryDomainAdmin - sets the specified user to be the primary domain admin of the specified domain.

## Mail List Administration

<http://127.0.0.1:9998/Services/svcMailListAdmin.asmx>

There is only one function for this service. Due to amount of possible commands for list serv, it would require an almost unusable amount of commands to manage list serv via web services. What is offered as a web service is simply the removal of all lists (settings concerning lists are in the domain setup service).

- DeleteAllLists - deletes all mailing lists that belong to the specified domain.

## Product Info Web Service

<http://127.0.0.1:9998/Services/svcProductInfo.asmx>

There are four (4) functions of this service available for customization. These services allow developers and/or System Administrators to dynamically activate or retrieve licensing information,

return product name and version number, and more using SOAP, an HTTP GET command, or an HTTP POST command. The functions, and their corresponding properties, are:

- `ActivateLicenseKey` - will activate the product with a previously set license key using the specified SmarterTools account credentials.
- `GetLicenseInfo` - returns the license key for the product.
- `GetProductInfo` - will return the product name and version number.
- `SetLicenseKey` - will set the product license key.

## Global Update Web Service

<http://127.0.0.1:9998/Services/svcGlobalUpdate.asmx>

There are three (3) functions for this service. These services allow server administrator to set/update settings for every domain on the server using SOAP, an HTTP GET command, or an HTTP POST command. The functions, and their corresponding properties, are:

- `UpdateAllDomainSettings` - sets the supplied fields and values for all domains on the server.
- `ListGlobalUpdateFields` - lists all the fields that can be updated using `UpdateAllDomainSettings`.
- `GetGlobalUpdateStatus` - gets the current status of the update (ex. 550 of 1335 domains updated).

## Domain Alias Administration

<http://127.0.0.1:9998/Services/svcDomainAliasAdmin.asmx>

There are four (4) functions for this service. These services allow server administrator to add/remove and check domain aliases for a given domain using SOAP, an HTTP GET command, or an HTTP POST command. The functions, and their corresponding properties, are:

- `DeleteDomainAlias` - deletes the specified domain alias.
- `GetAliases` - returns all domain aliases that belong to the specified domain .
- `AddDomainAlias` - creates a new domain alias and adds it to the specified domain.
- `AddDomainAliasWithoutMxCheck` - creates a new domain alias and adds it to the specified domain without doing an MX lookup on the new alias.

## User Administration

<http://127.0.0.1:9998/Services/svcUserAdmin.asmx>

There are twelve (12) functions of this service available for customization. These services allow developers and/or Administrators to dynamically create or delete users, return user statistics, return

user attributes, update user information and more using SOAP, an HTTP GET command, or an HTTP POST command. The functions, and their corresponding properties, are:

- AddUser - creates a new user and adds them to the specified domain.
- GetUserStats - returns statistics of the specified user for the specified time period.
- GetUser - returns attributes of the specified user.
- UpdateUserAutoResponseInfo - updates the specified user's auto response settings.
- UpdateUserForwardingInfo - updates the specified user's forwarding settings.
- GetUsers - returns attributes of each user in the specified domain.
- DeleteUser - deletes the specified user from the specified domain.
- GetUserAutoResponseInfo - returns the forwarding info of the specified user.
- GetUserForwardingInfo - returns the forwarding info of the specified user.
- AuthenticateUser - returns a response on whether the supplied user/domain/password is valid.
- LoginValidated - returns a LoginResult object with the LoginValidated field set to True if the specified username matches the specified password.

## 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, an Outgoing Gateway, and a 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**

- 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**

- 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.

## **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. A few examples are:

- 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 feels 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 mailing lists page at <http://www.smartertools.com/Pages/MailingLists.aspx> and

subscribe to the "Updates.SmarterMail" mailing list. 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. At the time 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 and (a) verify that the email account exists and (b) 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.

## **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.

## 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

It is also recommended that you update this setting in Default Domain Settings so that all new domains will require SMTP Authentication.

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.org/>.

## 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 dependant 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.

## Skinning Guide

SmarterMail allows you to customize its look and feel to suit your own needs. Instructions on skinning the web interface can be found below, as well as some notes that are important to understand.

## Skining Process

- Download the base skin module. [Click here to download](#)
- Extract the contents into a temporary folder.
- Modify the files using any of the common HTML / CSS editors on the market to adapt it to the look you want. Keep all tags that are surrounded by [brackets]. These are where controls will be added that contain the sidebar elements, body content, etc. For more details on each of the files and tags, see the section below.
- If desired, change any of the images in the Images directory.
- Edit the Skin.xml file with notepad or an XML editor and modify the following:
  - Title - Input the title of your skin.
  - Author - Input your name, or the name of your company.
- Save all files and make a new zip archive that contains all of the files. The structure of the zip file needs to remain the same as the skinbase.zip file you downloaded.
- Log in to SmarterMail as the administrator.
- Upload your skin in Settings - Skins, which will make it available to select as an active skin.

## Restrictions

- The name of the product (SmarterMail) must remain visible in the skin. You may use a term like "Powered by", but the reference to SmarterMail must exist on the page.
- The [Copyright] tag must exist in the page, and must remain visible in the skin.

## Skin Files

- Skin.xml - This XML file establishes the general properties of the skin, most notably the author and name of the skin. In the event that you give your skin to others, this helps to identify who made the skin.
- Login.htm - The template used for the display of the login page.
- Plain.htm - The template for the inner frame where messages are viewed, as seen when reading a message.
- Standard.htm - The template that is seen most of the time in SmarterMail, with a sidebar and a top menu.
- SysAdmin.htm - The template seen by the system administrator, with a sidebar and a top menu..
- Calendar.css - This style sheet establishes the look and feel of the popup calendar.
- Layout.css - General layout styles are contained in this style sheet, including colors, etc. You may modify the styles, but do not delete any styles from this file to ensure proper operation of SmarterMail.

- LayoutPlain.css - Layout styles for the Plain.htm file are contained in this file. You may modify the styles, but do not delete any styles from this file to ensure proper operation of SmarterMail.
- Skin.css - Skin-specific styles reside in this file. You may alter it as you see fit.

## Bracket Tags

- [PAGETITLE] - Inserts the title of the page. This is most frequently used between <title> tags.
- [HEADITEMS] - Required placeholder for additional items that SmarterMail needs to add to each page. Must be contained withing <head> tags.
- [LOGGEDINAS] - Sidebar box for "Logged In As".
- [FOLDERLIST] - Sidebar box for the folder list, or the real time statistics if user is the system administrator.
- [SEARCHBAR] - Sidebar search box that allows searching of domains for system administrators or email messages for other users.
- [PRODUCTNAMEANDVERSION] - Text for "SmarterMail Professional Edition" + version. It is required to use this tag in the skin.
- [DOMAINTITLE] - The name of the domain that is logged in to.
- [TIPTTEXT] - Placeholder for where errors and messages will appear in response to actions.
- [BODY] - Placeholder for the main inner content of the page. This is the big white area in the default skin.
- [COPYRIGHT] - This field is also required to be included and visible in the skin. Displays the SmarterMail copyright.
- [FOOTERCONTENT] - Used by SmarterMail internally. This tag must remain in all files in which it appears.
- [MENU] - Placeholder for the main pull-down menu.

## 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. For this reason, SmarterTools recommends that you change the administrator login as the very first step when configuring SmarterMail.

### Instructions

- Log in as the administrator with the current login
- Go to the Settings -> General Settings page
- Click on the Administrator tab

- Enter a new username and password (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 at <http://support.smartertools.com/Custom/KBArticle.aspx?articleid=5> .