



ExchangeDefender™

Domain Guide

For the latest version of this document please go to:
<http://www.exchangedefender.com/docs>

v 1.0

May 16, 2011
Audience: Staff

Table of Contents

ExchangeDefender Overview.....	3
ExchangeDefender Admin Site.....	4
Logging in.....	4
Password Reminders.....	4
Dashboard Overview.....	5
Creating new users.....	6
Managing User Accounts.....	7
Individual management options.....	8
Spam Czar	9
Configuration Options.....	10
Policies.....	11
Branding.....	12
Black/White Listing policies.....	13
Encryption Policies.....	14
Web Sharing Management.....	15
Web Filter Management.....	16
General Settings.....	17
Technical Help & Account Management.....	18
General Security Tips.....	18

ExchangeDefender Overview

The ExchangeDefender Domain Admin Site is a powerful tool that gives you management access to all of the benefits ExchangeDefender has to offer, from the safety and convenience of your web browser. This guide will familiarize you with our web site and offer helpful tips on how to manage your ExchangeDefender service for your domain.

ExchangeDefender is a cloud-based productivity suite that delivers security, business continuity, regulatory compliance and business information management tools. ExchangeDefender technology provides the following benefits: SPAM filtering, virus filtering, malware protection, DDoS protection, business continuity, Outlook integration, email SPAM quarantine reports, transparent and regulatory encryption, web filtering, desktop alerts, SMTP service monitoring and managed services, Exchange 2010 archive access, long term compliance archiving, HTML5 mobile application and so much more. The wide range of solutions in our portfolio is tightly integrated to give users a seamless experience, access different tasks, and be flexible enough for the unique way in which each company implements ExchangeDefender.

ExchangeDefender guides are intended to introduce basic service concepts and offer productivity tips that our customers have previously shared with us. If you have any suggestions or questions please don't hesitate to contact us.

ExchangeDefender Admin Web Site

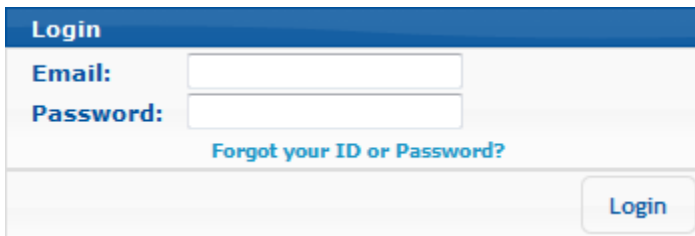
To manage your ExchangeDefender service simply open a browser and point it to:

<https://admin.exchangedefender.com>

This secure website is protected using the same level of encryption that your bank, credit card, and ecommerce sites rely on.

Logging In

Your ExchangeDefender domain level login credentials should have been emailed to you by your IT Solution Provider when your organization was protected by ExchangeDefender. Simply type in your domain name and your password to login.



The screenshot shows a login form with a blue header labeled "Login". Below the header, there are two input fields: "Email:" and "Password:". Below the "Password:" field, there is a link that says "Forgot your ID or Password?". At the bottom right of the form, there is a "Login" button.

If you encounter issues with your login credentials you can always request to have them emailed to you.

Password Reminders

To request a login credential reminder please click on Forgot your ID or Password? Link at <https://admin.exchangedefender.com>

Provide your domain name and the system will email the administrator address on record the login credentials to access the site.

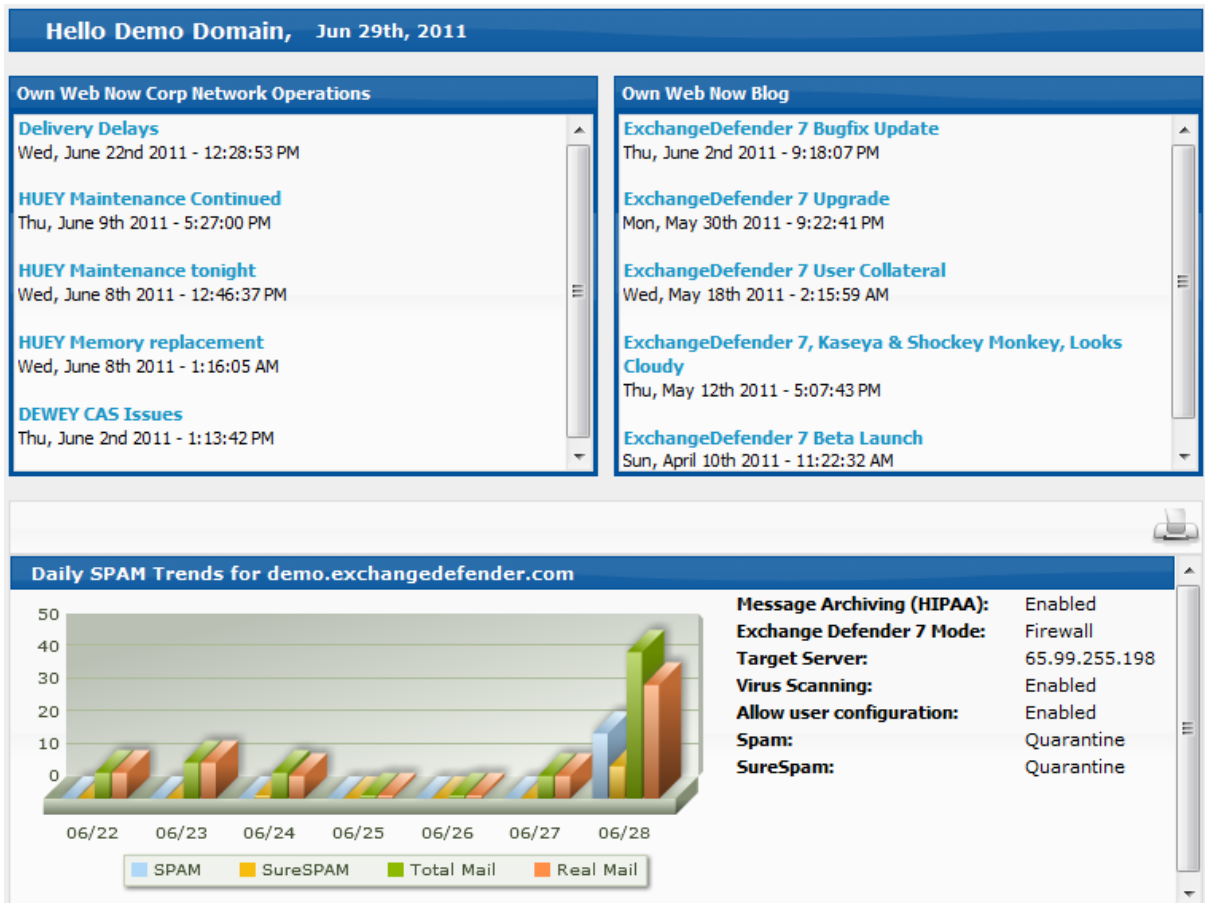
If your email address is not protected by ExchangeDefender you will have to contact your IT Solution Provider for further assistance. For security reasons, passwords cannot be emailed to a different address or reset without access to your mailbox.

Dashboard Overview

ExchangeDefender dashboard is the home screen for all ExchangeDefender applications. Based on the AJAX technology, the web site responds and behaves more like a desktop application and provides smooth transitions and faster load times.



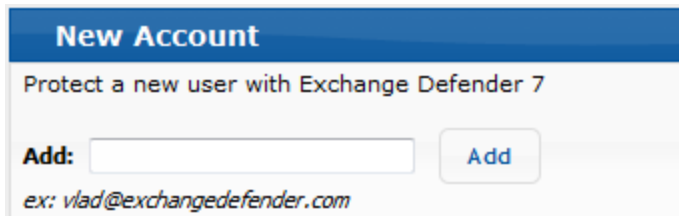
Across the top of the site you will see the navigation menu. You can access all the sections of the ExchangeDefender domain management from the navigation menu. On the left, you will see context navigation menus that will lead you to more advanced settings depending on what you are currently doing. Finally, the main section of the page takes up the majority of the web site and presents the most relevant data.



The dashboard section will offer your network operations alerts, product updates, a quick overview of the domain's SPAM statistics, and important domain level settings.

Creating New Accounts

In order to create a new account the process is pretty simple, from the Welcome screen's *Dashboard*, fill out the form below with the new user's email address and click "Add":



New Account

Protect a new user with Exchange Defender 7

Add: **Add**

ex: vlad@exchangedefender.com

This form will submit that information to our new user Wizard and you'll be prompted for the following information to complete the wizard:

- First & Last Name – All reports for this account will be addressed to this name.
- Password – View or Update current ED password.
- SPAM Action – Action to take on items found to be 80% certain to be SPAM.
- SURESPAM Action – Action to take on items found to be 99% certain to be SPAM.
- Report Options – Set the e-mail report options for this account.
- Report Schedule – Set the arrival times for the reports set above.
- Timezone – Sets the Timezone for the Welcome Message
- Notification – Toggle that sends a new user a welcome message if selected.

Managing User Accounts

ExchangeDefender is a full compliance, accountability, and security suite. As such, it needs to have every user within a domain listed as a user or an alias in order to protect the domain in its entirety.

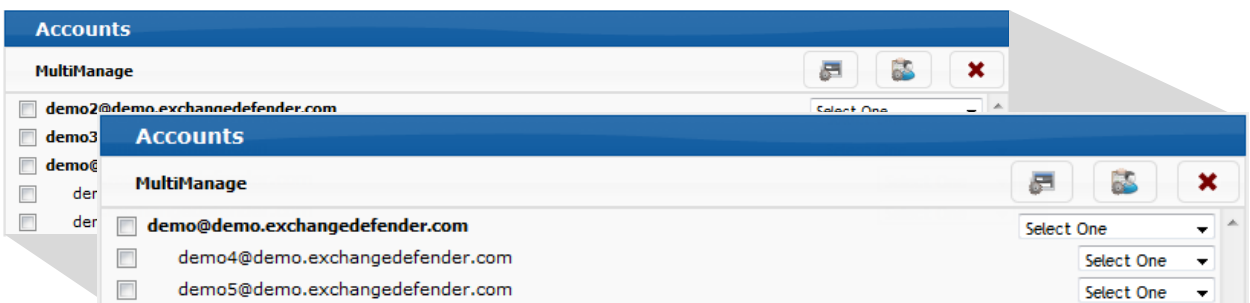
What happens if an address is not listed as a user or alias?

In order to completely protect your domain from SPAM, virus, trojans, DDoS attacks, ExchangeDefender will not accept mail for non-existent users by default. We recommend that mail-enabled public folders and distribution groups be listed as an alias for the person that manages that address on the client's site.

If you choose to have a distribution group address or mail-enabled folder maintain its own standalone Quarantine and e-mail Report, then you'd have to add that address as its own user.

Find Account	New Account
Which <i>e-mail</i> address are you looking for?	Protect a new user with Exchange Defender 7
Search: <input type="text"/> <input type="button" value="Find"/>	Add: <input type="text"/> <input type="button" value="Add"/>
<i>ex: vlad@exchangedefender.com</i>	<i>ex: vlad@exchangedefender.com</i>

There are two options above the account listing to assist you with account management. If you're looking to manage an individual account and you have a large user base the "Find Account" feature to truncate the user listing down to that address and its aliases.



The screenshot shows the 'Accounts' management interface. It features a 'MultiManage' toolbar with icons for account management. Below the toolbar is a list of accounts, including 'demo2@demo.exchangedefender.com', 'demo3', 'demo6', 'der', and 'demo@demo.exchangedefender.com'. Each account entry has a checkbox and a 'Select One' dropdown menu. The interface is designed for efficient account management in a large user base.

Once you've located the account you were planning on managing you'll be presented with the following management options:

- Modify Account
- Manage Account
- Delete
- Change Password
- Resend SPAM Report
- Resend Password
- Resend Welcome
- Add Alias

Modify Account

This menu selection will load up all the user account level options for the selected mailbox without having to log into the user's account to make modifications. These settings include the following:

Password – View or Update current ED password.
Domain Admin – Grant this individual User Domain Administrator Access.
SPAM Action – Action to take on items found to be 80% certain to be SPAM.
SURESPAM Action – Action to take on items found to be 99% certain to be SPAM.
LiveArchive – Enable/Disable LiveArchive
Report Options – Set the e-mail report options for this account.
Report Schedule – Set the arrival times for the reports set above.
Timezone – Sets the timezone for the user.

Manage Account

This selection will log into ExchangeDefender as the selected user which will allow you to control all of the above options and allow you to actually manage that individual user's SPAM quarantines and emulate the entire end user experience.

Other Options

The remaining options within this menu are self explanatory:

Delete – Deletes the account and aliases from ExchangeDefender.
Change Password – Changes the user's password to ExchangeDefender.
Resend SPAM Report – On Demand SPAM Report generation
Resend Password – Resends the user's password to their address on file.
Resend Welcome – Resends all new user information to their address on file.
Add Alias – Allows you to add an alias to the user.

SPAM Czar

The ExchangeDefender SPAM Czar allows a domain administrator to review all SPAM items for a domain. This feature is ideal for organizations that would need to ensure that SPAM is being reviewed by their users in a timely fashion or an employee is out of the office and you need to search for a specific e-mail to that user that may have been marked as SPAM.

The SPAM Czar search criteria are listed below:

Search

Domain Name:	<input type="text" value="demo.exchangedefender.com"/>	<i>Note: SPAM Czar is a limited-privilege account allowing an individual or team to manage entire organization's SPAM, blacklists and whitelists without having any higher level administrative access to settings, archives, passwords or accounts.</i>
From:	<input type="text" value="ilovespam.com"/>	
To:	<input type="text"/>	
Subject:	<input type="text"/>	

Which will yield all SPAM sent by ilovespam.com:

Results

	From	Subject	Received
<input type="checkbox"/>	address0@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address8@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address5@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address3@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address2@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address4@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address7@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM
<input type="checkbox"/>	address9@ilovespam.com	ExchangeDefender SURESPAM Test	6/28 - 08:30 PM

You'll have the ability to preview messages, preview the sender details, release, and trust that sender to that specific user (*not the entire domain*).

Note: SPAM Czar is a SPAM search not a quarantine search. Therefore, if a message is found and cannot be released most likely it means that the message was already delivered or destroyed. At this point you'd need to contact your IT Service Provider as they'd have the functionality to research where that email is, including the SPAM Action taken at the time of receipt.

Configuration Options

As a complex security, accountability, and compliance suite, ExchangeDefender's configuration is in depth and thorough. The configuration categories include the following:

- **Policies** - Various configurations that ExchangeDefender relies on to deliver and process mail for your client.
- **Branding** - Creates a domain level branded experience for the domain or matches it to the Service Provider branding.
- **Lists** - Allows the administrator to set blacklists and whitelists that affect both user and the entire domain.
- **Attachments** - If your business transacts with certain unique file extensions often you can set policies to account for that.
- **Encryption** - In addition to on demand encryption, this setting can encrypt messages at a policy level.
- **Web Sharing** - These policies set the guidelines for all of the libraries that can be created via the Web Sharing portal.
- **Web Filter** - All the domain level filtering settings and downloads are available here.



Configuration Policies

These settings greatly impact mail flow and performance and should only be changed by advanced and authorized users. Below you will find a brief description of the various settings:

Domains: Lists the domain(s) that will be affected by these settings.

Password: The domain level password for the current domain.

Administrator: This becomes our contact point at the domain.

Inbound IP Address: This is the address we will deliver this domain's email to.

Multihomed MX Record: ExchangeDefender can also deliver mail to a properly configured MX record

Outbound IP Address: This the address that your email server sends from.

Extra IP Address: We can accommodate your failover IP in this field.

Disaster Recovery - FailPOP: Enable POP3/IMAP+SSL business continuity service. Please review the feature closely before enabling this feature.

Migration Split MX: - This service is only available to new ExchangeDefender Hosted Exchange customers. It will deliver mail to the old email provider and our new Hosted Exchange environment for this domain.

SPAM Life: Number of days spam is to remain active in the quarantine.

- 7 Days, 14 Days, 24 Days, 30 Days

SPAM Action: Default action when Exchange Defender 7 encounters SPAM:

- Tag & Deliver, Quarantine, Delete

SURESPAM Action: Default action when Exchange Defender 7 encounters SureSPAM:

- Tag & Deliver, Quarantine, Delete

Report Options: When Exchange Defender 7 is set to quarantine SPAM or SureSPAM messages you can send the user daily and/or intraday SPAM quarantine reports to show them what Exchange Defender 7 intercepted.

- Disable e-mail reports, Enable daily e-mail report, Enable daily and intraday e-mail reports

Report Schedule: Allows you to set the generation time of the reports you enabled above.

Report Contents: Should we report empty quarantines or not.

Time zone: Establish the time zone for your domain in order to receive reports when expected.

LiveArchive: This settings toggles LiveArchive On or Off

Text Signature: This will be appended to all emails from your domain encoded in plain text.

HTML Signature: This will be appended to all emails from your domain encoded in HTML.

Branding

We understand that delivering a unique and branded experience can be important to every company. As such, we've given full control to the UI's Log and color schemes to your domain administrator. Some clients wish to only view their own branding and list it as a product requirement, you can now deliver this via ExchangeDefender.

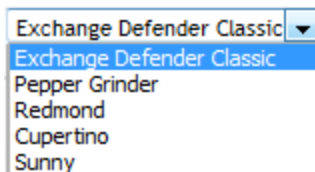
Domain Branding: This setting will tell ExchangeDefender whether they should load your IT Service Provider color scheme and logo or your domain's branding as designed below.

By enabling **Domain Branding**, you can override the (*Logo, Theme, Background Color*) for all users within this domain.

- Enable
- Disable

Logo: This section allows you upload the logo to be used for the domain level branding.

Scheme: This setting offers various color "Themes" to match with your uploaded logo.

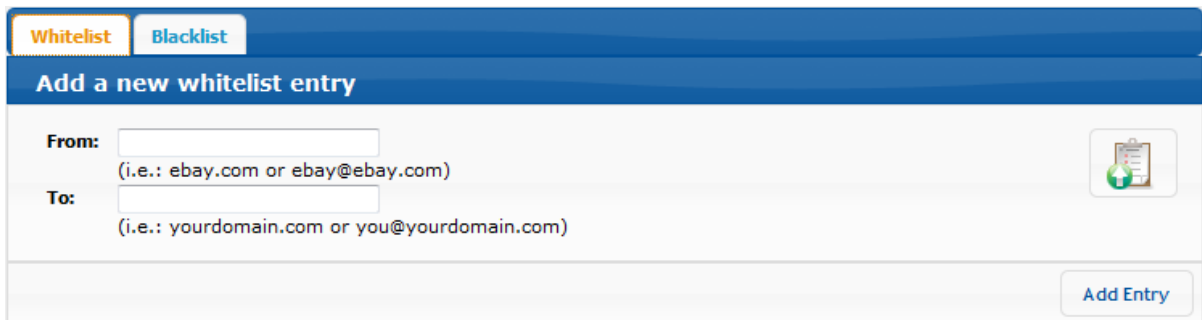


Background Color: Based on the color picker you can set back drop, for your theme and logo.



Managing Whitelists & Blacklists

ExchangeDefender allows you to manage your own whitelist of email senders that you never want screened for SPAM content as well as automatically quarantine addresses that you have known to be SPAM. ExchangeDefender constantly learns from your usage patterns and adjusts the SPAM scores for your individual users so this function should be used only when you are certain you wish to trust this sender.



The screenshot shows the ExchangeDefender interface with the 'Whitelist' tab selected. Below the tab is a form titled 'Add a new whitelist entry'. The form has two input fields: 'From:' and 'To:'. The 'From:' field has a placeholder '(i.e.: ebay.com or ebay@ebay.com)' and a clipboard icon to its right. The 'To:' field has a placeholder '(i.e.: yourdomain.com or you@yourdomain.com)'. At the bottom right of the form is an 'Add Entry' button.

For here you can scope a whitelist to the entire domain or to a specific user. In addition, you can white list IP addresses via the following format:

```
xxx.xxx.xxx.xxx  
xxx.xxx.xxx
```

The clipboard icon will allow you to do a mass upload if you had an existing whitelist file for your domain.



Each value needs to be separated by a comma, line breaks are not necessary in this file format (CSV).

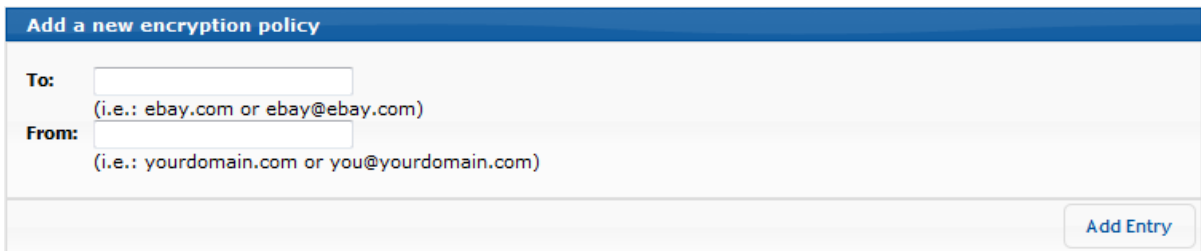
Currently, we do not offer mass uploads of blacklists due to the possible impact on mail flow. If your deployment is about 50 users or larger we may be able to help deploy that blacklist for you.

Note: These changes will take up to 2 hrs for propagation across the entire ExchangeDefender network.

Encryption Policies

ExchangeDefender features a built-in encryption solution that can satisfy many government and regulatory compliance requirements for data security. Compliant with such standards as FINRA, SOX, SEC and HIPAA, ExchangeDefender Encryption meets or exceeds business encryption needs with the unparalleled ease of use.

In addition to the on demand encryption discussed in our User Guides, a domain administrator can set encryption policies for their domain(s).



As illustrated above, the domain administrator can create an encryption rules to encrypt all from either an individual or a domain, to any individual address or domain.

Once these rules are set the On Demand [ENCRYPT] and [CLEARENCRYPT] are no longer necessary to encrypt mail flow on emails that fall under the rules created above. These rules only affect outbound mail.

Note: These changes will take up to 2 hrs for propagation across the entire ExchangeDefender network.

Web Sharing

ExchangeDefender Web File Sharing enables you to send files or sets of files to a large number of recipients without worrying about slowing down your email or if the message with your attachments will get there. Web File Sharing was designed to overcome the following limitations:

- Send large attachments or attachments to a large number of people.
- Send items with a password protection.
- Keep an audit trail of who received the attachment and when.
- Allow remote users/contractors/clients to upload attachments
- A system that doesn't require an administrator to manage permissions, settings or quotas.

This portion of the control panel allows the administrator to set the file thresholds for the web sharing to ensure that inappropriate content is not being shared through this system, you can see the restrictions under the following criteria:

- Allowed/Blocked File types
- File Quota
- Storage Quota
- Public Access
- Turn the feature entirely on/off



The screenshot shows the 'Allowed' tab of the 'Blocked' section in the ExchangeDefender control panel. It features a table with columns for 'Extension' and 'Action'. Below the table is an 'Add Entry' button. The 'Options' section includes fields for 'File Quota' (50 MB) and 'Storage Quota' (200 MB), radio buttons for 'Web Sharing' and 'Public Upload' (both set to 'Enable'), and a URL field with the value 'https://webshare.exchangedefender.com/upload/demo.exchangedefender.com'. An 'Update' button is located at the bottom right.

Extension	Action
-----------	--------

Extension: Add Entry

Options

File Quota: MB

Storage Quota: MB

Web Sharing: Enable Disable

Public Upload: Enable Disable

URL: <https://webshare.exchangedefender.com/upload/demo.exchangedefender.com>

Update

Web Filtering

In order to increase the productivity and accountability for your company, ExchangeDefender offers a client based Web Filtering application. Once installed, this application blocks access to the defined websites based on the registered user's settings in this section of our platform.

Web Filter - Manage Domain Rules

<input type="checkbox"/> Ads	<input type="checkbox"/> Clothing	<input type="checkbox"/> Gardening	<input type="checkbox"/> Manga	<input type="checkbox"/> Ring Tones
<input type="checkbox"/> Aggressive	<input type="checkbox"/> Culinary	<input type="checkbox"/> Government	<input type="checkbox"/> Medical	<input type="checkbox"/> Search Engines
<input type="checkbox"/> Anti Spyware	<input type="checkbox"/> Dating	<input type="checkbox"/> Guns	<input type="checkbox"/> Naturism	<input type="checkbox"/> Shopping
<input type="checkbox"/> Art Nudes	<input type="checkbox"/> Desktop Sillies	<input type="checkbox"/> Hacking	<input type="checkbox"/> News	<input type="checkbox"/> Social Networking
<input type="checkbox"/> Banking	<input type="checkbox"/> Dialers	<input type="checkbox"/> Home Repair	<input type="checkbox"/> Online Auctions	<input type="checkbox"/> Sports
<input type="checkbox"/> Beer & Liquor	<input type="checkbox"/> Drugs	<input type="checkbox"/> Humor	<input type="checkbox"/> Online Games	<input type="checkbox"/> Spyware
<input type="checkbox"/> Blogs	<input type="checkbox"/> Ecommerce	<input type="checkbox"/> Hygiene	<input type="checkbox"/> Pets	<input type="checkbox"/> Vacations
<input type="checkbox"/> Books	<input type="checkbox"/> Entertainment	<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Phishing	<input type="checkbox"/> Violence
<input type="checkbox"/> Celebrities	<input type="checkbox"/> File Hosting	<input type="checkbox"/> Jewelry	<input type="checkbox"/> Porn	<input type="checkbox"/> Viruses
<input type="checkbox"/> Cell Phones	<input type="checkbox"/> File Sharing	<input type="checkbox"/> Job Searching	<input type="checkbox"/> Proxies	<input type="checkbox"/> Warez
<input type="checkbox"/> Chatting	<input type="checkbox"/> Financial	<input type="checkbox"/> Magazines	<input type="checkbox"/> Radio	<input type="checkbox"/> Weapons
<input type="checkbox"/> Children	<input type="checkbox"/> Gambling	<input type="checkbox"/> Mail	<input type="checkbox"/> Religion	<input type="checkbox"/> Weather
<input type="checkbox"/> Cleaning	<input type="checkbox"/> Games	<input type="checkbox"/> Malware		

User Defined Rules

URL	Action

As shown above you can select predefined categories, or block specific on demand web sites. We recommend that categories be chosen carefully (to meet your company's needs) as the more categories selected the bigger the strain on the desktop as this is done at the desktop level.

Once the settings are set you can select the Accounts menu at the top then Web Filter on the left to actually enable users and download the application link.

Web Filter - Dashboard

Active Users

Username	Password	Last Check-in	Action

Inactive Users

Username	Password	Action
demo3@demo.exchangedefender.com	*****	Select Action ▼
demo2@demo.exchangedefender.com	*****	Select Action ▼

Settings

Lastly, the domain administrator has access to a small subset of settings that only impact the domain level administrator of ExchangeDefender.



Paging – Sets the paging size on portions of the website that exceed one screen

Time Zone – You'd set this to ensure the times you see on the portal match your domain.

Password – This would allow you to change/update the password for the domain level.

Technical Help & Account Management

Please contact (your local IT Solution Provider) for technical help and account management. Own Web Now Corp is a software developer that builds and manages the ExchangeDefender network and does not have access to your account, your data or your company information.

When contacting (you IT Solution Provider) for assistance please keep in mind that the more information you can provide about the issue the faster and more accurately the answer will be provided. Make sure to provide the following to expedite your request:

ExchangeDefender
8131 Vineland Avenue #102
Orlando, FL 32821 USA

Phone: (877) 546-0316
International: (407) 465-6800

www.exchangedefender.com



ExchangeDefender



ExchangDefender

- **Full description of the problem:** Provide a detailed explanation of the issue that you have experienced, if this is the first time you have experienced a problem or if it's repetitive, and if the issue is only affecting you or multiple users.
- **Relevant tracking data:** Provide any relevant information about where you are experiencing an issue: your computer, website, mobile phone, as well as the basic information that can narrow down the research (when the issue happened), what you were attempting to do, who the message was being sent to or received from).
- **Recent account or configuration changes:** Advise us if you have recently made any configuration changes to either your account or your computer/network so that we can double check if all systems are configured properly.
- **Screenshots:** If the issue is easy to see, such as an error message or prompt, take a screenshot. On Windows computers press ALT + PrintScreen at the same time, on Macintosh press Command+Shift+3 at the same time.

General Security Tips:

- ExchangeDefender will never ask you to provide or verify any billing or financial information.
- ExchangeDefender web sites are always encrypted and always contain ExchangeDefender.com
- Never share your ExchangeDefender password with anyone or use the same password across different services or service providers.
- Never save or store your password on portable or shared devices such as mobile phones, kiosks, or computer labs.
- Always follow your IT department or solution provider's security guidelines and report security concerns or breaches.

Get the latest service alerts: <http://www.exchangedefender.com/noc>