Additional Help Topics

Help Documentation

Additional Help Topics

Automating Login to SmarterMail

Companies using SmarterMail can easily automate user entry into the mail application by configuring the auto-login functionality. The HTML code shown below demonstrates how you can make a text link on a website (e.g. "Log into your mail") that automatically logs a user in to the SmarterMail site. By putting this hidden form on a simple web page, you can fill in the "Domain", "Email Address", and "Password" information by hard-coding the data or through a scripting language like ASP, ASP.Net, or ColdFusion. This implementation of auto-login works seamlessly across domains, so the two applications do not have to be hosted on the same server.

Some notes about the example code listed below:

We have the form values set to generic text (e.g. "USERNAME_GOES_HERE") to show where you would hard code values that are submitted to the login page. You could also dynamically generate these values using a scripting language like ASP or ColdFusion. A sample ASP script would substitute var domain = "USERNAME_GOES_HERE"; with var domain = "<% =email %>" .

The form action shown, https://DOMAIN_GOES_HERE , uses the default location of the Smartermail Web Interface. If you have created a separate web site 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. For example, a modified form action might take the format of https://mail.smartertools.com . In addition, this code assumes that your SmarterMail site is secured with SSL/TLS. If it is not, be sure to change the var domain URL from https to http.

Auto-Login Sample HTML Code

```
<!DOCTYPE html> <html> <head> <meta charset="utf-8"> <script> function autoLogin() { var domain = "https://DOMAIN_GOES_HERE"; var username = "USERNAME_GOES_HERE"; var password = "PASSWORD_GOES_HERE"; var xhr = new XMLHttpRequest(); xhr.open('POST', domain + '/api/v1/auth/authenticate-user'); xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8'); xhr.onload = function() { if (xhr.status === 200) { var success = JSON.parse(xhr.responseText); if (!success.success) { var res = ""; if(success.message) res = success.message else res = success.status document.getElementById("errors").innerText = res; return; } window.location.href = success.autoLoginUrl; } else { document.getElementById("errors").innerText = failure.message || failure; } }; xhr.send(JSON.stringify({ username: username, password: password,
```

```
retrieveAutoLoginToken: true })); } </script> </head> <body
onload="autoLogin()"> <div id="errors"></div> </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 Inbound Gateway, Outbound 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 outbound 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.

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. See more on the Backkup MX Servers page of Help.

Inbound 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.

Outbound 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.

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.

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):

• Log in to SmarterMail as a System Administrator.
• Click the Settings icon.
• Click on Bindings from the navigation pane on the left.
• 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 Antispam from the navigation pane on the left.
• Click on the IP Bypasses tab.
• Click New .
• Enter in the IP address of your backup MX server. Adjust the Bypass spam checks and Bypass greylisting options as necessary. If Bypass spam checks or Bypass greylisting are enabled, your primary SmarterMail server will perform IP based spam checks or greylisting against the original sending server and not the Backup MX.
• 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:

- Log in to SmarterMail as a System Administrator.
- Click the Settings icon.
- Click on Gateways / Failover from the navigation pane on the left.
- 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

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.

Major and minor SmarterMail version releases are announced on our social media pages as well as the News items on the Support Portal . Email notices are sent to SmarterMail customers who are subscribed to receive these notifications. You can manage your mailing list subscriptions at My Account .

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.
- Click on the Domains icon and edit the desired domain.
- Click on the Features tab.
- Uncheck Catch-All Alias .
- Click 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.
- Click on the Security icon .
- Click on Antispam Administration in the navigation pane and then the Options tab.
- Change Auto-Responders to either Disabled or Require message passed SPF .
- Change Content Filter Bouncing to either Disabled or Require message passed 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 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.
- Click on the Domains icon and edit the desired domain.
- Click on the Technical tab.
- Check 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.

Proper DNS Settings for Email

There are several major things to set up on your DNS server for every domain you set up within SmarterMail. How you set these up is dependent upon two things: who hosts your DNS and what DNS software is used. Therefore, you'll need to check with your DNS provider, or check your DNS server documentation, for instructions on how to set up the following records. NOTE: In the items below, simply 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.

General DNS Entries

There are several DNS entries that are required in order to run a mail server. These not only make the mail server visible to the world, but also can help ease the use of mail accounts by end users. Below, these are listed as well as their function.

- WebMail URL - In order to use a URL for allowing users to log in to their SmarterMail mailboxes, you'll need to add an A record for their domain. For example, "mail.example.com". This record will need to point to the IP address of the webmail interface for that domain.
- MX Record - This record should point to the A record you created. Again, "mail.example.com". This will allow other email servers to locate the mail server used for the domain.

• Reverse DNS Record - Add a reverse DNS record for any 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 Gmail and Yahoo! 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.

Optional, But Recommended DNS Entries

Autodiscover

Autodiscover is a way to allow users to quickly and easily set up accounts in email clients, both on desktop and mobile. Autodiscover is just that: a way for user settings to be discovered, automatically, by the email client. These settings include incoming/outgoing mail server info, ports used, etc. However, in order for autodiscover to work, it requires DNS entries.

To set up autodiscover in DNS, you need to add the following:

• A Record - This should be set to "autodiscover.example.com", and point to the IP address of that domain's mail server. (I.e, the IP assigned to the webmail URL.)
• SRV Record - This record returns the available domain and the service being used back to the client. The format for the SRV is "_autodiscover._tcp.example.com". Here's an example of the SRV for SmarterTools:

```
Domain: smartertools.com Service: _Autodiscover Protocol: _tcp Priority: 0 Weight: 0 Port: 443
```

In addition to the DNS settings, above, you will also want to create a host header for your autodiscover URL in IIS that's tied to the SmarterMail web interface for a domain. As an example, SmarterTools has an IIS binding to ports 80 and 443 for "autodiscover.smartertools.com". This is in addition to the bindings created for "mail.smartertools.com" as that URL is what we use for setting up our mail clients and for accessing the web interface.

NOTE: Not all devices and email clients handle autodiscover in the same way. Therefore, just because you set up autodiscover doesn't mean it will work for each user.

DKIM

Most major email providers require an additional layer of security before they'll accept incoming email. Free email providers like Gmail, Yahoo! and Outlook.com are using these "mail signing

protocols" as a way to further protect their users from unwanted email and phishing schemes. Therefore, having DKIM set up for your mail domains is a very, VERY good idea.

To set up DKIM, you'll first want to enable it for a domain within SmarterMail. This is handled on the Domain Admin side, so if you're logged in as a system administrator, you'll need to impersonate the Domain Admininstrator for any domain you set up with DKIM. Alternatively, you can Manage the domain as that automatically logs a system admin into a domain as the Domain Admininstrator.

Once you're managing the domain, go to the domain's Settings page. On the Email Signing card, click "Enable". A modal window opens up containing both a Text Record Name and a Text Record Value . BOTH of these need to be added as TXT records to the DNS for the domain in order for DKIM to work. You can simply copy/paste the values into whatever interface is used for DNS management. For example:

```
Host Name: 8D48750357DA749._domainKey.example.com Text:
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAk+caX2o1xAtkGdQSNrtNNhvNCpfbdXOVTmm+ol0E7
uKWYTqbFuyFEncusd1XGNQSC8Nzifn0qikrgSBG0xHUZJ+6GVcyQw42oRl7Kej1F8YY
bX4uHzLVv1uned2leDpSiSOLca2Q0arBtlyxzPNZ4P8YqujHydRsRwfJvYqvO9ge5eJFbEwCXq0d1bF8F

cCkm6gghYzQyaPPCpni8bu99uYwlqf7kJHEG4gH2YKhkYDgzg61+3wmu7gIv6ix3p5rBFmY6tC62d5p9Y8ZOyL1k
kFGMnvKc1CaxkTCoupBOflTOkDMzwht3RGClOk5DX3in6/80DQmwsFNfZkDa3QIDAQAB Time
to Live (TTL): 5 minutes
```

Once DKIM is set up for a domain in SmarterMail, the domain adminsitrator can modify the Settings and manage how closely the system monitors messages in transit. For more information, see the Settings page of SmarterMail help.

Changing the System Administrator Login

When installing SmarterMail for the first time, you will be required to create a System Admininstrator 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

- Login as the administrator with the current login.
- Click the Settings icon .
- Choose System Administrators in the navigation pane.
- Click on the Options tab and double-click on the Primary Administrator or right-click and choose Edit.
- Enter the current 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 Admininstrators the ability to impersonate users or Domain Administrators to accomplish these goals.

First things first: as a System Admininstrator, 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 Admininstrators 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 Admininstrator, it is definitely possible.

There are a couple of different ways to impersonate a user...

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 Admininstrator 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 Admin" type. Simply select that user then select Impersonat User by clicking on the Actions (...) button. A new browser tab will open up, and you'll be taken to that user's settings. From here, you can click the Domain Settings icon and see that all of that domain's settings. If you want to impersonate a specific user, you do the same: Select that user, then select the "Impersonate User" option from the Actions button.

If you're unsure which account is the Administrator for a domain, the best way to impersonate that Administrator is as follows:

Using Impersonate User

If you're sure of the account you want to impersonate -- that is, you have their username and domain -- you can simply go to the Manage area and select Impersonate User from the navigation pane. A modal window opens up and you can simply type their full email address (e.g., johnd@example.com) in the email address filed, then hit the Impersonate button. Alternatively, you cna select the domain name from the Domain dropdown, then type their username.

When impersonating using the Impersonate User options, SmarterMail will ensure the account you're typing in is an actual SmarterMail account before allowing you to impersonate it. So be sure to check your spelling when typing in the username or full email address.

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 he notices a lot of spam messages getting into his users' mailboxes that are failing a particular test, he may want to override a 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 noticed 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 thenew rule so that it has some affect on the final weight.