SmarterMail Lockdown Guide

This guide walks you through securing your server via SmarterMail installation by changing the user SmarterMail and IIS SmarterMail proxy site uses to run under, limiting access, protecting administrative accounts, and tightening key security settings.

Following the steps in this guide will help reduce the threat of a compromise within SmarterMail and if a compromise does occur, should limit the scope of the compromise to just the SmarterMail installation directories and not affect the rest of your system.

This guide has a video walk-through (below) that shows how you can accomplish each of these steps outlined in this guide.

COMING SOON!

Set SmarterMail and IIS SmarterMail Proxy Site to Run as Custom User

The goal for most attackers is to use SmarterMail as a means to gain access to their greater objective...your entire server. We recommend creating a custom Windows user that ONLY has access to the SmarterMail installation and data directory, which will prevent any access outside of these directories (prevent lateral compromises) if a compromise of SmarterMail were to occur.

Create a new windows user

Step 1: **Open** your Windows Administrative Tools, which you can access from within your Start Menu.

Step 2: **Double-click** on the "Computer Management" option listed under Administrative Tools.

Step 3: In the Computer Management window that opens, **expand** the "Local Users and Groups".

Step 4: **Right-click** on the "Users" folder and **select** the option for "New User".

Step 5: **Enter** the details of desired user that SmarterMail will run under, then **click** "Create" once satisfied.

- ***User name:*** this is the name of the user that we'll set SmarterMail and IIS proxy site to run as.
- ***Description:*** **give** the user a good description that lets you know what this user is intended for such as "Local Service User for SmarterMail".
- **Give** the user a good strong password. **Make note** of the password as we'll need it later on.
- **Uncheck** the option for "User must change password at next logon", then **enable** the option for "Password never expires".

Step 6: You can **close** the Computer Management window now, but **leave open** Administrative Tools for the next part below.

Give new user permission to logon as a service

After the user has been created, we need to tell the system that this user has permissions to run as a service.

Step 1: In the Windows Administrative Tools, **double-click** on the "Local Security Policy" option.

Step 2: **Expand** "Local Policies", then **select** "User Rights Assignment".

Step 3: **Scroll down** in the list until you find "Logon as a Service". **Right-click** this item and **choose** "Properties".

Step 4: **Click** on the "Add User or Group ..." option listed.

Step 5: **Enter** the name of the user you just created, then **click** "Check Names" and then "OK", then "OK" again.

Step 6: You can **close out** the Local Security Policy window now, but **leave open** the Administrative Tools.

Grant the New User Modify access to SmarterMail Files

In order for this user to have permissions to view and change files as needed by SmarterMail, we'll need to add this user to have "Read" and "Modify" permissions on the SmarterMail installation directory and the SmarterMail Data directory. Unless changed from the defaults, the two directories this needs to be done on are:

- C:\Program Files (x86)\SmarterTools\SmarterMail
- C:\SmarterMail

Open File Explorer on the server and perform the following on both the installation and data directory for SmarterMail.

Step 1: **Right-click** on the folder and **choose** "Properties".

Step 2: **Click** on the "Security" tab.

Step 3: **Click** "Edit".

Step 4: **Click** "Add".

Step 5: **Enter** the name of the user you created, then **click** "Check Names", and then "OK".

Step 6: **Check the box** for "Modify", while leaving the other permissions for the user enabled as they should be by default.

Step 7: **Click** the "Apply" button to apply the changes. Then **click** "OK" to close the dialog box.

Set SmarterMail to use the new user

Now that the user has been created, has permissions to the files, and ability to run as a service, we need to change SmarterMail to actually run as the new user.

Step 1: In Windows Administrative Tools, **double-click** on the "Services" option.

Step 2: Find the SmarterMail service in the list of services, then make sure the service is stopped. If it is running, then **click** the stop button to stop the service.

Step 3: **Right-click** on the SmarterMail service, then **choose** "Properties".

Step 4: **Click** on the "Log On" tab.

Step 5: **Click** on "Browse", then **enter** the name of your user and **click** "Check Names", then "OK".

Step 6: Although a password appears to be set, it is not the correct password. **Change** the password to the correct password that you set earlier for the user.

Step 7: **Click** "Apply" to save your changes, then **click** "OK".

Step 8: You can now **start** the SmarterMail service. If it fails, please make sure you followed the steps in above sections.

Set IIS proxy site for SmarterMail to use the new user

Having the SmarterMail service run as the new user secures the service part of SmarterMail, but for visitors accessing the webmail via the IIS proxy site in SmarterMail, this is still using a built-in user that we recommend changing to the new user you created earlier. After this change, any files that get executed within the IIS proxy site (your users webmail, for example) will run as the custom user, instead of the built-in user that has permissions to other systems on the server.

Step 1: In Windows Administrative Tools, **double-click** on the "Internet Information Services (IIS) Manager".

Step 2: **Expand** the server node, then **click** on "Sites". **Find** the site related to SmarterMail, then **right-click** and **choose** "Basic Settings".

Step 3: In the Basic Settings window, you should see the application pool SmarterMail website is using. **Close out** of the dialog and **click on** Application Pools now.

Step 4: **Find** the Application pool SmarterMail is using and **select** it. **Click** on the "Advanced Settings" on the actions pane.

Step 5: **Click into** the "Identity" field, then **click** the "**...**" (ellipsis) that follows.

Step 6: In the dialog that appears, **select the option** for "Custom Account".

Step 7: **Click on** "Set..." and then **enter the name** of the user you created and **enter the password**. Then **click** "OK" each time **(3 total times)**.

Step 8: **Test** that the webmail is still working properly now that IIS SmarterMail proxy site is using the custom user.

Restricting the Webmail to Specific IPs

Step 1: **Open** the IIS Manager that we used earlier in the guide, which you can find in the Windows Administrative tools, if needed.

Step 2: **Expand** the server node, then **click** on "Sites". Find the SmarterMail site in the list of websites and **double-click** it to go into the site settings.

Step 3: **Double-click** the "IP Address and Domain Restrictions" option, which is what allows IIS to restrict by IP.

- If you do not see this option, then install the "IP Address and Domain Restrictions" feature within the Server Manager > Add Roles and Features. ***See video guide for help on that.***

Step 4: Here you can use the following options from the actions pane:

- The ***"Add IP Address..."*** option will allow you to add an IP address to the allowed list, even if the default setting for access is set to Deny.
- The ***"Deny Entry..."*** option will allow you to add an IP to the blocked list, so they cannot gain access even if the default setting for access is Allow.
- The ***"Edit Feature Setting..."*** option allows you to change default access to either be allowed or denied.
- The ***"Dynamic Restriction Settings..."*** allows you to set rate limits for when an IP is making too many connections.

Note: If setting a default DENY rule here or using dynamic restriction (rate limiting), then we recommend making sure that all IP addresses expected to hit the IIS proxy site are added to the whitelist. If using protocols like EAS or MAPI for example, for added email client functionality, these rely heavily on HTTP protocol and your email clients may experience issues if blocked.

Disabling bindings or ports for webmail

Sometimes you may want to change what IP/Hostname can access webmail and over what port. For example, the initial installation of SmarterMail will default an initial configuration of any IP/Hostname can connect over port 9998. Since this 9998 port is known to be used for SmarterMail installations, it is common to see attackers scan servers to see what servers have this port open and respond with SmarterMail HTTP headers. This lets the attacker know they can try to find exploits on your SmarterMail server via webmail.

To change the bindings for the SmarterMail proxy site, follow the steps below:

Step 1: **Open** the IIS Manager, which you can do via the Windows Administrative tools.

Step 2: **Expand** the server node, then **click** on "Sites".

Step 3: **Find** the site related to SmarterMail and **select** it. Then on the right-hand side actions pane, **click** "Edit Bindings...".

Step 4: **Review** each entry in the bindings to see what is currently allowed. You can add, edit, or remove bindings here according to what setup you want. The bindings work as follows:

- ***Type:*** this is the protocol for the binding like "HTTP" or "HTTPS". This tells the webserver what type of traffic to listen for.
- ***Hostname:*** this can be a fully qualified domain name (FQDN) or left empty to match any domain (catch-all).
- ***Port:*** this is the port that the HTTP or HTTP (depending on what you choose on type) listener is bound to, listening for requests.
- ***IP address:*** this is the IP that resides locally on the server that should be listening for these types of requests. Use * for any IP on the server. If you only want the binding to be allowed locally you could choose 127.0.0.1 for example.

Note: You can also use the Windows firewall to restrict what ports are available as well, such as the 9998 port.

Locking down SmarterMail Administrator Users

Since the SmarterMail Administrator users use the exact same webmail interface as the normal users, which often needs to be left publicly accessible, this means that the administrator users can be brute forced and potentially accessed if they obtain the correct credentials. Due to this, we recommend locking the administrator users down to requiring two-factor authentication and IP restrictions, if possible.

Enable 2FA on Administrator Users

We recommend enabling two-factor authentication (2FA) for all administrator users. When 2FA is enabled, anytime a user attempts to login as the administrator user with 2FA enabled, it will require a time-based one-time password (TOTP) code, which is a 6-digit code provided in the users authenticator app.

You can use any authenticator app that supports TOTP codes. A popular choice is the Google Authenticator app available on your mobile device. A lot of password managers support enabling TOTP codes as well, if you want to keep your TOTP and the password for the user in one-place. Below are the steps to enable 2FA for your administrator user(s).

Step 1: **Login** to your SmarterMail administrator user.

Step 2: **Click** on the "Settings" tab, then **go to** "Administrators".

Step 3: **Find** and **click** the administrator user you want to setup 2FA for, then **go into** the settings for that user.

Step 4: Under the "Two-Factor Authentication" section, **click** on the "Enable" button.

Step 5: SmarterMail will prompt for the verification method. **Choose** "Authentication App", then **click** "Next".

Step 6: Within your authenticator app of your choice, **scan** the QR code presented on the screen now. Once scanned it will provide a 6 digit code that you need to **enter** in the "Verification Code" field back on the SmarterMail webmail page. **Click** "Check" once you enter the code.

Note: The 6-digit codes are time based, meaning they are only valid for 30 seconds at a time. Be quick to set this up and if needed, wait until the code refreshes if it is about to expire within a matter of seconds and you feel you may not be quick enough to type it out.

Step 7: If successful, the two-factor authentication should show that it is enabled now on the page. You will need to use your authenticator app to get the necessary code to enter and finish the login process every time you login.

Important: If you lose your authenticator app or ability to access the code, the user can be set back manually to not have the code. This setting can be changed by removing the 2FA properties of the administrator.json file found in the SmarterMail service installation directory, then restarting SmarterMail after the change. Be careful when doing this not to break the syntax of the json file or accidently change the password hash or other settings within the file.

Enable IP Restrictions on Administrator Users

Restricting what IP address(es) are allowed to even try logging into an administrator user is a great idea. If you do not have a static IP then you could either restrict access to 127.0.0.1 (local server access only) or connect to a VPN service that provides access to a static IP. We do offer Sophos Firewalls that allow you to connect to an SSL VPN and therefore have an IP within the SSL VPN IP range, which can be set in the restrictions for SmarterMail. If interested, please contact our Sales team for a quote.

The steps to enable IP restrictions for administrator users in SmarterMail are listed below:

Step 1: **Login** to your SmarterMail Administrator user.

Step 2: **Click** on the "Settings" tab, then **go to** "Administrators".

Step 3: **Find** and **click** into the administrator user you want to add IP restrictions for.

Step 4: Under the main options section, **enable** the option for "Restrict login access by IP".

Step 5: Once that option is enabled, the IP Restrictions section will become available. **Click** the "New Rule" to add a new IP.

Step 6: **Enter** the IP address (or IP range) you want to add allow entry for. We also recommend giving it a descriptive name so you remember what that IP belongs to (such as "Main Office"). **Click** the "OK" button to save the IP.

Step 7: Once done, be sure to **click** the "Save" button to save your changes. Then **test** to make sure you are able to access properly from your IP.

Enhancing the IDS Protection Rules

SmarterMail has built-in IDS (intrusion detection system) features that detect malicious actors trying to brute-force their way into users, trying to send email on behalf of your users, or even users not on the system, as well as DOS and DDOS based attacks. The default rules in place for IDS protection are very relaxed and need some fine-tuning to make sure that it blocks IPs that are causing harm to the servers performance and security. The steps to add or update existing IDS rules are below:

Step 1: **Login** to your SmarterMail Administrator user.

Step 2: **Click** on the "Settings" tab, then **go to** "Security".

Step 3: Under the "IDS Rules" page, you should see a list of IDS protection rules. **Click** "New" to add a new rule, or **click** an existing rule to modify the rule.

It is important to understand the Time Frame, Threshold and Block Time configurable columns. Explanations of each are below:

Time Frame: the amount of time of which the requested action type will look for events under. For example, a rule for 15 login failures within 30 minute period, the 30 minutes would be the time frame.

Threshold: the amount of times the specific event must occur within the time frame. For example, a rule for 15 login failures within 30 minute period, the 15 login failures is the threshold.

Block Time: the amount of time (in minutes) that the IP address that offended this rule should be blocked. After the allotted time period the IP will automatically be unblocked.

One of the rules we recommend modifying to enhance security and performance is the "Password Brute Force by IP" rule. We recommend setting this rule to something like 5 failures (threshold) within 30 minutes (timeframe) and block for 1440 (equivalent of 1 day).

Important: If a legitimate user fails login attempts and gets themselves automatically blocked by IDS, you can search for their IP and remove the block at any time. This can be done within the SmarterMail interface (Settings > Manage > IDS Blocks) by removing the IP from the block list. If needed, you can also whitelist the IP (Settings > Security > Whitelist) and choose the option for "Bypass IDS Brute Force" when whitelisting the IP to make sure it does not get blocked again.

Restricting the Uploadable File Extensions

It is very important to restrict what kind of files SmarterMail is able to create. SmarterMail has a few extensions that are blocked by default that are not typically used in email transactions and that could be harmful to your server if uploaded. As an example as to why this is important, a recent critical vulnerability exploit (CVE) was released that allowed attackers to reset the password for administrator users (has since been patched) that allowed the attacker to impersonate users webmail and use the file upload capabilities to upload bad .aspx files to servers. They then accessed these files via the webmail and used them to manipulate services on the server and upload files anywhere on the server they desired. Changing the user SmarterMail and IIS proxy site SmarterMail uses helps prevent these types of compromises from spreading, so be sure to read the above sections on how to do that as well.

The steps to add/remove file extensions to the blocked list are below:

Step 1: **Login** to your SmarterMail Administrator user.

Step 2: **Click** on the "Settings" tab, then go to "General".

Step 3: Under the "File System" section, you can **click** on the appropriate extension blacklist. The options are as follows:

- ***Inbound Extension Blacklist*** - prevents undesired attachments from being sent to users on the server, that have extensions in this list.
- ***Outbound Extension Blacklist*** - prevents any users on your server from sending undesired attachments that have extensions in this list.
- ***Extension Blacklist for Uploads*** - prevents any user from uploading file extensions to the server, such as through webmail.
- ***File System Restrictions*** - prevents SmarterMail from creating certain files on the system, regardless of how (Webmail, SMPT, etc.)

Step 4: Once you have selected your desired extension blacklist, you will see a list of existing extensions. **Add** or **remove** from the list accordingly and then **click** "OK" to save.

Disable SMTP Open Relay

If your SmarterMail server is configured to be an open relay, then anyone will be able to send email from your server even if they do not authenticate with user/password credentials. This can lead to bad IP or domain reputation due to spam being sent from your server, as well as slow down the mail processing due to large amounts of spam being in the mail queues.

To disable open relay in SmarterMail follow these steps:

Step 1: **Login** to your SmarterMail Administrator user.

Step 2: **Click** on the "Settings" tab, then **go to** "SMTP In".

Step 3: Under the "Connection and Session Settings" section, make sure sure that "Allow Relay" is set to Nobody. The options are as follows:

- ***Nobody (recommended):*** does not allow anyone to send email unless they authenticate with username/password or have their IP whitelisted in SMTP Auth Bypass (we'll go over this below).
- ***Only Local Users:*** allows anyone to send emails from users that exist on the server, even if they do not use SMTP auth (user/pass).
- ***Only Local Domains:*** allows anyone to send from any domains that exist on the server, even if they do not use SMTP auth (user/pass).
- ***Anyone:*** allows anyone to send email from your server, from any domain and without SMTP auth (user/pass).

Important: We'll highly recommend using the "Nobody" option to prevent undesired spam being sent from your server.

Step 4: After setting the option to "Nobody", be sure to **click** the "Save" button to save your changes.

Allowing specific IPs to still relay emails with SMTP Relay set to Nobody

It is very common for websites or applications hosted on your server(s) to send email, such as through a "contact us" form on your website. In the event you need to send emails from your server and have SMTP relay set to be disabled, you will either need to authenticate your web forms with a username /password, or you will need to tell SmarterMail that for the IP address making the connection from that website/application to bypass SMTP authenticate requirements.

To allow specific IP address(es) to relay email from your SmarterMail server, follow these steps:

Step 1: **Login** to your SmarterMail Administrator user.

Step 2: **Click** on the "Settings" tab, then **go to** "Security".

Step 3: Under the Security page, **click** on the "Whitelist" tab.

Step 4: You should see a list of IP addresses here. If your IP already exists, **select** it. Otherwise **click** "New".

Step 5: You should be prompted to enter the IP address the whitelist rule is for. **Enter** that now. Also, be sure to **select** the "Bypass SMTP Authentication" option listed here to allow this IP to relay emails without requiring authentication. You may also want to **choose** the option to bypass spam checks so your outgoing emails from these IP address(es) are not filtered such as for reverse DNS lookups.

Step 6: **Click** "Save" to save the whitelist rule. Then **test** your website/application mail functionality to ensure you are now able to send email without SMTP authentication.

- If needed you can view logs via SmarterMail interface (Manage > Troubleshooting > View Logs) to see if any errors are being thrown that may indicate what issues you are running into.

This guide is meant to help increase the security of your SmarterMail server and give you the steps to accomplish this task yourself. However, if you prefer to have our Vivio SysOps team assist with this process for any or all steps covered in this guide reach out and we will be happy to help!

Related articles

- SmarterMail Lockdown Guide

- SSL Certificate Validity Changes
- Software End of Life Dates
- How to Grant Vivio Access to Your Cloudflare Account
- How to Restart Lucee on Windows and Linux