Administration Center User Guide

Microsoft Corporation

Published: November 2009



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.
Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

©2009 Microsoft Corporation. All rights reserved.

Microsoft is a trademark of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Forefront Online Protection for Exchange Overview 15](#_Toc245186569)

[Filtering Service Components 16](#_Toc245186570)

[Antivirus Protection 16](#_Toc245186571)

[Layered Defenses Against Viruses 17](#_Toc245186572)

[Real-time Threat Response 17](#_Toc245186573)

[Fast Antivirus Signature Deployment 17](#_Toc245186574)

[Policy Enforcement 18](#_Toc245186575)

[Antispam Protection 18](#_Toc245186576)

[Layered Defenses against Junk Mail 18](#_Toc245186577)

[IP Reputation Blocking 18](#_Toc245186578)

[Connection Analysis 18](#_Toc245186579)

[Reputation Analysis 19](#_Toc245186580)

[Junk E-mail Protection 19](#_Toc245186581)

[Additional Spam Filtering Options 19](#_Toc245186582)

[IP-Based Authentication 19](#_Toc245186583)

[Fingerprinting 20](#_Toc245186584)

[Non-Delivery Report Backscatter Mitigation 20](#_Toc245186585)

[Rules-Based Scoring 20](#_Toc245186586)

[Outbound Spam Filtering 21](#_Toc245186587)

[Higher Risk Delivery Pool 21](#_Toc245186588)

[Routing of Delivery Status Notification Messages 22](#_Toc245186589)

[Accuracy and Effectiveness 22](#_Toc245186590)

[Accuracy 22](#_Toc245186591)

[Effectiveness 23](#_Toc245186592)

[Directory Based User Management 23](#_Toc245186593)

[User List Settings 23](#_Toc245186594)

[Directory Based Edge Blocking 24](#_Toc245186595)

[Message Reject 24](#_Toc245186596)

[Reject Test 25](#_Toc245186597)

[Pass Through 25](#_Toc245186598)

[Passive 25](#_Toc245186599)

[Virtual Domains 25](#_Toc245186600)

[Group Filtering 26](#_Toc245186601)

[Intelligent Routing 26](#_Toc245186602)

[Inbound Address Rewrite 26](#_Toc245186603)

[Disaster Recovery 26](#_Toc245186604)

[Optional Subscriptions 27](#_Toc245186605)

[Exchange Hosted Archive Subscription 27](#_Toc245186606)

[See Also 27](#_Toc245186607)

[Support to Help Satisfy Industry and Regulatory Retention Requirements 27](#_Toc245186608)

[See Also 27](#_Toc245186609)

[Granular Reporting and Auditing Capabilities 28](#_Toc245186610)

[See Also 28](#_Toc245186611)

[Rapid Search and Retrieval 28](#_Toc245186612)

[See Also 28](#_Toc245186613)

[Fully functional backup e-mail system 28](#_Toc245186614)

[See Also 28](#_Toc245186615)

[Exchange Hosted Encryption Subscription 29](#_Toc245186616)

[See Also 29](#_Toc245186617)

[Manage Encrypted E-Mail Messages 29](#_Toc245186618)

[See Also 29](#_Toc245186619)

[Read an Encrypted E-mail Message 29](#_Toc245186620)

[See Also 30](#_Toc245186621)

[Send an Encrypted Reply 30](#_Toc245186622)

[See Also 30](#_Toc245186623)

[Forefront Online Protection for Exchange Setup Checklist and Service Highlights 31](#_Toc245186624)

[Log On to the Services 31](#_Toc245186625)

[See Also 32](#_Toc245186626)

[Set Up Forefront Online Protection for Exchange 32](#_Toc245186627)

[Checklist 32](#_Toc245186628)

[Validate Your Domain(s) on the Administration Center 33](#_Toc245186629)

[Step 1: Validate Your Domain(s) on the Administration Center 33](#_Toc245186630)

[See Also 34](#_Toc245186631)

[Enable Your Domain(s) 34](#_Toc245186632)

[Step 2: Enable Your Domain(s) 34](#_Toc245186633)

[See Also 34](#_Toc245186634)

[Add Other Domains (If Desired) 34](#_Toc245186635)

[Step 3: Add Other Domains (If Desired) 34](#_Toc245186636)

[See Also 35](#_Toc245186637)

[Update Your MX Record 35](#_Toc245186638)

[Step 4: Update Your MX Record 35](#_Toc245186639)

[See Also 35](#_Toc245186640)

[Set up Outbound E-mail Filtering 35](#_Toc245186641)

[Step 5: Set up Outbound E-mail Filtering 35](#_Toc245186642)

[See Also 36](#_Toc245186643)

[Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service 36](#_Toc245186644)

[Step 6: Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service 36](#_Toc245186645)

[See Also 37](#_Toc245186646)

[Set up E-mail Deferral Notifications 37](#_Toc245186647)

[Step 7: Set up E-mail Deferral Notifications 37](#_Toc245186648)

[See Also 38](#_Toc245186649)

[Forefront Online Protection for Exchange Service Highlights 38](#_Toc245186650)

[Directory Synchronization Tool 38](#_Toc245186651)

[SPF Record Settings 38](#_Toc245186652)

[Network Connection Settings 39](#_Toc245186653)

[Security 39](#_Toc245186654)

[IP Restrictions 40](#_Toc245186655)

[Password Policies 40](#_Toc245186656)

[Additional Spam Filtering Options 40](#_Toc245186657)

[False-Positive Submissions 41](#_Toc245186658)

[Policy Filters 41](#_Toc245186659)

[Policy Rules 41](#_Toc245186660)

[Phishing and Spoofing Prevention 41](#_Toc245186661)

[Extension Blocking 42](#_Toc245186662)

[See Also 42](#_Toc245186663)

[Additional Resources: Forefront Online Protection for Exchange Setup Checklist and Service Highlights 42](#_Toc245186664)

[See Also 43](#_Toc245186665)

[Forefront Online Protection for Exchange Administration Center Help 43](#_Toc245186666)

[About the Administration Center 43](#_Toc245186667)

[Core features of the Administration Center 43](#_Toc245186668)

[Sign in and out of the Administration Center 44](#_Toc245186669)

[Quick Search 44](#_Toc245186670)

[Supported Browsers 44](#_Toc245186671)

[Supported Languages 45](#_Toc245186672)

[How to Set the Language Preference 45](#_Toc245186673)

[Information Tab 46](#_Toc245186674)

[Service Statistics 46](#_Toc245186675)

[Welcome Pane 47](#_Toc245186676)

[Administration Tab 47](#_Toc245186677)

[Tabs on the Administration tab: 48](#_Toc245186678)

[Tasks and Views Pane 48](#_Toc245186679)

[Company Settings 48](#_Toc245186680)

[Edit Company Preferences 49](#_Toc245186681)

[View Service Subscriptions 49](#_Toc245186682)

[Company Contacts 49](#_Toc245186683)

[Company IP Address Settings 50](#_Toc245186684)

[Inbound Multi-SMTP Profiles 50](#_Toc245186685)

[Create an Inbound Multi-SMTP Profile 51](#_Toc245186686)

[Delete an Inbound Multi-SMTP Profile 52](#_Toc245186687)

[Outbound IP Address Settings 53](#_Toc245186688)

[Add Outbound IP Addresses 53](#_Toc245186689)

[Delete Outbound IP Addresses 54](#_Toc245186690)

[Company Service Settings 54](#_Toc245186691)

[Filtering Settings 54](#_Toc245186692)

[See Also 55](#_Toc245186693)

[Archive Setting 55](#_Toc245186694)

[See Also 55](#_Toc245186695)

[Edit Company-Wide Archive Settings 55](#_Toc245186696)

[Add a Keyword List 57](#_Toc245186697)

[Security 57](#_Toc245186698)

[Add IP Address Restrictions 57](#_Toc245186699)

[Create a Password Policy 58](#_Toc245186700)

[Password Policy Options 58](#_Toc245186701)

[Edit Password Policy Settings 59](#_Toc245186702)

[Create a Custom Archive Role 60](#_Toc245186703)

[Send Emergency Notification 62](#_Toc245186704)

[Domain Management 62](#_Toc245186705)

[Add a New Domain 63](#_Toc245186706)

[Transfer Settings 63](#_Toc245186707)

[Validate a Domain 64](#_Toc245186708)

[Validate DNS Settings for a Domain 65](#_Toc245186709)

[Enable or Disable a Domain 66](#_Toc245186710)

[Delete a Domain 67](#_Toc245186711)

[Domain Settings 68](#_Toc245186712)

[Preferences 68](#_Toc245186713)

[Catch-All Domains 68](#_Toc245186714)

[Outbound E-Mail Filtering 69](#_Toc245186715)

[BCC Option for Outbound Suspicious E-mail 69](#_Toc245186716)

[Default Outbound Service Domain 69](#_Toc245186717)

[Edit Domain Preferences 70](#_Toc245186718)

[Edit Domain Services 71](#_Toc245186719)

[Archive 71](#_Toc245186720)

[Spam Filtering 72](#_Toc245186721)

[Virus Filtering 72](#_Toc245186722)

[Policy Filtering 72](#_Toc245186723)

[E-mail encryption 73](#_Toc245186724)

[Virtual and Parent Domains 73](#_Toc245186725)

[Group Filtering 74](#_Toc245186726)

[Intelligent Routing 74](#_Toc245186727)

[Inbound Address Rewrite 74](#_Toc245186728)

[Manage Notification Settings 76](#_Toc245186729)

[Notification options 76](#_Toc245186730)

[Configure Spam Quarantine Notifications 76](#_Toc245186731)

[Configure Inbound Virus Recipient Notifications 79](#_Toc245186732)

[Configure Virus Sender Notifications 80](#_Toc245186733)

[Configure Inbound Virus Admin Notifications 81](#_Toc245186734)

[Configure Outbound Virus Admin Notifications 82](#_Toc245186735)

[Configure Deferral Notifications 83](#_Toc245186736)

[Notification Samples 84](#_Toc245186737)

[Spam Quarantine Notifications 84](#_Toc245186738)

[HTML Notifications 84](#_Toc245186739)

[See Also 84](#_Toc245186740)

[Text Notifications 85](#_Toc245186741)

[See Also 85](#_Toc245186742)

[Sample Virus Notifications 85](#_Toc245186743)

[Inbound Virus Recipient Notification 85](#_Toc245186744)

[Sample Warning Notification 86](#_Toc245186745)

[Sample Virus Recipient Notification 87](#_Toc245186746)

[Domain IP Address Settings 87](#_Toc245186747)

[Add a Mail Server Address 88](#_Toc245186748)

[See Also 89](#_Toc245186749)

[Add an Outbound IP Address for Your Domain 89](#_Toc245186750)

[Domain Service Settings 90](#_Toc245186751)

[User List Settings 90](#_Toc245186752)

[Specify the User List Source 90](#_Toc245186753)

[Directory-Based Edge Blocking 91](#_Toc245186754)

[Archive Settings 92](#_Toc245186755)

[See Also 92](#_Toc245186756)

[Edit Company-Wide Archive Settings 92](#_Toc245186757)

[Spam Action Settings 94](#_Toc245186758)

[Spam Quarantine 94](#_Toc245186759)

[Spam Redirection 95](#_Toc245186760)

[Modify Subject 95](#_Toc245186761)

[Add X-Header 95](#_Toc245186762)

[Spam Submission Evaluation 96](#_Toc245186763)

[The Spam Evaluation Process 96](#_Toc245186764)

[Spam Rules Deployment Information 97](#_Toc245186765)

[How to Report Spam 97](#_Toc245186766)

[Additional Spam Filtering Options 97](#_Toc245186767)

[Additional Spam Filtering (ASF) Options 98](#_Toc245186768)

[Additional Spam Filtering Test Mode Options 104](#_Toc245186769)

[Additional Spam Filtering Test Mode Options 105](#_Toc245186770)

[Policy Filter Settings 105](#_Toc245186771)

[Enable and Disable HIPAA Rules 106](#_Toc245186772)

[See Also 108](#_Toc245186773)

[Create an E-mail Footer for Outbound E-mail 108](#_Toc245186774)

[Edit Archive Settings for a Domain 109](#_Toc245186775)

[Configure Quarantine Settings 109](#_Toc245186776)

[Quarantine Settings Options 110](#_Toc245186777)

[User Account Management 111](#_Toc245186778)

[User Settings 111](#_Toc245186779)

[Preferences 112](#_Toc245186780)

[Domain 112](#_Toc245186781)

[Virtual Domain 112](#_Toc245186782)

[About User Roles and Permissions 112](#_Toc245186783)

[Edit Archive Settings for a User 114](#_Toc245186784)

[Assign Archive Roles to User Accounts 115](#_Toc245186785)

[Manage User Relationships 116](#_Toc245186786)

[Edit User Account Settings 117](#_Toc245186787)

[Edit User Preferences 118](#_Toc245186788)

[User Service Settings 118](#_Toc245186789)

[E-mail and IM Addresses 119](#_Toc245186790)

[Change Your Password 120](#_Toc245186791)

[Change Another User's Password 121](#_Toc245186792)

[Have Your Password Sent to You 121](#_Toc245186793)

[Assign Hosted Filtering Permissions to a User 122](#_Toc245186794)

[Add Users 122](#_Toc245186795)

[Primary ways to add user accounts to your hosted services 123](#_Toc245186796)

[Add New Users in the Administration Center 125](#_Toc245186797)

[Import Multiple Users 126](#_Toc245186798)

[Update Service Settings for Multiple Users 127](#_Toc245186799)

[Additional User Upload Information 127](#_Toc245186800)

[Enable or Disable User Accounts 128](#_Toc245186801)

[Delete a User Account 129](#_Toc245186802)

[Use Secure FTP to Add User Accounts 129](#_Toc245186803)

[Subdirectory Structure 130](#_Toc245186804)

[Comparison of Import Users from File and Secure FTP-Based Upload Methods 130](#_Toc245186805)

[File Replication Schedule 131](#_Toc245186806)

[File Validation Checking 131](#_Toc245186807)

[Secure FTP File Format 132](#_Toc245186808)

[Specify the Directory Service Option 132](#_Toc245186809)

[Specify Domains and Users 132](#_Toc245186810)

[Specify Virtual Domains 133](#_Toc245186811)

[Add End-of-File Tag 133](#_Toc245186812)

[Add User Accounts by Using Secure FTP 133](#_Toc245186813)

[Directory Synchronization Tool 134](#_Toc245186814)

[Administration Center Settings for the Directory Synchronization Tool 135](#_Toc245186815)

[Notification address 135](#_Toc245186816)

[Domains 135](#_Toc245186817)

[Legacy Directory Synchronization Tool 135](#_Toc245186818)

[Policy Rules 136](#_Toc245186819)

[See Also 137](#_Toc245186820)

[Policy Rule Match Options 137](#_Toc245186821)

[E-Mail Header match options 137](#_Toc245186822)

[E-Mail Sender match options 138](#_Toc245186823)

[E-Mail Sender policy rule actions overview 140](#_Toc245186824)

[E-Mail Recipient match options 140](#_Toc245186825)

[Additional match options 141](#_Toc245186826)

[Attachment match options 146](#_Toc245186827)

[Additional match options 148](#_Toc245186828)

[Message Subject and Message Body match options 148](#_Toc245186829)

[Additional match options 150](#_Toc245186830)

[Message Properties 150](#_Toc245186831)

[Policy Rule Settings 151](#_Toc245186832)

[Policy Filter Actions 152](#_Toc245186833)

[Inbound Policy Filter Actions 152](#_Toc245186834)

[Outbound Policy Filter Actions 153](#_Toc245186835)

[Policy Rule Syntax 155](#_Toc245186836)

[Basic syntax 155](#_Toc245186837)

[Definition of basic syntax 155](#_Toc245186838)

[RegEx syntax 156](#_Toc245186839)

[Definition of RegEx syntax 157](#_Toc245186840)

[More examples for creating match expressions with RegEx 159](#_Toc245186841)

[About Regular Expressions 160](#_Toc245186842)

[Create, Edit, or Delete a Policy Rule 160](#_Toc245186843)

[Set Compliance Policy Rules 161](#_Toc245186844)

[Policy Rule Processing 162](#_Toc245186845)

[Additional Policy Rule settings 165](#_Toc245186846)

[Expiration Date 166](#_Toc245186847)

[Description 166](#_Toc245186848)

[Notifications 166](#_Toc245186849)

[Filters 167](#_Toc245186850)

[My Reports Tab 169](#_Toc245186851)

[About Reports 170](#_Toc245186852)

[Reports Overview 170](#_Toc245186853)

[Saved Reports 170](#_Toc245186854)

[Scheduled Report Delivery 170](#_Toc245186855)

[Create, Modify, or Delete a Report 171](#_Toc245186856)

[View and Export Results for Saved Reports 173](#_Toc245186857)

[Run Archive Report 173](#_Toc245186858)

[Activity Summary Report 174](#_Toc245186859)

[Archive Summary Report 174](#_Toc245186860)

[Attachment Summary Report 174](#_Toc245186861)

[Audit Events Report 174](#_Toc245186862)

[Daily Statistics Report 174](#_Toc245186863)

[Destruction Report 175](#_Toc245186864)

[Email Summary Report 175](#_Toc245186865)

[Employee Roster Report 175](#_Toc245186866)

[Privileged Roles Report 175](#_Toc245186867)

[SEC 17a-4 Report 175](#_Toc245186868)

[Supervisory Review Evidentiary Report 175](#_Toc245186869)

[System Statistics Report 176](#_Toc245186870)

[Tools Tab 176](#_Toc245186871)

[Run a Message Trace 176](#_Toc245186872)

[Message Trace Tool Known Limitations 177](#_Toc245186873)

[Voltage Encryption: 177](#_Toc245186874)

[IP Edge Blocks: 178](#_Toc245186875)

[Redirected messages: 178](#_Toc245186876)

[Deferred message: 178](#_Toc245186877)

[Directory Services: 178](#_Toc245186878)

[Virus Cleaned: 178](#_Toc245186879)

[Messages that travel between data centers: 178](#_Toc245186880)

[Virtual Domains: 179](#_Toc245186881)

[MAIL FROM: 179](#_Toc245186882)

[Policy Rule Updates: 179](#_Toc245186883)

[View the Audit Trail 179](#_Toc245186884)

[Technical Support 180](#_Toc245186885)

[The four ways to contact Technical Support to open a support incident 180](#_Toc245186886)

[International Support and Dialing Codes 180](#_Toc245186887)

[Messaging Knowledge Base 181](#_Toc245186888)

[Submit a Service Request on the Web 181](#_Toc245186889)

[Checking Incident Status 181](#_Toc245186890)

[Guidelines for Successful Spam Submissions 181](#_Toc245186891)

# Forefront Online Protection for Exchange Overview

Welcome to the Microsoft Forefront Online Protection for Exchange Filtering Service. This guide will introduce you to the Administration Center, a Web-based tool that allows you to create reports and customize your e-mail filtering account services. The Hosted E-mail Filtering network includes a number of data centers that are geographically distributed. When you make changes to your services in the Administration Center, the changes are typically saved and replicated in all data centers within 30 minutes. The following diagram illustrates how filtering works with Exchange Hosted Services.



 Forefront Online Protection for Exchange is powered by a global network of data centers, which are based on a fault-tolerant and redundant architecture, and is load-balanced both site-to-site and internally within each data center. If a data center suddenly becomes unavailable, traffic is automatically routed to another data center without any interruption to service. Thousands of e-mail servers across the network of data centers accept e-mail on your behalf, providing a layer of separation between your servers and the Internet. Furthermore, Microsoft algorithms analyze and route message traffic between data centers to ensure the most timely and efficient delivery. This approach, built on a distributed server and software model, has proven successful in helping to protect our customers' corporate networks and e-mail servers from common threats such as dangerous worms, denial-of-service assaults, directory harvesting, and dictionary attacks.

All messages processed by Forefront Online Protection for Exchange are encrypted using Transport Layer Security (TLS). To help ensure privacy and message integrity, the service will attempt to send and receive e-mail using TLS but will automatically rollover to SMTP if the sending or destination e-mail server is not configured to use TLS.

# Filtering Service Components

To provide effective message security for corporate networks, Forefront Online Protection for Exchange (FOPE) offers five services that apply a blend of preventive and protective measures to stop both increasingly complex e-mail–borne threats from infiltrating businesses and also to stop violations of corporate policy for e-mail use. The services are as follows:

[Antivirus Protection](#zf116dc34d0f14d839f02c174110e3be3) - These features help protect businesses from receiving e-mail–borne viruses and other malicious code by scanning for unknown viruses with a multi-step process that includes multiple scan engines and heuristic detection to minimize the window of vulnerability during emerging threats.

[Policy Enforcement](#z03839a41f3b04db3bcdbcde6cc49e819) - These features provide administrators with the ability to craft highly flexible policy rules to regulate e-mail flow for compliance.

[Antispam Protection](#z5474345309234ad290d462e3acab4807) - This feature demonstrates layering antispam technologies. The antispam filter can detect all types of spam before they reach the corporate network.

[Directory Based User Management](#z74002ffed63a4dca816beffdfaf21cff) - This feature allows organizations to specify all valid users on a domain and to configure different service settings for groups of users within a domain.

[Disaster Recovery](#z5df3b5c9f3a742d6920fef66eb10ef0d) - This feature helps ensure that no e-mail is lost by instantly and automatically queuing messages for later delivery if the destination e-mail server is unavailable.

[Optional Subscriptions](#zd1ea0b721f38422fa94b758365bb5c93) - Additional subscriptions are needed in order to provide administrators with the ability to configure gateway and policy-based e-mail encryption rules.

Developed as a family, these services easily integrate with one another as a package and require little to no user-modification to be effective. Even with little custom configuration, FOPE blocks more than 98 percent of unwanted e-mail and 100 percent of known viruses, reducing message traffic and improving the efficiency of the corporate messaging infrastructure.

# Antivirus Protection

Antivirus protection options include the following:

[Layered Defenses Against Viruses](#z5b6982ca2a674cbb8170dbea471751a1)

[Real-time Threat Response](#z224eb21bf36046fd8ec5360ce4888a21)

[Fast Antivirus Signature Deployment](#zea8bb596ef5e47618232f3fd39ca8763)

# Layered Defenses Against Viruses

Microsoft Forefront Online Protection for Exchange (FOPE) employs a layered approach to offer protection from both known and unknown threats for both inbound and outbound e-mail. FOSE uses multiple antivirus engines to help protect against viruses and other e-mail threats. The antivirus engines include powerful heuristic detection to provide protection even during the early stages of a virus outbreak. The multi-engine approach has been shown to provide significantly more protection than using just one antivirus engine.

Other antivirus protection options include the following:

[Real-time Threat Response](#z224eb21bf36046fd8ec5360ce4888a21)

[Fast Antivirus Signature Deployment](#zea8bb596ef5e47618232f3fd39ca8763)

# Real-time Threat Response

During some virus outbreaks, the Forefront Online Protection for Exchange (FOPE) anti-malware team may have enough information about a virus or other form of malware to write sophisticated policy rules that detect the threat even before a signature is available from any of the antivirus engines used by the service. These rules are published to the global network every 2 hours to provide your organization with an extra layer of protection against attacks.

Other antivirus protection options include the following:

[Layered Defenses Against Viruses](#z5b6982ca2a674cbb8170dbea471751a1)

[Fast Antivirus Signature Deployment](#zea8bb596ef5e47618232f3fd39ca8763)

# Fast Antivirus Signature Deployment

Fast Antivirus Signature Deployment is closely tied with its antivirus partners, integrating each antivirus engine at the application programming interface (API) level. As a result, Fast Antivirus Signature Deployment receives and integrates virus signatures and patches before they are publicly released; often, its connection with the antivirus partners allows it to develop virus remedies. The service checks for updated virus signatures for all antivirus engines every 15 minutes and applies them in minutes to the global filtering network.

Other antivirus protection options include the following:

[Layered Defenses Against Viruses](#z5b6982ca2a674cbb8170dbea471751a1)

[Real-time Threat Response](#z224eb21bf36046fd8ec5360ce4888a21)

# Policy Enforcement

FOSE offers an integrated approach to message security through policy enforcement. It allows companies to automatically monitor outbound and inbound e-mail, stop sensitive or inappropriate messages from leaving and entering the corporate network, and allow specific senders to bypass spam filtering completely. For more information about the Policy Rule options, see the [Policy Rules](#zd43d92b98b8c43a3869b6bb4ca4e0682) topic.

# Antispam Protection

Left unchecked, spam can overwhelm businesses, destroying e-mail productivity and the benefits of this vital business communication tool. The sheer volume of spam, coupled with spammer creativity, leaves businesses with no option but to turn to technology to combat this ever-present threat.

# Layered Defenses against Junk Mail

FOSE achieves enhanced accuracy with proprietary, multilayer spam technology that helps ensure that unsolicited e-mail is automatically filtered before it enters your corporate messaging systems. Once a domain has been configured and enabled for the service, an MX record for your domain is appointed to route mail through the service. After this, ongoing intervention by your IT users or administrators is no longer needed.

# IP Reputation Blocking

FOSE IP-reputation blocking serves as the first line of defense against unwanted e-mail and blocks about 90 percent of inbound junk e-mail through connection analysis and reputation analysis.

# Connection Analysis

Each connection to the FOSE network is monitored closely and evaluated based on the SMTP commands issued by the connecting server. Nonstandard connection requests that deviate significantly from RFC standards and spoofed connection attempts are immediately dropped. This helps to shield your networks from these connection attempts that are not valid.

# Reputation Analysis

FOSE reputation-based connection blocking employs a proprietary list that, based on analysis of historical data, contains the addresses of computers connected to the Internet that are responsible for the majority of spam. Through an ongoing partnership with Microsoft® Windows Live™ Hotmail®, FOSE aggregates both consumer and corporate junk e-mail data to populate a massive and comprehensive reputation database.

FOSE also utilizes Internet Protocol (IP) reputation information from other companies and ISPs in order to provide enhanced protection from spammy IP’s and botnet attacks, which come from a collection of compromised computers running software under a common infrastructure of command and control. Spammers are frequently creating malicious web sites that they use for phishing and infecting malware. FOSE leverages a variety of sources to quickly update lists of known malicious URLs and update its content filters to block these messages.

# Junk E-mail Protection

Once a message passes the edge blocking, it must then pass the following four additional layers of antispam technology:

1. Additional Spam Filtering options (ASF)

2. IP-based authentication

3. Probabilistic-based content filtering

4. Rules-based scoring

# Additional Spam Filtering Options

Many customers want more control over e-mail that may contain obscene graphics, affect privacy, or attempt to trick users into disclosing sensitive information. The additional spam filter (ASF) feature within FOSE lets you apply filtering flags and quarantine messages that contain various kinds of active or suspicious content. For detailed information about the ASF filtering flags that are available, see [Additional Spam Filtering Options](#z074002c0d00e4f378225a1f254079562).

# IP-Based Authentication

FOSE authenticates the identity of the sender of each e-mail message. If a message cannot be authenticated and the message is determined to be from a spoofed sender, it is more likely to be scored as spam. Sender Policy Framework (SPF), an industry standard that prevents return-path address forgery by using SMTP Mail From identity in e-mail, makes it easier to identify spoofs. SPF lookups help verify that the entity listed as the sender did indeed send the e-mail message.

# Fingerprinting

When messages contain known spam characteristics, they are identified and fingerprinted; that is, they are given a unique ID based on their content. The fingerprinting database aggregates data from all spam blocked by the Forefront Online Protection for Exchange (FOPE) system, which improves and refines the fingerprinting process as more messages are processed. If a message with a particular fingerprint passes through the system a second time, the fingerprint is detected and the message is marked as spam. The system continually analyzes incoming messages to determine new spamming methods. The FOPE spam analysis team updates the fingerprint layer as new campaigns are detected.

# Non-Delivery Report Backscatter Mitigation

There are a number of causes for a surge in non-delivery reports (NDRs) that may affect an e-mail environment. For example, one of the e-mail addresses within a domain may be affected by a spoofing campaign or be the source address for a directory harvest attack. Any of these issues could result in a sudden increase in the number NDRs being delivered to end users. NDR backscatter, which refers to the many messages received when an e-mail address is forged as the sender on spam, has become a serious issue for many customers. In addition to NDR detection rules, an additional ASF rule helps block backscatter. This option will filter out NDR messages and send them to the quarantine.

For outbound filtering customers, logic is used to help detect NDRs that are legitimate bounce messages, and these are delivered to the original sender without enabling the ASF option. For outbound customers, intelligent detection of legitimate NDRs is enabled by default.

# Rules-Based Scoring

Based on more than 20,000 rules that embody and define characteristics of spam and legitimate e-mail, scores are assigned to messages. Points are added to the score if a message contains characteristics of spam, while points are subtracted if it contains characteristics of legitimate e-mail. When a message’s score reaches a defined threshold, the message is flagged as spam.

Message characteristics that FOSE evaluates and scores include the following:

 Phrases in the body and subject of the message, including URLs

 HTTP obfuscation, which is disguising spammy URLs as legitimate URLs

 Malformed headers, which are headers that have been incorrectly constructed

 E-mail client type

 Formation of headers; for example Message-ID, Received, random characters

 Originating mail server

 Originating mail agent

 From and SMTP From address

The current rules are modified and new rules are added as needed many times each day, every day, by the spam team.

# Outbound Spam Filtering

All outbound messages that exceed the spam threshold are delivered through a Higher Risk Delivery Pool. The Higher Risk Delivery Pool is a secondary outbound e-mail pool that is used to send messages that may be of low quality, thus helping to protect the rest of the network from sending messages that are more likely to result in the sending IP address being blocked.

The use of a dedicated Higher Risk Delivery Pool helps ensure that the normal outbound pool is only sending e-mail that is known to be high-quality. The possibility of the Higher Risk Delivery Pool being placed on a blocked list remains a risk. This is by design. This secondary server pool helps to reduce the probability of the normal outbound-server pool being added to a blocked list.

Additionally, some e-mail filtering agents will throttle messages where the sending domain has no address record (A record), which gives you the IP address of the domain, and no mail exchange record (MX record), which helps direct mail to the servers that should receive the mail for a particular domain in the DNS. Such outbound mail, regardless of its spam disposition, is routed through the Higher Risk Delivery Pool.

# Higher Risk Delivery Pool

When a customer's e-mail system has been compromised by a virus or malicious spam attack, and it is sending outbound spam through Forefront Online Protection for Exchange, this could result in the IP addresses of the Hosted Filtering Data Center being listed on other block lists. In addition, destination servers that do not use the Hosted Filtering service, but do use these block lists, end up rejecting all e-mail sent from any of the Hosted Filtering IP addresses that have been added to those lists.

The Higher Risk Delivery Pool is a secondary outbound e-mail pool that is used to send messages that may be of low quality. This pool helps to protect the rest of the network from sending messages that are more likely to result in the sending IP address being blocked.

The use of a dedicated Higher Risk Delivery Pool helps to ensure that the normal outbound pool is only sending high-quality e-mail. The possibility of the Higher Risk Delivery Pool being placed on a third-party block list remains a risk (and is by design). However, having this secondary server pool helps to reduce the probability of the normal outbound server pool being added to a third-party block list.

# Routing of Delivery Status Notification Messages

The outbound Higher Risk Delivery Pool manages the delivery for all messages identified as Delivery Status Notifications (DSN) or Non-Delivery Reports (NDR).

Possible causes for a surge in NDRs include the following:

 A spoofing campaign affecting one of the customers using the Hosted Filtering service

 A directory harvest attack

 A spam attack

 A rogue SMTP server

All of these issues could result in a sudden increase in the number NDRs being processed by the service. Many times these NDRs appear to be spam to other e-mail servers and services.

Both valid and potentially non-valid NDR messages are routed through the Higher Risk Delivery Pool. The following guidelines are intended to help prevent messages from being routed through the Higher Risk Delivery Pool:

 Do not send legitimate e-mail from an address that has been configured in the Administration Center as the CUSTOM SCANNER ADDRESS on a Virus Bounce.

 Do not send legitimate e-mail from an address that has been configured in the Administration Center as the BOUNCE ADDRESS on a Policy Filter rule notification.

 If it is necessary to forward an NDR message through the Hosted Filtering service, place the message inside of a compressed file and attach it to a new e-mail message.

# Accuracy and Effectiveness

Ineffective spam filters frustrate users and expose companies to infection and risk of data loss. FOSE simultaneously delivers high accuracy and effectiveness by both identifying spam and keeping it from reaching customer mailboxes. By using FOSE, customers can preserve the integrity of their e-mail environment and communications, boosting productivity and improving total cost of ownership for their corporate e-mail systems.

# Accuracy

A false positive is a legitimate message that is incorrectly identified as spam. These can be either bulk messages such as newsletters, person-to-person legitimate business communication, or personal e-mail. Through extensive monitoring, Forefront Online Protection for Exchange (FOPE) has found that the ratio of false-positive messages is smaller than approximately 1 in 250,000, which is 0.0004 percent.

Your users and administrators can report e-mail abuse by submitting messages to the abuse e-mail alias. The Spam Analysis Team examines the submitted messages and tunes the filters accordingly to prevent future occurrences of spam. As a result, the service is constantly updating and refining the spam prevention and protection processes. Any submitted items are evaluated at the network-wide level. False-positive submissions are examined and assessed for possible rule adjustment to allow future messages through the spam filters. Therefore, notifying the service of false positives and unfiltered spam is advantageous for you and all customers utilizing the FOPE global network.

# Effectiveness

Without tuning, the Forefront Online Protection for Exchange solution can block 98 percent of spam. However, adding the additional spam filtering (ASF) capability can allow your organization to further customize spam filtering according to your needs, which may increase effectiveness.

# Directory Based User Management

The Administration Center allows you to add and manage users for both the Forefront Online Protection for Exchange (FOPE) Filtering and the Exchange Hosted Archive services subsequent to version 8.1.

# User List Settings

The four primary methods for adding user accounts to your hosted services are as follows:

1. Use the Directory Synchronization tool (recommended): The Microsoft Directory Synchronization Tool (DST) is an on-site application that communicates with your company’s on-site Microsoft Active Directory® Domain Services AD DS and Microsoft Exchange Server messaging environment to build a user e-mail address list for your FOSE and Exchange Hosted Archive services later than version 8.1. With this, you can manage your user accounts by using your on-site AD DS environment. Users who are synchronized with the DST will be automatically added in the Administration Center. Specific service settings can be controlled for these users. Quarantine accounts are pre-populated, they can be used for Directory-Based Edge Blocking, and for the Exchange Hosted Archive service later than version 8.1. For more information, see [Directory Synchronization Tool](#zab46365b12a74adfbc36acb619e9094f).

2. Use the Administration Center: User accounts can be added by using the Administration Center, either one at a time or in batches. This can be done by uploading a comma-separated values (CSV) file that contains a list of user names and their related service information. After you add user accounts, you can then modify the user account information and assign roles and permissions. The following are some of the key features that apply to user accounts: Specific service settings, pre-populated quarantine accounts, Directory-Based Edge Blocking, and the Exchange Hosted Archive service later than version 8.1.

3. Upload a user list by using Secure file transfer protocol (FTP): You can create a user e-mail address list and upload it to a Secure FTP (SFTP) directory for your domain. FOSE first verifies that the user list meets the correct format requirements, and then adds the users to your services. Users who are synchronized through SFTP will not show up in the Administration Center, but can be used for Directory-Based Edge Blocking. In order to remove users from Directory-Based Edge Blocking who have been uploaded through SFTP, upload an empty SFTP list to the domain. For more information, see [Use Secure FTP to Add User Accounts](#z169777a9f0b9436e952d279818f306f1).

4. Use the Legacy Directory Synchronization tool: The Microsoft Exchange Hosted Services Directory Synchronization Tool (legacy DST) is an on-site application that communicates with your company’s on-site Active Directory and Microsoft Exchange Server messaging environment to build a user e-mail address list for your FOSE or Exchange Hosted Archive services later than version 8.1. With this, you can manage your user accounts by using your on-site AD DS environment. Users who are synchronized with the Legacy DST will not show up in the Administration Center, but can be used for Directory-Based Edge Blocking and for the Exchange Hosted Archive service later than version 8.1.
 For more information, see [Microsoft Exchange Hosted Services Directory Synchronization Tool](http://go.microsoft.com/fwlink/?LinkID=137140).

# Directory Based Edge Blocking

FOSE Directory-Based Edge Blocking (DBEB) is a multifunctional service that improves message handling and routing for inbound message traffic. The FOSE Filtering service normally processes all of the messages that are sent to any SMTP address within your domain. Hosted Filtering can also help keep unwanted e-mail from reaching your system by the use of user e-mail address lists. When you create a user list, you can block all e-mail that appears to be legitimate, but is sent to e-mail addresses that are not in your user list.

# Message Reject

The message reject functionality rejects all e-mail (spam and legitimate mail) at the network perimeter for recipients not on the domain’s user list. Therefore, if a message is received for a recipient that is included on the user list, the message is processed according to the domain’s settings. If however, a message is received for a recipient who is not included on the user list, then FOSE responds with a 554 error message, which reads as follows: smtp;554 <badaddress@contoso.com>: Recipient address rejected: Access denied).

# Reject Test

To be used for short periods of time, the reject test function validates the accuracy of a user list. All e-mail for recipients that are not on a domain’s user list is redirected to a specific e-mail address after filtering. Therefore, if a message is received for a recipient on the user list, the message is processed according to the domain’s settings. If however, a message is received for someone not on the user list, that message is processed according to the domain’s settings and delivered to the final e-mail address listed for the domain.

# Pass Through

Administrators can define a subset of users who are included, or “opted in” for service evaluation purposes, while all others by default are not included, or “opted out” of all filtering services, even if all users share the same domain. Therefore, if a message is received for someone whose name is included on the user list, that is, the end user is “opted in,” the message is processed according to the domain’s settings. If however, a message is received for someone not on the user list, that is, the end user is “opted out,” the message bypasses the message switch and any filtering settings and is delivered to the corporate mail server directly.

The e-mail messages for users who are not present in the Pass Through list do not bypass the IP Reputation Blocks on the FOSE network edge.

# Passive

Passive mode on a domain allows you to configure virtual domains for that domain without needing to provide a user list for the parent domain.

# Virtual Domains

Virtual domains can be configured in order to provide group filtering, intelligent routing, or inbound address rewrite. For more information, see [Virtual and Parent Domains](#z643fe906820d42c489cdf1d4e559536f).

E-mail for a particular virtual domain is processed for all e-mail addresses that are included in an upload list for that virtual domain, as specified by the settings in the Administration Center. If e-mail is received for an address that is not listed in the upload list for the given virtual domain, it is processed according to the edge blocking settings for the parent domain.

# Group Filtering

The group filtering function allows for different groups of user accounts to have their own sets of filtering rules, even if all user accounts share the same domain. For example, the human resources department can have different filtering rules than the information technology department.

# Intelligent Routing

A function of group filtering, the intelligent routing feature routes a subset of user messages to specific delivery locations based on virtual domain IP address settings, even if users all share the same domain. For example, the United Kingdom office can receive all mail for local users at a specific location, one that is different than the destination for mail sent to United States users. As in group filtering, each user account is associated with a virtual domain. Each virtual domain is then configured to redirect e-mail to specific servers within the organization.

In order to revert the recipient address to the original parent domain naming, the recipient address needs to be rewritten by the receiving mail server. If the recipient address is not rewritten by the receiving mail server, then the user would be able to view the virtual domain name in the message header. When the end user replies to a message that was routed using this functionality, the Reply-To address for the end user would not be affected, as this is inserted by the sending server (your mail server) based on the primary SMTP proxy address associated with the user in your environment.

# Inbound Address Rewrite

A function of Group Filtering, the inbound address rewriting feature rewrites the recipient addresses for specific users and will deliver messages for those recipients based on the virtual domain IP address settings. For example, the HR department at Contoso needs to receive e-mail at hr.contoso.com, even though the delivery location may be the same as the main contoso.com domain. As in Group Filtering, each user account is associated with a virtual domain. Each virtual domain is then configured to deliver e-mail to specific servers within the organization.

# Disaster Recovery

If your e-mail server becomes unavailable for any reason, FOSE helps ensure that no e-mail is lost or bounced. FOSE servers spool and queue e-mail for up to five days. A message may be in the retry queue and delivery attempts made every 20 to 30 minutes until the 5-day timeout is exceeded. Once an e-mail server is restored, all queued e-mail is forwarded in a flow-controlled fashion. In cases of extended downtime, e-mail can be rerouted to another server or made available through a Web-based interface.

The system can be set up to provide deferral notification in the event that e-mail cannot be delivered, sending a text-based page to an administrator if e-mail is unable to be delivered. For more information, see [Configure Deferral Notifications](#z9bd8a3ce106e4122b6121bc664890e26).

# Optional Subscriptions

Forefont Online Security for Exchange offers the following optional subscriptions:

[Exchange Hosted Archive Subscription](#z0722c7be2bbb46a795e2459b63424869)

[Exchange Hosted Encryption Subscription](#zb18d41b4a96440fea528e0720f5361a5)

# Exchange Hosted Archive Subscription

Microsoft Exchange Hosted Archive (EHA) provides a centralized, easily accessible, and multi-functioning e-mail and instant message (IM) repository to help organizations manage increasingly complex retention, compliance, e-discovery, and regulatory requirements.

## See Also

[Support to Help Satisfy Industry and Regulatory Retention Requirements](#z8ecbec7e48ae4d278ac3ac9fa728797b)

[Granular Reporting and Auditing Capabilities](#zc9c9306513804fd884bd971434623bee)

[Rapid Search and Retrieval](#z0ce5747b8172441cbf04c943335a1c5f)

[Fully functional backup e-mail system](#zdea10d090d4b44f0801ea32b8c08d97b)

# Support to Help Satisfy Industry and Regulatory Retention Requirements

Exchange Hosted Archive has many features that aid in compliance, including the following:

 Multiple retention periods

 Legal hold

 Supervision by keyword or percentage

 Immutable storage

## See Also

[Granular Reporting and Auditing Capabilities](#zc9c9306513804fd884bd971434623bee)

[Rapid Search and Retrieval](#z0ce5747b8172441cbf04c943335a1c5f)

[Fully functional backup e-mail system](#zdea10d090d4b44f0801ea32b8c08d97b)

# Granular Reporting and Auditing Capabilities

A robust security policy encompasses granular audits and logging system transactions. EHA has numerous auditing reports available in addition to several traceable administrative and user events.

## See Also

[Support to Help Satisfy Industry and Regulatory Retention Requirements](#z8ecbec7e48ae4d278ac3ac9fa728797b)

[Rapid Search and Retrieval](#z0ce5747b8172441cbf04c943335a1c5f)

[Fully functional backup e-mail system](#zdea10d090d4b44f0801ea32b8c08d97b)

# Rapid Search and Retrieval

Indexed storage enables fast retrieval of messages for e-discovery and other investigations.

## See Also

[Support to Help Satisfy Industry and Regulatory Retention Requirements](#z8ecbec7e48ae4d278ac3ac9fa728797b)

[Granular Reporting and Auditing Capabilities](#zc9c9306513804fd884bd971434623bee)

[Fully functional backup e-mail system](#zdea10d090d4b44f0801ea32b8c08d97b)

# Fully functional backup e-mail system

If primary e-mail systems fail, users and administrators will still have access to archived e-mail and can send and receive new messages in real time.

## See Also

[Support to Help Satisfy Industry and Regulatory Retention Requirements](#z8ecbec7e48ae4d278ac3ac9fa728797b)

[Granular Reporting and Auditing Capabilities](#zc9c9306513804fd884bd971434623bee)

[Rapid Search and Retrieval](#z0ce5747b8172441cbf04c943335a1c5f)

# Exchange Hosted Encryption Subscription

Microsoft Exchange Hosted Encryption (EHE) is a convenient, easy-to-use e-mail encryption service that helps safely deliver your confidential business communications. The service enables users to send and receive encrypted e-mail directly from their desktops as easily as regular e-mail, to anyone at any time.. The ability to encrypt specific messages can be configured through the use of policy rules. The rules are gateway based, and require no public or private key management.

## See Also

[Manage Encrypted E-Mail Messages](#z185333fb1c014f28ae4fba7776be4a61)

# Manage Encrypted E-Mail Messages

If your organization subscribes to the encrypted e-mail service, your users can send and receive encrypted e-mail directly from their desktops in the same manner as regular e-mail.
Encryption is policy rule based. Messages are encrypted at the gateway based on policy rules that you have set. Zero download messenger (ZDM) enables a more secure Web-based encryption and decryption for any recipient of encrypted e-mail. A managed key server eliminates the need for certificate maintenance.
When you set the Encrypt rule action on the policy rule for outbound mail, e-mails sent by users in the organization can be encrypted automatically based upon rule-matching by subject and message keywords, regular expressions, sending and receiving e-mail address, or domains.

## See Also

[Read an Encrypted E-mail Message](#z59d5c6623b694c1bbb5deee33e6b2940)

[Send an Encrypted Reply](#z4a8eeb18295346d38e1c16eb1652eafa)

# Read an Encrypted E-mail Message

How to open e-mail messages using the Zero Download Manager (ZDM)

|  |
| --- |
| 1. Open the secure e-mail message.2. Click the Read Message button. 3. Enter your password and click Continue. |

For security purposes, the link provided to read your encrypted e-mail can only be clicked once. If you attempt to click on the same link a second time, you will receive the error This link has already been used. If you are trying to view your secure message, return to your inbox, click on the message you are attempting to read, and open the attachment titled message\_zdm.html.

In order to read the e-mail, you will need to go back to the original e-mail you received and follow the authentication process again. This will cause a new e-mail to be sent to you with a new link. Alternatively, you will need to clear your Internet cookies and cache. If you are still unable to decrypt the message, contact the sender and let their support team know of the issues with decrypting the message. From this point they will need the Encryption team for further investigation. You may wish to escalate this matter to your local technical support if you continue to have problems with retrieval of the cookie required.

Important

The timeout for an encrypted message is 15 minutes when accessing the messages through Zero Download Messenger (ZDM). This timer starts as soon as you process the authentication through the message\_vsr.html attachment. You will have 15 minutes to authenticate, open authentication e-mail answer back, click the token that was sent, read your decrypted message in the ZDM, compose a reply to the sender and send through ZDM in order to have your response encrypted as well.

If the e-mail answer back is delayed for any reason or the message that you are replying with is long, and takes more than 15 minutes to compose, the session will timeout and you will get an error.

As soon as you have received one answer back that has expired, you must request another answer back from the HTML message in order to view the encrypted message again.

## See Also

[Send an Encrypted Reply](#z4a8eeb18295346d38e1c16eb1652eafa)

# Send an Encrypted Reply

How to send a secure reply using Zero Download Manager

|  |
| --- |
| 1. Click Reply or Reply All from an open message. A new window will open.2. Type your message and attach any applicable files.3. Click Send Secure when you have finished composing the message.  |

## See Also

[Read an Encrypted E-mail Message](#z59d5c6623b694c1bbb5deee33e6b2940)

# Forefront Online Protection for Exchange Setup Checklist and Service Highlights



Use this seven-step checklist to complete the basic setup and configuration of your Microsoft Forefront Online Protection for Exchange Hosted Filtering service.

Highlights about key service features have been listed below the checklist and are based on customer feedback about the best ways to ensure that you get the most out of your service.

Need more information or help? The following resources offer additional information:

 [Online training](http://go.microsoft.com/fwlink/?LinkID=137241): Offers an overview of the Administration Center site, along with more tips for setting up and configuring your service.

 [Administration Center User Guide](http://go.microsoft.com/fwlink/?LinkID=135918): Comprehensive information about service configuration and settings.

 Information tab on the Administration Center: The best place to go for feature announcements, network maintenance updates, details on virus outbreaks, support resources, training modules, and configuration information.

 Technical support:

a. Site: <http://go.microsoft.com/fwlink/?LinkID=149248>

b. E-mail: support@messaging.microsoft.com/

c. Phone: 866.291.7726

## Log On to the Services

You must log on to access the Administration Center, where you configure your services.

To log on to your services

|  |
| --- |
| 1. In your Internet browser (Internet Explorer or Firefox), enter the link provided when you signed up for the services.2. You will receive an e-mail with a link to set up your password.3. Once your password has been created, you will automatically be directed to and logged on to the Administration Center.  |

See the Setup Checklist to walk through the process of setting up and configuring Microsoft Forefront Online Protection for Exchange.

## See Also

[Forefront Online Protection for Exchange Service Highlights](#zfe17212be0ac43b8815d7405f62eba75)

# Set Up Forefront Online Protection for Exchange

This checklist outlines the process of setting up and configuring Microsoft Forefront Online Protection for Exchange. Each task in the checklist is linked to the steps required to perform the task. For more detailed information on service configuration and settings, read the [Administration Center User Guide](http://go.microsoft.com/fwlink/?LinkID=135918)

## Checklist

| **Step** | **Completed** | **Date** |
| --- | --- | --- |
| 1: [Validate Your Domain(s) on the Administration Center](#zab98f4209ff04544aac9163768dd36d4) |  |  |
| 2: [Enable Your Domain(s)](#zc3765f89ec764095bf4b14b1130c8eef) |  |  |
| 3: [Add Other Domains (If Desired)](#z3db7f58ca2124a3eadc8b339a90e6ab9) |  |  |
| 4: [Update Your MX Record](#zed860c81a4484a70aa0bbc60890d850c) |  |  |
| 5: [Set up Outbound E-mail Filtering](#z5ca511c1b7204c5d80d30f274febc0b0) |  |  |
| 6: [Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service](#zf1348ce82e88471e8dd5bd15c84f1671) |  |  |
| 7: [Set up E-mail Deferral Notifications](#z119b5f109f53410f9a703578447057af) |  |  |

# Validate Your Domain(s) on the Administration Center

## Step 1: Validate Your Domain(s) on the Administration Center

1. Set your password by clicking the “Need your password?” link and following the steps outlined in the URL that will be mailed to you.

2. In your Internet browser (Internet Explorer or Firefox), enter the link provided when you signed up for the services, and enter your password. Click Enter. You are now logged on.

3. On the Administration tab, click the Domains subtab.

4. In the Domains list, click the domain(s) you want to validate. To search for a domain, enter the name of the domain in the search box and click Go. The domain details page will open.

5. In the Tasks pane, click Validate Domain.

The Validate Domain dialog box displays the information you need to create the CNAME entry in your Domain Name System (DNS) that will allow the service to validate your domain. For example:

|  |  |  |
| --- | --- | --- |
| Associated Domain: | contoso.com  | (your domain) |
| Alias (sub domain): | 1955b1ad-cec0-4115-8041-ad91fd2d5a34 | (GUID) |
| Resource Record Type: | CNAME |  |
| Associated Domain: | admin.messaging.microsoft.com. | (hostname) |

Tip

You can copy this information and then click Cancel and come back later if needed.

6. In your domain’s DNS record, or in your ISP domain's DNS settings, add the CNAME entry and enter the GUID and hostname for each domain to the CNAME. If you have questions on how to add the CNAME, contact your DNS provider.

Tip

Be sure to include the period at the end of the hostname to your domain's DNS record. If this action fails, try removing the period from the end of the hostname before adding it to your domain’s DNS record. Some systems automatically add a period to the end of the hostname.

7. Allow enough time for the DNS changes to propagate, and then return to the Validate Domain dialog box and click Start to begin the validation process. During the validation process, a CNAME query is conducted to verify the entry. A successful match indicates that the domain has been validated.

Important

Propagation of domain DNS changes across all DNS servers on the Internet can take from a couple of minutes up to 72 hours. If the DNS CNAME validation fails, wait a little longer and then try again. If the domain validation is still failing after 72 hours, please check your domain's CNAME entry to verify that the GUID and hostname are correct. If you have verified the entry and the validation is still failing, please contact Technical Support for help.

8. Repeat these steps for all domains using the services.

To proceed to Step 2, go to [Enable Your Domain(s)](#zc3765f89ec764095bf4b14b1130c8eef)

## See Also

[Enable Your Domain(s)](#zc3765f89ec764095bf4b14b1130c8eef)

# Enable Your Domain(s)

## Step 2: Enable Your Domain(s)

1. On the Administration tab, click the Domains subtab.

2. In the Domains list, click the domain(s) you want to enable. To search for a domain, enter the name of the domain in the search box and click Go. The domain details page will open.

3. In the Tasks pane, click Enable Domain.

To proceed to Step 3, go to [Add Other Domains (If Desired)](#z3db7f58ca2124a3eadc8b339a90e6ab9)

## See Also

[Add Other Domains (If Desired)](#z3db7f58ca2124a3eadc8b339a90e6ab9)

# Add Other Domains (If Desired)

## Step 3: Add Other Domains (If Desired)

1. Click the Administration tab, and then click the Domains subtab.

2. In the Tasks pane, click Add Domains.

3. In the Add New Domains dialog box, type the name of the domain or domains that you want to add.

Multiple domains can be added at the same time by adding one domain per line in the Domain names: window. The service settings on an existing domain can be used as a template for the configuration of the domains being uploaded by entering the name of the existing domain in the Choose an existing Domain as template (optional) text box.

4. Click Save.

5. Follow Steps 1 and 2 above to validate and enable your new domains.

To proceed to Step 4, go to [Update Your MX Record](#zed860c81a4484a70aa0bbc60890d850c).

## See Also

[Update Your MX Record](#zed860c81a4484a70aa0bbc60890d850c)

# Update Your MX Record

## Step 4: Update Your MX Record

After your domain has been validated and enabled, change the MX record for your domains to mail.messaging.microsoft.com. Note that only one MX record is necessary, making the Priority option unnecessary at this point.

Important

Do not resolve mail.messaging.microsoft.com to an IP address. For optimal performance, this address should be your only MX record.

To proceed to Step 5, go to [Set up Outbound E-mail Filtering](#z5ca511c1b7204c5d80d30f274febc0b0)

## See Also

[Set up Outbound E-mail Filtering](#z5ca511c1b7204c5d80d30f274febc0b0)

# Set up Outbound E-mail Filtering

## Step 5: Set up Outbound E-mail Filtering

1. Ensure that the outbound domains you are using are not being used as open relays. (If your outbound IP address is found to be sending spam, it may be disabled to protect the rest of the network until the problem is resolved.)

How to add outbound IP addresses to your domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the IP Address Settings section of the center pane, next to Outbound IP Addresses, click Add.4. In the IP Addresses dialog box, enter the outbound IP addresses that you want the domain to use to send e-mail. Separate multiple IP addresses with a comma (,). |

5. Configure your e-mail server to direct all outbound e-mail messages to mail.messaging.microsoft.com.

Outbound access through the Forefront Online Protection for Exchange service network is IP and domain-restricted. All outbound e-mail messages that are sent through the Forefront Online Protection for Exchange pool of outbound e-mail servers are scanned for viruses, matches to Policy Filter rules, and spam characteristics before they are sent.

Important

Outbound e-mail from domains listed in the Administration Center will be delivered as normal by one Outbound Pool of IP addresses. E-mail classified as possible junk will still be delivered, but through a separate pool of IPs, known as the Higher Risk Delivery Pool. If an IP in the Higher Risk Delivery Pool is added to a third-party block list, the delivery of junk e-mail generated by compromised machines or improperly configured domains may be affected, whereas legitimate e-mail flow will not be affected.

To proceed to Step 6, go to [Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service](#zf1348ce82e88471e8dd5bd15c84f1671).

## See Also

[Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service](#zf1348ce82e88471e8dd5bd15c84f1671)

# Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service

## Step 6: Restrict Incoming E-mail to E-mail Sent through the Hosted Filtering Service

1. Wait 72 hours after changing your MX record to allow full propagation across the Internet.

2. Restrict inbound port-25 SMTP traffic on your firewall or mail server(s) to only accept mail from the Hosted Filtering service data centers. The current list of data center IP addresses are listed on the Configuration tab in the Administration Center.

To proceed to Step 7, go to [Set up E-mail Deferral Notifications](#z119b5f109f53410f9a703578447057af)

## See Also

[Set up E-mail Deferral Notifications](#z119b5f109f53410f9a703578447057af)

# Set up E-mail Deferral Notifications

## Step 7: Set up E-mail Deferral Notifications

Important

The Deferral Notification Alert must be set up to alert administrators if inbound e-mail is being deferred. In the event that the Forefront Online Protection for Exchange service servers cannot connect to your mail servers to deliver incoming e-mail, the service will automatically queue e-mail for later delivery, and then alert the addresses as determined by the Deferral Notification Alert settings.

1. On the Administration tab, click the Domains subtab.

2. Click the name of the domain you want to set up the deferral notification alerts for.

3. In the Notification Settings pane (lower left), select Activate next to Deferral Notification.

4. Enter the number of desired deferrals that can be allowed to occur before an administrator is notified, along with the administrator’s e-mail address.

Examples:

|  |
| --- |
| Notification 1: threshold=100, alert = network administrator  |
| Notification 2: threshold=500, alert = operations manager  |
| Notification 3: threshold=1000, alert = operations distribution list |

You have now completed the most essential setup steps. For an overview of other important service information, see [Forefront Online Protection for Exchange Service Highlights](#zfe17212be0ac43b8815d7405f62eba75).

## See Also

[Forefront Online Protection for Exchange Service Highlights](#zfe17212be0ac43b8815d7405f62eba75)

# Forefront Online Protection for Exchange Service Highlights

Our customers have found that knowing the following about their Forefront Online Protection for Exchange service has helped them get the most out of the service and ensure that it runs as smoothly as possible.

## Directory Synchronization Tool

The free Directory Synchronization Tool is a good way to securely and automatically synchronize valid end-user proxy addresses (and their Safe Senders if available) between an on-premise Active Directory and the Microsoft Forefront Online Protection for Exchange and Exchange Hosted Archive services. The Directory Synchronization Tool is located at the following address:<http://www.microsoft.com/downloads/details.aspx?FamilyID=3cda6dcc-1124-4e0b-b991-de9d85ed12e1&DisplayLang=en>

Once the Directory Synchronization Tool (DST), has been downloaded, a list of users (and their e-mail addresses) can be uploaded via the DST to the Hosted Services network. The uploaded list of users can then be used for Directory Based Edge Blocking (by setting the domain’s Directory Based Edge Blocking to Reject mode), Quarantine access, or Archive services.

If your company does not have a Microsoft Windows Active Directory environment, you can set the User List source to Admin Center or Secure FTP (alternate options for uploading user lists).

## SPF Record Settings

SPF is employed to prevent unauthorized use of a domain name when sending e-mail communications, a technique also known as "spoofing", by providing a mechanism to validate sending hosts. If you wish to configure SPF record settings, use the following tips as a guide:

1. For domains sending outbound through the filtering network, you can include "spf.messaging.microsoft.com" in your SPF record as well as your individual outbound mail server IP addresses. SPF is employed to prevent unauthorized use of a domain name when sending e-mail communications, a technique also known as "spoofing", by providing a mechanism to validate sending hosts.

Important

These instructions are only valid for domains sending e-mail outbound through the filtering network.

2. Since SPF is used to validate that a given IP address is authorized to send mail for a given domain, the outbound IP addresses for the filtering network will also need to be included in the SPF record. The easiest way to add the entire set of IPs is to use the "include: spf.messaging.microsoft.com" statement in your SPF record.

3. In addition to this, you can list all of your outbound mail server IP addresses. These IP addresses are required to ensure mail delivery to other clients of Forefront Online Protection for Exchange. Each IP address should be added via an ip4: statement. For example, to include "127.0.0.1" as an accepted outbound sending IP you would add "ip4:127.0.0.1" to your SPF record. If you know all of the authorized IPs they should be added using the –all (Fail) qualifier. If you are not sure that you have the complete list of IPs then you should use the ~all (SoftFail) qualifier.

Example:

|  |  |
| --- | --- |
| Contoso.com has three outbound mail servers as follows: | 127.0.0.1127.0.0.2127.0.0.3 |
| Contoso's original SPF record looked like this: | "v=spf1 ip4:127.0.0.1 ip4:127.0.0.2 ip4:127.0.0.3 -all" |
| After routing mail through FOPE Contoso's SPF record looks like this: | "v=spf1 include:spf.messaging.microsoft.com ip4:127.0.0.1 ip4:127.0.0.2 ip4:127.0.0.3 -all"  |

## Network Connection Settings

The following tips will help ensure a smooth and continuous data transfer to the Hosted Filtering service.

 Configure settings on the SMTP server with a connection time out of 60 seconds.

 Once your firewall rules have been restricted to only allow inbound SMTP connections from the IP addresses used by the Hosted Filtering service, we recommend that the SMTP server be configured to accept the highest number of concurrent inbound connections from the service that you feel comfortable with.

 If the server is sending outbound e-mail through the Hosted Filtering service, we also recommend that the server be configured to send no more than 50 messages per connection and to use fewer than 50 concurrent connections. Under normal circumstances, these settings will help ensure that the server has smooth and continuous data transfer to the service.

## Security

### IP Restrictions

Access to the subscribed services can be restricted to users connecting to the Web sites from specified IP addresses. Access from other IP addresses would not be allowed with this configuration, which minimizes probability of unauthorized access. IP restriction settings are available at the company scope, the domain scope, and at the user scope.

### Password Policies

Strong passwords should be used at all times and for all accounts, especially administrator accounts. Strong passwords adhere to the following rules:

 Require lower and upper case letters, numbers, and special characters (?, !, @, $)

 Passwords should be set to expire frequently, such as every 3, 4, or 6 months.

### Additional Spam Filtering Options

Additional spam filtering (ASF) options are also available. Consider enabling these options in Test mode to identify additional aggressive spam options in order to maximize spam blocking based upon your environment.

Customers should submit any spam that gets through to their desktop to the Hosted Filtering service Spam Team at abuse@messaging.microsoft.com for review.

Customers also have the option of allowing their end users to install the Junk E-mail Reporting Tool. For use with Microsoft® Office Outlook®, the Junk E-mail Reporting Tool enables the end user to quickly submit junk e-mail messages to abuse@messaging.microsoft.com for analysis to improve junk e-mail filtering effectiveness.

The Junk E-mail Reporting Tool can be downloaded here: <http://www.microsoft.com/downloads/details.aspx?FamilyID=53541292-ce94-4c5b-9127-b7d56f11b619&displaylang=en>

It is also possible to configure your domain to display the download link for the Junk E-mail Reporting Tool to the end users when they sign into the Quarantine web site.

The following additional spam filtering options are recommended:

 Images from remote sites

 Numeric IP in URL

 Empty messages

These rules may be added to increase spam blocking above 95% with little risk to increasing false positives.

For customers with high spam percentages, we recommend that you first test these rules before implementing them in your production environment.

## False-Positive Submissions

The vast majority of messages submitted as false positives are indeed spam messages that were accurately filtered, but are still wanted by the intended recipients.

In order to gain insight into the type and number of messages reported to the Hosted Filtering service as false positives, administrators should configure the false positive submission copy feature of the spam filter to provide them with a copy of the messages for review.

Important

Prior to sending false-positive submission, end users must either sign in to the Quarantine Web site to view the message first, or salvage the message to view it, and then forward to false\_positive@messaging.microsoft.com.

False positive messages must be submitted by forwarding the entire message and all Internet headers to the false\_positive mailbox.

## Policy Filters

### Policy Rules

In addition to spam and virus filtering, the Administration Center Policy Rules allow you to enforce specific company policies by configuring customizable filtering rules. You can create a specific set of rules that identify messages and take a specific action against them while they are being processed by the Hosted Filtering service. For example, you can create a policy rule that will reject any incoming e-mails that have a certain word or phrase in the Subject field. Additionally, Policy Rules Filters allow you to add and manage large lists of values (such as e-mail addresses, domains, and keywords) for multiple policy rules by uploading a file (Dictionary).

Policy rules can be configured for a variety of e-mail match criteria:

 Header field names and values

 Sender IP addresses, domains, and e-mail addresses

 Recipient domains and e-mail addresses

 Attachment file names and file extensions

 E-mail subject, body, and other message properties (size, number of recipients)

For more information about Policy Rules, see [Policy Rules](#zd43d92b98b8c43a3869b6bb4ca4e0682).

### Phishing and Spoofing Prevention

The policy filter may be used to defend corporate networks from e-mail attacks and protect end users’ confidential information.

Additional anti-phishing protection can be accomplished through the detection of personal information in e-mails exiting the organization. The following regular expressions, for example, can be used to detect transmission of personal financial data or information that may compromise privacy:

 \d\d\d\d\ \d\d\d\d\ \d\d\d\d \d\d\d\d (MasterCard, Visa)

 \d\d\d\d \d\d\d\d\d\d \d\d\d\d\d\d (American Express)

 \d\d\d\d\d\d\d\d\d\d\d\d\d\d\d\d (Any 16-digit number)

 \d\d\d\-\d\d-d\d\d\d (Social Security Numbers)

Spam and Anti-phishing can be prevented by blocking inbound e-mails that appear to have been sent from your own domain. Create a reject rule for messages from yourdomain.com sent to yourdomain.com to block this type of sender forgery.

Important

This rule should only be created if you are certain that no legitimate e-mail from your domain is sent from the Internet to your mail server.

### Extension Blocking

The policy filter can be used in various ways to defend corporate networks from e-mail attacks and protect end users’ confidential information.

Threat prevention through file extension blocking

 At a minimum, the following extensions should be blocked: EXE, PIF, SCR, VBS

 For increased protection, blocking some or all of the following extensions is recommended:ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, exe, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh

## See Also

[Set Up Forefront Online Protection for Exchange](#zf6a25070863b424eba5b4d589a185bf6)

[Additional Resources: Forefront Online Protection for Exchange Setup Checklist and Service Highlights](#zff2af85a903144beb342e8698997f2d0)

# Additional Resources: Forefront Online Protection for Exchange Setup Checklist and Service Highlights

You can find more information about configuring and using Forefront Online Protection for Exchange online:

 In the Administration Center, under the Information tab, the Resources subtab contains Administration Center content that you can use to help roll out the service to end users.

 [Administration Center User Guide](http://go.microsoft.com/fwlink/?LinkID=135918): Comprehensive information about service configuration and settings.

 [Online training](http://go.microsoft.com/fwlink/?LinkID=137241): Offers an overview of the Administration Center site, along with more tips for setting up and configuring your FOPE service.

## See Also

[Forefront Online Protection for Exchange Setup Checklist and Service Highlights](#ze0e0be99c3d34c4fb4f3a161722d2318)

# Forefront Online Protection for Exchange Administration Center Help

Browse the Administration Center Help for information about how to manage your Microsoft Forefront Online Protection for Exchange service.

[About the Administration Center](#z7867057515454f8bbd2efb482c16b6af)

[Sign in and out of the Administration Center](#z8d3aa94a54b547f1940bc08cfa0633be)

[Quick Search](#zd7edb899236c48a481db5cf91e59e2bc)

[Supported Browsers](#z4df09e9954bc41ebb5315f9f944e4951)

# About the Administration Center

The Administration Center is a Web portal that you, the service administrator, use to manage settings for your company, its user accounts, and the Forefront Online Protection for Exchange and Exchange Hosted Archive (EHA) services that your company has subscribed to.

## Core features of the Administration Center

 [Information Tab](#z2dc70ee350104e27a9624429e0361175): The Information tab displays service announcements and alerts, and filters reports at the company and network levels.

 [Administration Tab](#z96dfed413ad546c68e0443d4e407d28c): The Administration tab provides you with a single point of administration for all of your hosted services. From this tab, you can manage both FOPE and EHA settings for your company, domains, users, and policy rules.

 [My Reports Tab](#z873ec87299ac4408bdedbba083114892): With the My Reports tab, you can create and run reports for all of your services.

 [Tools Tab](#zee60700b99524e85803a60d7e826ad6b): From the Tools tab, you can trace messages and view service events by using the Audit Trail feature.

 Advanced: If you are an Administrator with permission to more than one company in the Administration Center, then you will have access to the Advanced tab. It displays a list view of all of the companies that a user has permission to view. This tab is not displayed if the user has permission to view only one company.

# Sign in and out of the Administration Center

The Administration Center is a Web console that allows you to administer your Forefront Online Protection for Exchange (FOPE) and Microsoft Exchange Hosted Archive (EHA) services.

How to log on to the Administration Center

|  |
| --- |
| 1. From your Web browser, go to the Administration Center sign-in page.2. Type your user name and password, and then click Sign in.  |

# Quick Search

The Quick Search feature allows you quickly find domains, users, or policy rules without having to navigate through the Administration Center user interface.

How to use the Quick Search feature

|  |
| --- |
| 1. In the upper right area of the Administration Center, click Quick Search.2. In the Quick Search dialog box, select the type of item (domain name, e-mail address, or policy rule ID) you want to search for. 3. Enter the name of the item in the corresponding search box, and then click Search.The search will direct you to the appropriate page within the Administration Center. |

# Supported Browsers

To use the Administration Center, you must use one of the following Internet browsers:

 Microsoft Internet Explorer 6

 Internet Explorer 7 and 8

 Mozilla Firefox 3

 Safari 3

# Supported Languages

The Administration Center may be viewed in the following languages:

 Simplified Chinese

 Traditional Chinese

 Dutch

 French

 French Canadian

 German

 Italian

 Japanese

 Korean

 Portuguese

 Portuguese (Brazil)

 Spanish

## How to Set the Language Preference

In order to view the Administration Center in one of the 13 supported languages, your Internet browser’s language preferences must be configured to accept the appropriate language(s). Forefront Online Protection for Exchangesupports the following browsers:

1. Microsoft Internet Explorer 6

2. Windows Internet Explorer 7 and 8

3. Firefox 3

4. Safari 3

How to set language preferences for Internet Explorer 7

|  |
| --- |
| 1. Using Internet Explorer 7, open a browser 2. On the Tools menu, click Internet Options3. Click the General tab4. Select Languages5. Select Language Preference6. Add the language you would like to see when using the Administration Center |

How to set language preferences for Internet Explorer 8

|  |
| --- |
| 1. Using Internet Explorer 8, open a browser 2. On the Tools menu, click Internet Options3. On the General tab, click Languages4. In the Language Preference box, click Add5. Add the language you would like to see when using the Administration Center |

How to set language preferences for Firefox 3

|  |
| --- |
| 1. Using Firefox 3, open a browser 2. On the Tools menu, click Options3. Click the Content tab4. Select Languages5. Click the Choose button6. Choose the language you would like to see when using the Administration Center |

How to set language preferences for Safari 3

|  |
| --- |
| 1. Using Safari 3, open a browser 2. Select System preferences3. Select International4. Select Language5. Select the language you would like to see when using the Administration Center |

# Information Tab

On the Information tab of the Administration Center, you can view service announcements from the Technical Support and Operations teams, along with other helpful information such as virus and network alerts.

[Service Statistics](#z785ae032b8744455a3d1a1a5d5a001b3)

[Welcome Pane](#zef0dbdefbca84557b6cabfe57d4cf81a)

# Service Statistics

On the Information tab, you can view e-mail filtering information about the Hosted Filtering service and for the domains in your company. These service reports will give you an idea of how the traffic for your company compares with the traffic for the service as a whole. Reports can be filtered to show information for the previous 30, 90, 180, or 365 days.

Service reports available on the Information tab:

Filtering Report: This report shows you what types of e-mail were filtered for all domains in your company.

Network Report: This report shows filtering statistics for the entire Forefront Online Protection for Exchange service.

# Welcome Pane

The Welcome pane in the center of the Information tab provides the most up-to-date information about your Hosted Services. Announcements are separated into sectional tabs. Be sure to check the Welcome pane frequently, as it always offers the most up-to-date information about the service.

Tabs on the Welcome pane:

 Announcements — This tab includes general information about upcoming changes to the services, new releases, and new feature announcements.

 Network Alerts — This tab includes information about any scheduled maintenance updates or service-wide issues.

 Virus Alerts — This tab includes specific information about high-risk virus threats if and when they may be a threat.

 Resources — This tab is updated regularly with links to service documentation and technical support information.

 Training — This tab contains links to automated, self-paced training.

 Configuration — This tab displays the list of IP addresses that correspond to inbound Simple Mail Transfer Protocol (SMTP) data centers for your filtering services.

Note

To receive the maximum benefit from your services, restrict your inbound SMTP connections on port 25 so that they only allow e-mail from this list of IP addresses.
These restrictions should be placed on your firewall 72 hours after changes are made to the mail exchange (MX) record. This will ensure complete Internet propagation. If you have settings on your mail server that control the IP addresses that are allowed to connect for mail relay, ensure that those settings are also updated.

# Administration Tab

The Administration tab provides a single point of administration for all of your hosted services. From this tab, you can manage service settings for company, domains, users, and policy rules.

## Tabs on the Administration tab:

 Company—On this tab, you can update your company-wide settings, including the following:

 Default language and time zone settings

 Contacts

 Company security settings

 Hosted Archive settings

 Domains—The tools on this tab allow you to view and modify domain-level settings for each domain in your company. Additionally, you can edit domain setting options for your Hosted Filtering service, domain-level retention periods, and domain-level Legal Hold settings for your Hosted Archive service.

 Users—Here, you can manage all of the user accounts for your hosted services. From the tabs on this tab, you can create and delete user accounts, change passwords, assign permissions, and modify user account service settings. You can also edit user-level retention periods and user-level Legal Hold settings for your Hosted Archive service.

 Policy Rules— On this tab, you can create new policy rules for your domains, and update Hosted Filtering and Hosted Archive policy rules.

 Filters — The tools on this tab allow you to add and manage large lists of values, called Dictionaries, for policy rules.

# Tasks and Views Pane

On most tabs of the Administration Center, important tasks are now available in the Tasks pane.

Each Tasks pane provides links to the most commonly used tasks for a feature or functional area. The Tasks pane helps you complete the most important tasks for your service without having to navigate through multiple tabs. When Track Changes is selected, you will be taken directly to a filtered view of the audit trail, where you can view the changes which apply specifically to the property you were viewing. When investigating changes to an object, use the Track Changes feature from the properties of that object to make the filtering the audit trail information more simple.

The View pane filters items according to a specific set of criteria, to provide you with quick access to the items that you need to manage. The View pane is available for Domains, Users, Policy Rules, Reports, and Audit Trail events.

# Company Settings

On the Company tab on the Administration tab, you can modify settings that apply to your company and the domains within your company. The following sections provide further information about these settings.

[Edit Company Preferences](#z54fc0e2d17464304b6ad65856c2f68a8)

[View Service Subscriptions](#z7bcb688bd9444aabb376fc8d65394833)

[Company Contacts](#z084332489921470292fafe1465f76dda)

# Edit Company Preferences

You can edit your company settings to match your company’s preferred language and time zone settings. The language and time zone preferences can be configured at the domain or user level. The most specific (detailed) setting will be applied; for example, if the domain-level preferences are most specific, these are the preferences that will be applied.
Time zone preference will automatically pre-populate message traces and reports with the specified time zone.
Language preferences are applied to spam notifications and the archive viewer Web pages.

How to update your company’s language and time zone settings

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Company Settings pane, click Edit.3. In the Preferences dialog box, select the notification language and time zone settings for your company. For a list of time zone settings, see [Microsoft Time Zone Index Values](http://msdn.microsoft.com/en-us/library/ms912391.aspx) 4. Click Save.  |

# View Service Subscriptions

You can view the current hosted service subscriptions that are configured for your company.
The seat count for each service is also listed here. Seat count refers to the actual number of users, not the number of e-mail addresses or domains in your organization. This field is based on your service contract, and your billing is based on this number.

# Company Contacts

The Administration Center provides separate entries for your company’s important contacts; for example, main contact, technical contact, account manager, compliance manager. This information will be used to contact people within your company when there are issues with the service, which makes it important for you to keep contact information, including off-hours information, up to date.

Any contacts listed here will receive status updates about the service. They are also authorized to request help with making changes on behalf of the company when contacting technical support. Contact types may be different depending on the services to which you are subscribed.

How to add a contact for your service

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Contacts pane, click Add.3. In the Contact dialog box, fill out the information for this contact.4. Click Save.  |

How to edit a contact for your service

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Contacts pane, click Edit next to the contact that you want to edit.3. In the Contact dialog box, update the contact information.4. Click Save. |

How to delete a contact for your service

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Contacts pane, click Remove next to the contact that you want to edit.3. When prompted to confirm your choice, click OK to remove this contact. |

# Company IP Address Settings

The following topics provide information about the IP address features and how to configure your company’s IP address settings.

[Inbound Multi-SMTP Profiles](#ze30e311011d4432882229b49febfa56d)

[Outbound IP Address Settings](#z15356e00b49e4c9e847df17d9a43cbe6)

# Inbound Multi-SMTP Profiles

For each domain in your company, you must specify an incoming mail server IP address that your inbound e-mail messages can be delivered to after they have been filtered. If you have multiple mail server IP addresses, you can create an inbound multi-SMTP profile that will cause e-mail to be delivered to multiple mail servers in your network by using what is known as round-robin load balancing.

With round-robin load balancing, if the mail server delivering messages to your domain is required to open multiple connections to transfer multiple messages, it won’t always select the exact same IP address to connect to. This switching of IPs is dependent on two things: First, the mail server initiating conversation must be aware that the other IP has already been contacted. Second, the weight on the IPs must be equal, otherwise it will continue attempting to connect to the lowest-weighted IP.
Note that you can create multiple multi-SMTP profiles for a single company.

# Create an Inbound Multi-SMTP Profile

After you create your inbound multi-SMTP profiles, they are available to individual domains.

Important

All messages that are processed by the hosted filtering service will use these inbound server settings to deliver messages to your domain. It is critical that this information (IP settings) be kept up-to-date at all times.

How to create a multi-SMTP profile

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the IP Address Settings section of the center pane, next to Inbound Multi-SMTP Profiles, click Add. The Inbound Multi-SMTP Profile Settings dialog box should appear.3. In the Mail servers area, type the mail server IP addresses and assign them an MX priority. Use one line per entry. For each entry, separate the IP address and the MX priority/weight with a space. Example: 192.168.0.1 10192.168.0.2 15192.168.0.3 20In this example, the numbers 10, 15, and 20 represent the MX priorities, or weight. The IP with the lowest number (lightest weight) – in this case, the IP ending in 10 is preferred, and the higher-weighted IPs will only be used if the lower-weighted IPs fail to respond to the connection attempts.4. In the Profile name box, type the name of your profile. You will assign this profile name to your domains.5. Click Save.  |

The following image shows the Inbound Multi-SMTP Profile Settings box.



# Delete an Inbound Multi-SMTP Profile

You can delete an inbound multi-SMTP profile if it is no longer in use. When you delete a profile, the profile information is completely eliminated from your service.

Important

Before you can delete a profile, you must first remove the profile from the inbound IP address settings of all the domains that use it. If the profile is being used by a domain, the service does not allow you delete the profile and you receive an error message.

How to delete an inbound multi-SMTP profile

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the IP Address Settings section, next to Inbound Multi-SMTP Profiles, click Remove next to the profile that you want to delete.3. When prompted, click OK to confirm that you want to remove the profile. |

# Outbound IP Address Settings

If you have outbound e-mail servers that are configured to use the Microsoft® Forefront™ Online Security for Exchange (FOSE) service, you must add the IP addresses of those servers to your service by using the Administration Center.

All outbound e-mail that is sent through the FOSE pool of e-mail servers is scanned for viruses, scanned that it matches to policy filter rules, and scanned for spam characteristics before it is sent. Outbound e-mail from domains listed and enabled in the Administration Center will be delivered by one Outbound Pool of IP addresses. E-mail classified as possible junk will still be delivered, but through a separate pool of IPs, known as the Higher Risk Delivery Pool. If an IP in the Higher Risk Delivery Pool is added to a receiver’s blocked list, the delivery of junk e-mail generated by compromised machines or improperly configured domains may be affected, whereas legitimate e-mail flow will not be affected.

This filtering process helps reduce the risk of spam being sent from the hosted filtering environment, which could lead to some of the outbound IP addresses of the hosted filtering service being blocked by companies and by other security organizations.

Important

If your outbound IP address is found to be sending spam, it may be disabled to protect the rest of the network until the problem is resolved.

You will need to specify the IP addresses for all servers that are configured for routing outbound e-mail through the hosted filtering service.
If you are using envelope journaling, which archives full mail delivery information such as SMTP MAIL FROM, list of actual recipients, or blind carbon copy recipients with the hosted archive service, then the IP addresses for the servers that are sending the journaled messages must be specified in this setting as well. For details about how to specify the IP addresses, see the [Edit Domain Services](#zff2f3b0769fb46cd96952d54989d9f4b) topic.

# Add Outbound IP Addresses

Outbound IP addresses can be configured on a company-wide level or specifically on each domain.

To add an outbound e-mail IP address to your service

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the IP Address Settings section in the center pane, next to Outbound IP Addresses, click Add.3. In the Add Outbound IP Addresses dialog box, enter the IP addresses of the outbound mail servers that will use the outbound filtering service. Separate multiple IP addresses with a comma.4. Click Save. |

# Delete Outbound IP Addresses

If you are no longer using the outbound Hosted Filtering service for an outbound IP address, you should remove it from your service settings.

How to delete an outbound e-mail IP address from your service

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the IP Address Settings section of the center pan, next to Outbound IP Addresses, click Remove next to the IP address that you want to delete.3. When prompted to confirm the deletion, click OK. |

# Company Service Settings

You can access the following two company service settings on the Administration Tab:

[Filtering Settings](#z8a264799f5464e4cb31f191ef5227112)

[Archive Settings](#z8cb1ce9ac1b14f82ac9384b959f43b61)

# Filtering Settings

The user list upload notification address in the Filtering Settings section is where the notification address to be used as the domain default is entered. After you begin the upload process, status notifications are sent to the e-mail address you specified in this field. This address will be read by the Directory Synchronization Tool (DST) and will be the default address displayed in the Administration Center manual user list upload dialog box. You can overwrite this address in the Import Users From File dialog box that is launched from the Users tab and change it in the User List Settings section of a specific domain through the Administration Center. However, you cannot change it in the DST version 9.1.

How to configure the User List upload notification address

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Service Settings section of the center pane, click Edit.3. In the User List upload notification address: text box enter the address that should receive the user list upload notifications.4. Click Save.  |

Note

The e-mail address specified here must belong to one of the domains that is configured for your company.

## See Also

[Archive Settings](#z8cb1ce9ac1b14f82ac9384b959f43b61)

# Archive Setting

If you subscribe to the Exchange Hosted Archive service you will be able to see some of your archive settings here.

## See Also

[Filtering Settings](#z8a264799f5464e4cb31f191ef5227112)

# Edit Company-Wide Archive Settings

Archive settings can be configured at multiple levels. Company-wide settings are the default settings for all domains and all users. A setting made at the domain level will override the company default. Settings configured at the user level override both the domain and company settings. This allows customization of archive settings down to the user level.

How to edit company-wide archive settings

|  |
| --- |
| 1. On the Administration tab, click the Company subtab.2. In the Service Settings section of the center pane, next to Archive Settings, click Edit.3. Set the archive settings and then click Save. |

The following table summarizes the configuration options that are available.

| **Option** | **Description** |
| --- | --- |
| Administrator alert | Selects whether users can receive Administrator alerts from Hosted Archive services. |
| Exclude users | Selects whether to enable excluding specific users from the archive. |
| Internal messages | Selects whether to automatically mark internal messages as reviewed. |
| Message review | Selects whether to activate daily message harvest to capture messages for review based on sampling rates and keyword lists. |
| Legal hold | Selects whether to suspend message destruction for the entire company. Messages reaching the end of their retention period will not be destroyed while legal hold is enabled. |
| Journaling address | Sets the Journaling address for Envelope Journaling. This setting is configured during service activation. |
| IM copy address | This setting is configured by Technical Support. Contact support if your company will be archiving instant messages. |
| Retention period | Defines how long messages will be held in the archive before they are destroyed. |
| Tombstone policy | Selects Tombstone policy which defines archive behavior after message expiration. Available options include:  Permanent deletion: Message is fully deleted. Minimal: The time, date and recipients are retained, and the rest of the message is deleted. Full headers: The time, date, recipients, subject, attachment, and delivery path are retained, and the rest of the message is deleted. |
| Tombstone retention period | Sets the Retention period for Minimal and Full header tombstones. |

Note

To configure archiving for your organization’s Bloomberg messages, contact Technical Support.

# Add a Keyword List

You can set keyword lists for nightly message harvest, which will capture messages containing the keywords for supervisors and compliance managers to review.
Before you add a keyword list, you need to create a text file listing the desired keywords.

How to add a keyword list

|  |
| --- |
| 1. On the Administration tab, click the Company subtab.2. In the Service Settings section of the center pane, next to Keywords List, click Add.3. On the Add keyword list dialog box, type a name for the keyword list in the Name box, and then click Browse to navigate to the text file containing the keywords.4. Click Save. |

# Security

The following topics provide information about how to set up and configure security settings for your company.

[Add IP Address Restrictions](#z439c2edb871644d7b232408de07e206c)

[Create a Password Policy](#zd40342023118401d87765160e23ae0dc)

[Edit Password Policy Settings](#za6d3ca8add7a4e06b003b9900fb49f2c)

# Add IP Address Restrictions

As a security precaution, you can restrict user access to all hosted services Web sites and applications, limiting access to a specific set of IP addresses for users within your company. Restrictions can be set at company, domain, and individual user levels. The restriction configuration supports entries at the IP subnet mask level, or for individual IP addresses.

How to create an IP restriction rule

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Security pane, next to IP Address Restriction, click Add.3. In the Add Allowed IP Addresses dialog box, in the IP addresses area, add the list of IP addresses that will be allowed to access hosted services Web sites and applications. You can enter a single IP address (192.168.0.1) or an IP subnet mask (192.168.0.1/24). Use one line for each entry. 4. Click Save.  |

Warning

IP restrictions affect access to all hosted services Web applications. Users with Administrative permissions to the Administration Center will not have IP restrictions applied to their accounts.

# Create a Password Policy

To help comply with varying corporate password policies, you have the option of creating password policies for user accounts. Password policies are enforced at the company level and apply to all user accounts. If the password policy changes for your company, then the users who are out of compliance will be required to change their passwords the next time they log in.

How to create a password policy

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Security pane, next to Password Policy, click Add.3. In the Password Policy dialog box, enter the password policy settings you want to use. For a description of each policy setting, see the password policy options table below.4. Click Save. |

## Password Policy Options

| **Policy option** | **Description** |
| --- | --- |
| Minimum password length | The minimum number of characters for a password. |
| Maximum password length | The maximum number of characters for a password. |
| Maximum password age for administrators (days) | The number of days before administrator passwords expire. |
| Maximum password age for users (days) | The number of days before user passwords expire. |
| Allow password reuse | Specifies that users can use their existing passwords when they are prompted by the service to create a new one. By default, users must create unique passwords for each mandatory password change. |
| Allow only alphanumeric characters | Specifies that all passwords must contain both letters and numbers. By default, user passwords are not required to contain a mix of letters and numbers. |
| Require a mix of uppercase and lowercase letters | Specifies that users must use both uppercase and lowercase letters in passwords. By default, user passwords can contain any combination of lowercase and uppercase letters.  |
| Allow duplicate, consecutive characters | Specifies that users can use the same character consecutively in a password. By default, no duplicate consecutive characters are permitted. |
| Allow user name as password | Specifies that users can set their own user name as their password. By default, users cannot set their user name as their password. |
| Allow reversed user names in passwords | Specifies that users can use a reversed version of their user name as their password. By default, users cannot use a reversed version of their user name as their password. |

# Edit Password Policy Settings

To update your password policy, you can edit your existing policy or delete it and create a new one.

How to edit an existing password policy

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Security pane, next to Password Policy, click Edit. 3. In the Password Policy dialog box, update the password policy settings, and then click Save. For a complete description of the password policy settings, see the options table in the [Create a Password Policy](#zd40342023118401d87765160e23ae0dc) topic.4. Click Save. |

How to delete a password policy

|  |
| --- |
| 1. On the Administration tab, click the Company tab.2. In the Security pane, next to Password Policy, click the delete icon (red X).3. When prompted, click OK to confirm your deletion. |

# Create a Custom Archive Role

In addition to the standard archive roles provided, you can add new archive roles with customized permissions. The standard archive roles can be used as templates for custom roles by selecting a standard role and adding or subtracting permissions.

How to create a custom archive role

|  |
| --- |
| 1. On the Administration tab, click the Company subtab.2. In the Security section of the center pane, next to Custom User Roles, click Add.3. In the Add Custom User Role dialog box, type a name for the user role in the Name box, and then select the check box(es) next to the archive permissions you want. You can also use a standard role as a template by selecting it from the Template box and then using the check box(es) to add or remove permissions.4. Click Save. The following table summarizes the permissions that are available. |

| **Permission** | **Description** |
| --- | --- |
| Customer Extended | Reserved for future use. |
| Customer Data Import | Reserved for future use. |
| Customer Limited | Allows users to see alerts in the Hosted Archive. |
| Customer Report | Allows users to run System Statistics and Audit Events reports. |
| Customer Retention Report | Reserved for future use. |
| Customer Review | Allows users to view attorney-client privileged rules, and policy based exclusion rules, and company-wide dictionaries. |
| Customer Review Report | Reserved for future use. |
| Folder Extended | Allows users to shore folders or remove sharing permissions for folders. |
| Folder Limited | Allows users to view and update their own folders or folders shared to them. |
| Message All | Allows users to view, search, export, restore, copy, and annotate all messages in the Hosted Archive. |
| Message All Handle Escalation | Allows users to view, search, export, restore, copy, escalate, and annotate all escalated messages in the Hosted Archive. |
| Message All Report | Allows users to run the following reports: Activity Summary, Archive Summary, Attachment Summary, Daily Statistics, Destruction, Email Summary, SEC 17a-4. |
| Message All Review | Allows users to view, search, export, restore, review, copy, annotate, and update all harvested messages in the Hosted Archive. |
| Message All Review Report | Allows users to run Supervisory Review Evidentiary report. |
| Message Handle Escalation | Allows users to view, search, export, restore, copy, escalate, and annotate messages escalated to them. |
| Message Individual | Allows users to view, search, export, restore, copy, and annotate their own messages. |
| Message Review | Allows users to view, search, export, restore, review, copy, annotate, and update harvested messages belonging to the users’ subordinates. |
| Message Shared Limited | Allows users to view, search, export, restore, copy, and annotate messages shared to them. |
| Message Subordinate | Allows users to view, search, export, restore, copy, and annotate subordinate’s messages. |
| Notification E-mail Send | Allows users to send emergency notification messages from within the Archive Viewer. |
| Relationship All Report | Reserved for future use. |
| Relationship Individual | Allows users to view details and summary of their own relationships. |
| User All Report | Allows users to run the following reports: Activity Summary, Archive Summary, Attachment Summary, Daily statistics, Email Summary, Employee Roster, SEC 17a-4, Supervisory Review Evidentiary, Privileged Roles. |
| User Extended | Reserved for future use. |
| User Limited | Allows users to view alerts posted by the Exchange Hosted Service. |
| Viewer Login | Allows users to sign in to the Archive Viewer. |

# Send Emergency Notification

You can send notification messages for emergency.
In the event of a disaster, it is important to set up communications with users. Notifications keep users apprised of events and of what to do in emergency situations.

How to send an emergency notification

|  |
| --- |
| 1. On the Administration tab, click the Company subtab.2. In the Tasks pane, click Send Emergency Notification. The New Message window in the Archive Viewer will be displayed.3. Create the message, including recipients, subject, message text and any attachments, and then click Send to send the message. |

# Domain Management

The Domains tab of the Administration Center allows you as an administrator to update service settings for individual domains. You can get a quick view of some of the basic settings to your domains such as whether they are enabled, or configured as Catch-All domains; if they are Virtual Domains, or when they were initially created in the Administration Center.

You can also complete tasks such as adding new domains, disabling or deleting domains, or enabling domains so that they can be used as part of your service. Domains must be enabled before the services that they have subscribed to will be able to apply the configured settings. To delete a domain, you must first disable the domain. The Disabled Domains view includes a button for deleting the disabled domain. Note that the Delete button is not available to customers with the Hosted Archive Service subscription.

# Add a New Domain

You can add domains for your company in the Administration Center, by using the Domains tab on the Administration tab.

How to add a new domain to your company

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Tasks pane, click Add Domains.3. In the Add New Domains dialog box, type the name of the domain or domains that you want to add. Multiple domains can be added at the same time by adding one domain per line in the Domain names: window. The service settings on an existing domain can be used as a template for the configuration of the domains being uploaded by entering the name of the existing domain in the Choose an existing Domain as template (optional) text box.4. Click Save.  |

Note

The domain will be added to your company’s list of domains; however, it cannot be enabled until it has been validated. For information about how to validate a domain, see [Validate a Domain](#z0f5b7b94c1434a20b33abaf55b1b81c7).

# Transfer Settings

When you add new domains, you have the option of using settings that are available on an existing domain as a template for the new domains. You can also use the Transfer Settings button to transfer the domain settings of one domain to all of the domains you selected in the active page of the domains list view. Enter a source domain, and then select the settings you want to transfer.

The following settings can be transferred from one domain to another:

 Language, time zone, and IP addresses

 Archive settings (requires Archive subscription)

 Spam filtering (enabled/disabled)

 Virus filtering notification

 Policy filtering (enabled/disabled; copy Outbound Footer to other domains)

 Policy rules

 Spam, policy quarantine, and notifications

 Directory-based edge blocking

 Deferral monitoring notifications

 E-mail encryption settings (requires Encryption subscription)

 User list settings

The User List Settings menu contains the following options:

 Blank (default option)

 Transfer User List Source/Disable DBEB

 Verify User List Source/Transfer DBEB

If you leave the User List Settings field blank, no action will be performed.

If you select Transfer User List Source/Disable DBEB, the user list source value of the source domain will be copied to the destination domains. The Directory-Based Edge Blocking (DBEB) setting of each destination domain will be set to Disabled.

If you select Verify User List Source/Transfer DBEB, the system will verify that the user list source of the source domain and the destination domains is the same. The Directory-Based Edge Blocking (DBEB) source domain will be copied to each destination domain

Note

If the source or one or more of the destination domains selected is a virtual domain, this operation will fail because you cannot conduct transfer settings for user list settings.

Important

If you have selected the Transfer Settings (all pages) option, the settings will be applied to all domains for the current view. By doing this, you will override any existing domain settings for your target domains. Therefore, make sure that only the domains that should be modified are selected.

# Validate a Domain

Before you can begin using the Forefront Online Protection for Exchange Filtering service with a newly added domain, you must validate the domain in the Administration Center. When you validate a domain, you ensure that your company is the owner of the domain and that you have the right to process e-mail for that domain through our services.

How to validate a domain

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list select the domain you want to validate from the domains list by clicking the domain name (or search for the specific domain you want to validate by using the search box). 3. From the domain properties, click Validate Domain in the Tasks pane.4. In the Validate Domain dialog box, you can see the domain alias (or subdomain) and hostname "admin.messaging.microsoft.com." for the canonical name (CNAME) entry that needs to be created within your Domain Name System (DNS).

| **Example** |  |
| --- | --- |
| Associated Domain: | contoso.com (your domain) |
| Alias (sub domain): | 1955b1ad-cec0-4115-8041-ad91fd2d5a34 (GUID) |
| Resource Record Type: | Canonical name (CNAME) |
| Value: | admin.messaging.microsoft.com. (hostname) |

5. Keep the Validate Domain dialog opened and add this GUID and hostname to the CNAME entry of your domain’s DNS record (or ISP domain's DNS settings). The steps required for adding the CNAME can differ depending on your DNS provider. If you have questions on how to add the CNAME, please contact your specific DNS provider for instructions. For general information about how to do this, see [Validate DNS Settings for a Domain](#z953b2a4df2d34ac0b2363fc567b79407).Note Please ensure that you add the period after the TLD of the hostname mentioned in the Validate Domain dialog box to your domain's DNS record. The GUID and hostname shown in the Validate Domain dialog box will not change if you select Cancel and return later.6. After you have successfully added the new CNAME entry to your DNS settings and enough time has passed to ensure that the changes have been applied correctly, click Start to begin the validation process. During the validation process, a CNAME query is conducted to verify the entry. A successful match indicates that the domain has been validated.Note Propagation of domain DNS changes across all DNS servers on the Internet can take from a couple of minutes to up to 72 hours. If the DNS CNAME validation fails, please come back and try again later. If the domain validation is still failing after 72 hours, please check your domain's CNAME entry to verify that the GUID and hostname are correct. If you have verified the entry and the validation is still failing, please contact Technical Support for help. |

# Validate DNS Settings for a Domain

During the domain validation process, you must add a CNAME or alias entry to your DNS record. DNS records are usually managed by one of these three authorities:

 A domain registrar (a company, accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) or by a national ccTLD (country code top-level domain) authority, to register Internet domain names). Click here for a list of ICANN Accredited Registrars: <http://www.icann.org/en/registrars/accredited-list.html>.

 A domain reseller or Internet hosting provider (these companies use ICANN accredited registrars to order domains and change DNS settings).

 Your internal IT department that manages your own DNS server (name server) for your domains.

The following instructions provide general guidance about how to update DNS settings for your domain.

How to add a CNAME or alias entry to DNS settings

|  |
| --- |
| 1. Log on to your company’s domain registrar account. 2. In another browser window or tab, log onto the Administration Center, click the Administration tab, and then click the Domains tab.3. Click the name of the domain that you need to validate.4. In the Tasks pane, click Validate Domain.5. In the Validate Domain dialog box, copy the GUID that appears in the second paragraph for Alias. Do not click Start.6. In your domain DNS settings, select or add the CNAME for the RR-Type (Resource Record Type), paste the GUID that you've copied to the alias or sub domain, and add the hostname "admin.messaging.microsoft.com." as the value of the CNAME entry.Note Please ensure that you add the period after the TLD of the hostname mentioned in the Validate Domain dialog box to your domain's DNS record. 7. Save your changes in your DNS record, and then log out of your domain registrar account.Note It takes between 15 minutes and 72 hours for the alias you created on your domain registrar account to propagate (spread across the Internet through replication). |

# Enable or Disable a Domain

Before a domain can start sending and receiving e-mail through the Hosted Filtering service, it must be enabled.

Notes

Domains can be enabled only after they have been created and validated in the Administration Center.

If you are no longer using a domain or would like to suspend the use of it without deleting its configuration settings, you can disable it.

How to enable a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Tasks pane, click Enable Domain. Note To enable a domain, it must first be validated. For more information about validating a domain, see [Validate a Domain](#z0f5b7b94c1434a20b33abaf55b1b81c7). |

If you are no longer using a domain or would like to suspend the use of it without deleting its configuration settings, you can disable it.

How to disable a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Tasks pane, click Disable Domain. |

# Delete a Domain

You can only delete domains for your company from the Disabled Domains view on the Domains tab on the Administration tab.

Note

Once a domain has been deleted it is not recoverable. All users and settings for the domain will be deleted from the Administration Center.

How to disable and delete a domain from your company

|  |
| --- |
| 1. On the Administration tab, click the Domains tab2. From the Domains list, check the box by the target domain and click the Disable button Read the prompt and choose OK to continue if appropriate.3. OR click the target domain to go to the domain properties and use the Disable Domain link in the Tasks pane. Read the prompt and choose OK to continue if appropriate4. From the Domains list select the Disabled Domains option from the Views pane.5. Check the box by the target domain and click the Delete button (Note: the Delete button is not available to customers with the Hosted Archive Service subscription.)6. Read the prompt and choose OK to continue if appropriate. |

Note

The delete functionality is only available for customers who do not subscribe to the Hosted Archive service.

# Domain Settings

From the list view on the Domains tab on the Administration tab, you can click on the domain name to see and modify the properties for any domain in your company.

# Preferences

You can edit your domain settings to match your domain’s preferred language and time zone settings. The Language and Time Zone preferences can be configured at the company or user level also. The most specific setting will be applied. Language preferences are applied to Spam Notifications and the Archive Viewer Web pages.

# Catch-All Domains

With the Catch-All Domain feature, you can filter a domain and all of its subdomains without having to add each individual subdomain to the Administration Center. The Catch-All feature ensures that mail for those subdomains is processed according to the parent (primary) domain profile. If you enable the Catch-All Domain feature for a domain in your organization, ensure that you change the mail exchange (MX) record (the entry in your Domain Name System [DNS] settings that identifies the mail server responsible for handling e-mail for that domain name) for each subdomain.

Note

You cannot use the Catch-All domain feature if you also use Directory-Based Edge Blocking (DBEB). For more information about using the Catch-All Domain feature with Directory-Based Edge Blocking, contact Technical Support before you enable the feature.

Important

When you set the Spam Quarantine feature for a catch-all domain, the naming convention used for the e-mail aliases of any subdomain accounts must match that of the parent (primary) domain. This allows the feature to correctly filter spam. For example, if the parent domain address is wilson@contoso.com, the SMTP address for the subdomain account must be wilson@hr.contoso.com.

# Outbound E-Mail Filtering

All outbound e-mail that is sent through the Hosted Filtering pool of e-mail servers is scanned for viruses, Policy Filter rules matches, and spam characteristics before it is sent. This action helps reduce the risk of spam being sent from the Hosted Filtering environment, which could lead to some of the outbound IP addresses being blocked by companies and by third-party security organizations.
All domains that use the outbound e-mail servers for Hosted Filtering must be added to your domains list and must be enabled in the Administration Center.

# BCC Option for Outbound Suspicious E-mail

You can configure a mailbox within your company to receive a copy of all outbound messages that exceed the spam threshold of the service and are being routed out through the Higher Risk Delivery Pool of IP addresses. It is important that this mailbox be monitored, in order to make sure that the information is received in a timely manner. If delivery to this BCC mailbox fails for any reason, those messages cannot be recovered. This option should be used only for active troubleshooting (in other words, if you are not investigating something, then there is a real risk that you will fill up the mailbox and tip over your mail server). If you use the mailbox for monitoring, be sure to configure rules for it that will alert you the event of a spike in traffic.

# Default Outbound Service Domain

The Default Outbound Service domain can be selected (checked) for one domain within a Company. The service settings for this domain are applied to outbound messages from a Company's IP address, when the From Address is not a domain defined within the company. Messages that are routed outbound through the Filtering Service from domains not configured in the Administration Center are more likely to be flagged as suspicious mail by the outbound spam filters.
Message count information for messages that are processed according to the configuration settings of the Default Outbound Service domain will show up in the Reporting data for the Default Outbound Service domain.

How to change the Default Outbound Service domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to assign as the Default Outbound Service domain. You can search for a specific domain name by using the search box.3. In the Preferences section of the Domains Settings pane, click Edit.4. In the Preferences dialog box, check Use this domain settings as the default settings for outbound e-mail.5. Click Save. |

Note

You will see a warning that shows you the current Default Outbound Service domain. If you do not want to change the Default Outbound Service domain, click Cancel.

# Edit Domain Preferences

For each domain in your company, you can specify the default language, time zone, catch-all domains setting, and Outbound filtering settings by editing the domain’s preferences.

How to edit domain preferences

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Domain Settings pane, in the Preferences section, click Edit.4. Update the domain's language and time zone settings.The language setting specifies the language used for Spam Notifications, if you have Spam Notifications enabled.5. To have the Filtering Service automatically filter all subdomains for this domain, select the Catch-all domain check box (not available if DBEB is enabled). Note If you leave the Catch-all domain check box cleared, then you must add all subdomains to the Administration Center to enable Hosted Filtering for those domains. If you have the Catch-all domain check box selected for a domain, and you have configured specific settings for a subdomain, only the configuration settings of the root domain will be applied to messages. 6. To configure the Filtering Service to allow outbound filtering on messages from your domain, select the Outbound filtering check box.7. To receive a blind carbon copy (BCC) of all the outbound e-mail filtered and routed through the Higher Risk Delivery Pool, enter an SMTP address in the BCC all suspicious outbound e-mail to the following e-mail address. The SMTP address must belong to a domain configured within your company.8. To change the Default Outbound Service domain to the current domain, check Use this domain settings as the default settings for outbound e-mail. 9. Click Save. |

# Edit Domain Services

You can view the current service subscriptions that are available on your domain.

[Archive](#z75031877ba574ee7b5a42a7c1c02ba7e)

[Spam Filtering](#zb550d1efaa034848958d980cbc2e4aa9)

[Virus Filtering](#z89fc7839a0a14dd98416d5e88fd5ea28)

[Policy Filtering](#z03fe3fa9ee7846d7bebda2e4a947c4f1)

[E-mail encryption](#z4053209861394e83bc02a8d806375589)

# Archive

If you subscribe to the Exchange Hosted Archive (EHA) service you will see this option. In order to activate Archiving for your domain, you must enable the domain and configure its IP Address Settings. In order to correctly route the e-mail from the other customers on the Hosted Services network, the inbound Mail Server Address must be configured to connect to your e-mail server by IP or by host name, even if you do not actively use the FOSE service for filtering your e-mail. The Outbound IP Addresses must be configured because the Hosted Services network will not accept journaled e-mail (e-mails that contain full mail delivery information such as SMTP MAIL FROM, list of actual recipients, Blind Carbon Copy recipients, etc.) from unknown hosts.

Archiving settings include the following:

 Enabled – in addition to the message being sent to your company, a copy will be routed to EHA as it is processed by the Hosted Services network.

 Journal Only – any mail routed by the Hosted Services network will be delivered to your company without sending a copy to EHA. The only messages that will be archived are those sent to EHA through journaling from your servers.

 Disabled – no e-mail messages will be stored in EHA for the domain that has the service disabled.

# Spam Filtering

FOSE achieves enhanced accuracy with proprietary, multilayer spam technology that helps ensure unsolicited e-mail is automatically filtered before it enters your corporate messaging systems. For more information, see [Antispam Protection](#z5474345309234ad290d462e3acab4807) in the Filtering Service Components section.

Spam filtering settings include the following:

 Enabled – inbound and outbound messages will be evaluated to identify messages that appear to be consistent with spam, and the configured settings will be applied.

 Disabled – inbound messages will not be evaluated to identify messages that appear to be consistent with spam. Disabling spam filtering on the domain does not bypass the IP Edge Blocking, which is done by the Reputation Block Lists (RBLs), nor does it stop the outbound spam filtering if you are sending outbound messages through the Hosted Services network.

# Virus Filtering

Your Hosted E-mail Filtering service has partnerships with a number of virus engines. By default, your organization will always have at least two virus engines enabled.

In the event of a virus outbreak, the virus engine (from whichever partner comes out with a patch first) will be turned on for all customers. Once a patch is released for the new virus, the default virus engines will be turned on again.
The virus engines scan all text files, as well as the text within each message body. Any text file or message body that contains the complete code for a known virus will be blocked. The virus engines also examine each message for partial virus code and will attempt to block these e-mail messages as well.
At times, if there is not enough text to fully scan and the message can be identified as inactive or non-malicious, the message may be allowed. This can apply to mailer-daemons, bounces, or damaged virus attachments that only contain a small portion of the original virus code. For more information on the Virus filtering service, see [Antivirus Protection](#zf116dc34d0f14d839f02c174110e3be3) in the Filtering Service Components section.

# Policy Filtering

FOSE offers an integrated approach to message security through policy enforcement. It allows companies to automatically monitor outbound and inbound e-mail, and stop sensitive and inappropriate messages from leaving and entering the corporate network. For more information, see [Policy Rules](#zd43d92b98b8c43a3869b6bb4ca4e0682).

Policy filtering settings include the following:

 Enabled – inbound and outbound messages will be evaluated to identify messages that match specifically configured Policy Rules, and the configured settings will be applied.

 Disabled – inbound and outbound messages will not be evaluated to identify messages that match specifically configured Policy Rules.

# E-mail encryption

If you subscribe to the Exchange Hosted Encryption (EHE) service, you will see this option. EHE is a convenient, easy-to-use e-mail encryption service that helps to safely deliver your confidential business communications. The service enables users to send and receive encrypted e-mail directly from their desktops as easily as regular e-mail, to anyone at any time.

E-mail encryption settings include the following:

 Enabled – Encrypt and Decrypt Policy Rules can be configured for this domain.

 Disabled – Encrypt and Decrypt Policy Rules cannot be configured for this domain.

# Virtual and Parent Domains

A Virtual Domain is a formatted like a subdomain, and can have its own filtering settings and configurations. The domain to which the Virtual Domain belongs is called its Parent Domain. The Virtual Domain is not an actual DNS mail domain; it is used for internal configuration purposes only. For example, for a Parent Domain called contoso.com, you can create a Virtual Domain called marketing.contoso.com.
Virtual domains allow you to apply different configuration settings to users who belong to the same domain. After creating a Virtual Domain, you can upload a subset of users who belong to the Parent Domain and then associate them to the Virtual Domain in order to customize service settings for that group of users. Users who have been assigned to the Virtual Domain will adhere to the domain settings that are set for the Virtual Domain. In order to disassociate users from a Virtual Domain, you will need to either associate the users with a new Virtual Domain or disable the Virtual Domain. For more information on associating users with a Virtual Domain in the Administration Center, see [Import Multiple Users](#zf8cbf329773241c0aba1763353062b87).

Important

After a domain has been configured as a Virtual Domain, it cannot be reconfigured as a non-Virtual Domain.

In order to add a Virtual Domain, you must first validate and enable the Parent Domain. The User List Settings on the Parent Domain must be set to Admin Center or SFTP, and it must have Directory-Based Edge Blocking (DBEB) set to Reject or Passive mode. When a new Virtual Domain is created, it inherits the service settings of the Parent Domain. If the Parent Domain's DBEB setting is changed to something other than Reject or Passive mode, then the Virtual Domain is automatically disabled. If the User List Settings on the Parent Domain is changed to something other than Admin Center or SFTP then the settings on the Virtual Domain will no longer be applied. If the Parent Domain is disabled, the Virtual Domain will also be disabled.

Edge blocking options are not available for Virtual Domains. E-mail for a particular Virtual Domain is processed for all e-mail addresses that are included in an upload list for that Virtual Domain, as specified by the settings in the Administration Center. If e-mail is received for an address that is not listed in the upload list for the given Virtual Domain, it is processed according to the edge blocking settings for the Parent Domain.

# Group Filtering

This function allows for different groups of users to have their own set of filtering rules, even if all users share the same domain. (For example, the HR department can have different filtering rules than the IT department.)

# Intelligent Routing

A function of Group Filtering, the Intelligent Routing feature routes a subset of users’ messages to specific delivery locations based on Virtual Domain IP Address Settings, even if users all share the same domain. For example, the U.K. office can receive all mail for U.K. users at a specific location, one that is different than the destination for mail sent to U.S. users. As with Group Filtering, each user is associated with a Virtual Domain. Each Virtual Domain is then configured to redirect e-mail to specific servers within the organization.

You will need to configure the receiving mail server within your environment to accept e-mail for the Virtual Domain namespace. In order to revert the recipient address to the original Parent Domain naming, the recipient address needs to be re-written by the receiving mail server. If the recipient address is not rewritten by the receiving mail server, then the user would be able to view the Virtual Domain name in the message header. When the end user replies to a message which was routed using this functionality, the Reply-To address for the end user would not be affected, as this is stamped by the sending server (your mail server) based on the Primary SMTP proxy address associated with the user in your environment.

# Inbound Address Rewrite

A function of Group Filtering, the Inbound Address Rewrite rewrites the recipient addresses for specific users and delivers messages for those recipients based on the Virtual Domain IP Address Settings. For example, the HR department at Contoso needs to receive e-mail at hr.contoso.com, even though the delivery location may be the same as the main contoso.com domain. As in Group Filtering, each user is associated with a Virtual Domain. Each Virtual Domain is then configured to deliver e-mail to specific servers within the organization.

How to create a Virtual Domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to associate as the Parent Domain to the new Virtual Domain. You can search for a specific domain name by using the search box.3. In the Domain Settings pane, in the Virtual Domains section, click Add.4. Enter the name for the Virtual Domain in the Virtual domain name text box.Note The Virtual Domain must be formatted like a subdomain of the Parent Domain. In order to add a Virtual Domain the Parent Domain must be validated and enabled. The User List Settings on the Parent Domain must be set to Admin Center or SFTP, and it must have Directory-Based Edge Blocking (DBEB) set to Reject or Passive mode.5. If you are using the Virtual Domain for Grouping and not for Intelligent Routing, check Deliver to original address in parent domain. If you are using the Virtual Domain for Intelligent Routing, do not check the box.6. Click Save. The following is a view of the Add Virtual Domain dialog box. |

# Manage Notification Settings

The Microsoft Forefront Online Protection for Exchange (FOPE) Filtering service can send automatic notifications to end users and administrators when an event has occurred that affects their service. You can configure scheduled notifications to alert users when messages are redirected to the Spam Quarantine service, or per-message notifications that are sent every time an e-mail virus has been detected in an inbound or outbound message.

## Notification options

Notification options include the following:

 Spam Quarantine Notifications: These notifications are sent to recipients when an incoming e-mail message has been quarantined as spam.

 Inbound Virus Recipient Notifications: These notifications are sent to recipients when an inbound message has been filtered because it contained a virus.

 Virus Sender Notifications: These notifications are sent to a sender when a message was filtered because it may have contained a virus.

 Inbound Virus Admin Notifications: These notifications are sent to administrators when an inbound message is filtered because it contained a virus.

 Outbound Virus Admin Notifications: These notifications are sent to administrators when an outbound message is filtered because it contained a virus.

 Deferral Notifications: These notifications are for inbound messages that have been deferred by the filtering service. You can set up multiple SMTP addresses to receive e-mail notifications of delivery delays for e-mail destined for your domain. Each entry can have its own individual threshold settings.

# Configure Spam Quarantine Notifications

If you are using the Forefront Online Protection for Exchange Spam Quarantine feature and you have enabled Spam Quarantine notifications, end users receive periodic e-mail reminders to review their newly filtered spam mail. It is not necessary to populate the User List in the Administration Center before the end users will receive the Spam Notifications.

The service will send a Spam Notification to all SMTP addresses that have any spam messages quarantined for them. Suppression of the Spam Notifications for a subset of users can be done only after the user information has been uploaded into the Administration Center. For more information about how to update service settings on a subset of users, see [Update Service Settings for Multiple Users](#zc879a458f0c84c288faf1e0d6582c318).

You can send Spam Quarantine notifications to end users as plain text or HTML messages:

 Text: In the text message, end users will receive a plain-text–formatted e-mail message with instructions on how to open Spam Quarantine and review their messages. The text spam notification includes a URL and brief instructions for the user on how to log on and view their spam.

 HTML: The HTML-based notification provides users with a summary of the new spam messages delivered to their Junk E-mail Quarantine mailbox since their last notification. From the notification, users can scan the list of messages that have been quarantined. If users have been granted access to the Quarantine mailbox, then they will have the option to click the message subject to view the message within the Quarantine Junk E-mail folder. Those users can also click Move to Inbox or Not Junk from the spam notification. The Not Junk option is not available for messages that were quarantined because of an Additional spam Filtering (ASF) rule configured for the domain. Users who do not have access to their Quarantine can only use the Move to Inbox link from the spam notification.
The subject line of the HTML notification includes the number of new spam messages (as displayed in the HTML notification), as well as the total number of new messages in the Spam Quarantine account: Subject: Spam Notification: 10 New 10 Total

How to configure Spam Quarantine notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Notification Settings pane, next to Spam Quarantine Notification Settings, click Subscribe.4. In the Spam Quarantine Notification Settings dialog box, in the Notification e-mail format list, click the format type for these notifications.5. In the Notification interval in days (3 – 14) box, type the notification interval.Note If Directory-Based Edge Blocking (DBEB) is configured on the domain in either Reject or Pass Through mode, then, in addition to the 3 -14 day interval, one-day notifications can also be configured. If DBEB is later changed so that Reject or Pass Through is no longer being applied, then the notifications will automatically revert to an interval of 3 days instead of 1 day.6. In the Notification e-mail section, select one of following options: Default settings: Select this option to send notifications from the Hosted Filtering service with the default subject line and message body.  Custom settings: Select this option to create a customized From address, subject line, and message body. You can customize the message body for text notifications only.7. Click Save.  |

The following is a view of the Add Spam Quarantine Notification Settings dialog box.



How to modify Spam Quarantine notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Spam Quarantine Notifications, click Edit. 4. Modify the settings you want to change, and then click Save. |

How to remove Spam Quarantine notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to the Spam Quarantine Notification Settings, click Unsubscribe. |

# Configure Inbound Virus Recipient Notifications

Inbound virus recipient notifications inform message recipients that an infected message has been rejected by the Hosted Filtering service. This notification includes the sender’s e-mail address and the virus name.

If a virus is detected in a message and can be cleaned, a warning message is sent to the recipients notifying them that the message had a virus and was rejected by the Hosted Filtering service.

If a virus is detected in a message and cannot be cleaned, a rejection notification is sent to the recipients. The notification explains that an incoming message was infected with a virus, and that it could not be cleaned.

We do not recommend enabling the virus notifications. By default, Inbound Virus Recipient notifications are disabled.

To enable inbound virus recipient notifications

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Inbound Virus Recipient Notification, click Subscribe.4. In the Notification e-mail section, select one of following options: Default settings: Send notifications from the Hosted Filtering service with the default subject line and message body. Custom settings: Select this option to create a customized subject line and message body. The custom Display name and From address for the Virus Sender notifications is used for both Virus Sender notifications and Virus Recipient notifications.5. Click Save. |

How to edit inbound virus recipient notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Inbound Virus Recipient Notification, click Edit. 4. Modify the settings you want to change, and then click Save. |

How to remove inbound virus recipient notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Inbound Virus Recipient Notification, click Unsubscribe. |

# Configure Virus Sender Notifications

A virus sender notification informs the sender of an outbound message that the message has been rejected by the Forefront Online Protection for Exchange filtering service because it contains a virus.

If a virus is detected in a message and can be cleaned, a warning notification is sent to the sender, notifying the sender that the message contained a virus and was removed from the message by the Hosted Filtering service.
If a virus is detected in a message and cannot be cleaned, a rejection notification is sent to the sender. The notification explains that the message was infected with a virus and could not be cleaned; therefore, the message was not delivered.
We do not recommend enabling the virus notifications. By default, these notifications are disabled.

How to enable virus sender notifications

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Virus Sender Notification, click Subscribe.4. In the General section, select one of the following message direction options: Inbound only Outbound only Inbound and outbound5. In the Notification e-mail section, select one of following options:  Default settings: This allows you to send notifications from the Hosted Filtering service with the default subject line and message body for warning and rejection notifications. Custom settings: This allows you to customize the notification subject lines and message bodies for Warning and Rejection notifications. The custom Display name and From address for the Virus Sender notifications is used for both Virus Sender notifications and Virus Recipient notifications. Click Save.  |

How to edit virus sender notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Virus Sender Notifications, click Edit. 4. Modify the settings you want to change, and then click Save. |

How to remove virus sender notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Virus Sender Notifications, click Unsubscribe. |

# Configure Inbound Virus Admin Notifications

Inbound Virus Admin notifications send copies of all inbound virus notifications to the administrator.

Note

This feature is available only if the Virus Sender Notification feature is enabled.

How to enable Inbound Virus Admin notifications

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Inbound Virus Admin Notification, click Subscribe. 4. On the Domains tab, click the name of the domain that you want to modify.5. In the Administrator e-mail address box, type the administrator address that should receive copies of all inbound virus notifications.6. Click Save.  |

How to edit Inbound Virus Admin notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Inbound Virus Admin Notification, click Edit.4. Modify the settings you want to change, and then click Save. |

Insert subsection body here.

How to remove Inbound Virus Admin notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Inbound Virus Admin, click Unsubscribe. |

# Configure Outbound Virus Admin Notifications

Inbound Virus Admin notifications send copies of all inbound virus notifications to the administrator.

Note

This feature is available only if the Virus Sender Notification feature is enabled.

How to enable Outbound Virus Admin notifications

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Outbound Virus Admin Notifications, click Subscribe. 4. On the Domains tab, find and select the domain that you want to modify by clicking the domain’s name.5. In the Administrator e-mail address box, type the administrator address that should receive copies of all inbound virus notifications.6. Click Save.  |

How to edit Outbound Virus Admin notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Outbound Virus Admin, click Edit.4. Modify the settings you want to change, and then click Save. |

How to remove Inbound Virus Admin notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Outbound Virus Admin, click Unsubscribe. |

# Configure Deferral Notifications

For each domain in your company, you can set up multiple SMTP addresses to receive e-mail notifications of delivery delays for e-mail destined for your domain. Each entry can have its own individual threshold settings. These SMTP addresses must be for domains outside of the domain being configured.

How to enable deferral notifications

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Deferral Notifications, click Subscribe. 4. In the Number of deferrals before notification box, type the number of messages that can be deferred before a deferral notification is sent. For example, if you enter 300 in this box, then 300 messages can be deferred before a deferral notification is sent.5. In the Administrator e-mail address box, type the e-mail address where you want deferral notifications sent.Note For each domain in your company, you can set up multiple SMTP addresses to receive e-mail notifications of delivery delays for e-mail destined for your domain. Each entry can have its own individual threshold settings. These SMTP addresses must be for domains outside of the domain being configured. 6. Click Save.  |

How to edit deferral notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Deferral Notifications, click Edit.4. Modify the settings you want to change, and then click Save. |

How remove deferral notification settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. On the Domains tab, click the name of the domain that you want to modify.3. In the Notification Settings pane, next to Deferral Notifications, click Unsubscribe. |

# Notification Samples

The following topics describe examples of notification messages that are sent from the Hosted Filtering:

[Spam Quarantine Notifications](#z58bf422d83c5420f809aa46d0e56f5e3)

[Sample Virus Notifications](#z1a91075322d5467aa48763c18878a5e3)

# Spam Quarantine Notifications

Spam quarantine notifications are available in either HTML or text formats:

[HTML Notifications](#zf58a4a2314794c3e9c4a62738b076446)

[Text Notifications](#z93e8b11a4aae4133a58165f93608aede)

# HTML Notifications

The following is a sample HTML-based notification message from the Spam Quarantine service.



## See Also

[Text Notifications](#z93e8b11a4aae4133a58165f93608aede)

# Text Notifications

The following is a sample text notification from the Spam Quarantine service.



## See Also

[HTML Notifications](#zf58a4a2314794c3e9c4a62738b076446)

# Sample Virus Notifications

The following examples describe sample notifications for the virus filtering service.

## Inbound Virus Recipient Notification

The following is a sample notification of a message that was rejected because it contained a virus:

|  |
| --- |
| From: Virus Scanner <> or <CUSTOM SCANNER ADDRESS> To: <SENDER> Subject: Undeliverable message returned to sender OR <CUSTOM REJECT SUBJECT> This message was created automatically by mail delivery software. A message you sent was virus infected. The message could not be cleaned. OR <CUSTOM REJECT TEXT> Virus Scan Report: ----------------------------<FILENAME> infected by: <VIRUS NAME(s) HERE> Delivery failed for the following recipients(s): <ORIGINAL RECIPIENT(s)> For more information about this virus, visit http://www.antivirus.com/vinfo/virusencyclo/----- Original Message Header ----- <ORIGINAL MESSAGE HEADER> |

## Sample Warning Notification

The following is a sample warning message of a message that contained a virus and was cleaned by the virus filtering service:

|  |
| --- |
| From: Virus Scanner <> or <CUSTOM SCANNER ADDRESS> To: <SENDER> Subject: Warning: A message you sent contained a virus or <CUSTOM WARNING SUBJECT> This message was created automatically by mail delivery software. A message you sent was virus infected. The message was cleaned and delivered. OR <CUSTOM REJECT TEXT> Virus Scan Report:  ----------------------------<FILENAME> infected by: <VIRUS NAME(s) HERE> -> CLEANED! Recipient(s) of the original message: <ORIGINAL RECIPIENT(s)> For more information about this virus, visit http://www.antivirus.com/vinfo/virusencyclo/ ----- Original Message Header ----- <ORIGINAL MESSAGE HEADER> |

## Sample Virus Recipient Notification

The following is a sample notification sent to the recipient of a message that contained a virus:

|  |
| --- |
| From: Virus Scanner <> or <CUSTOM SCANNER ADDRESS> To: <RECIPIENT> Subject: [NOTIFICATION] Virus infected message rejected or <CUSTOM WARNING SUBJECT>This message was created automatically by mail delivery software. A message sent to you by <SENDER> was rejected because it was virus infected. The message could not be cleaned. <CUSTOM WARNING TEXT> Virus Scan Report:  ----------------------------<FILENAME> infected by: <VIRUS NAME(s) HERE> For more information about this virus, visit http://www.antivirus.com/vinfo/virusencyclo/----- Original Message Header ----- <ORIGINAL MESSAGE HEADER> |

# Domain IP Address Settings

For each domain in your organization, you must specify the mail server IP address or host name that your inbound mail is delivered to after it has been filtered. If you have multiple mail server IP addresses, you can configure these as multiple-SMTP profiles on the Company tab.
Similar to adding outbound IP addresses for your entire company, you can also specify outbound IP addresses for individual domains. All e-mail sent through these outbound IP addresses will be filtered by the outbound FOSE service.
 For more information, see [Add a Mail Server Address](#z59cb70e9a37b45b89236e8b17cfb0281) and [Add an Outbound IP Address for Your Domain](#z134162e76d234f83ad7474251f2e13d4).

# Add a Mail Server Address

For each domain in your organization, you must specify the mail server IP address or host name that your inbound mail is delivered to after it has been filtered. If you have multiple mail server IP addresses, you can configure these as multiple-SMTP profiles on the Company tab.

Be sure to specify whether the IP addresses should be prioritized, and if so, in what order. Or, if you prefer a round-robin format, be sure to specify that. Keep in mind that all messages processed by the Hosted Filtering service will use these inbound server settings to deliver messages to your domain. It is critical that the IP address settings for the domain be kept up to date at all times.

Add a mail server address in the Administration Center by selecting the mail server IP address information for that domain’s e-mail service. You can add single IP addresses or use one of the multi-SMTP profiles that you created for your company.

How to add or edit the mail server address for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the domain name that you want to modify. You can search for a specific domain name by using the search box.3. In the IP Address Settings section of the center pane, next to the Mail Server Address box, click Edit.4. Do one of the following: Select Enter your e-mail server address, and then type the IP address or Host Name of your mail server. Select Use your multi-SMTP profile, and then click the multi-SMTP profile that should be used for this domain. See [Create an Inbound Multi-SMTP Profile](#z3a2eadfcd6e841c780f97446dc6587d4) for more information about how set up a multi-SMTP profile. Click Save.  |

The following is a view of the Add or Edit Mail Server Address dialog box.



## See Also

[Add an Outbound IP Address for Your Domain](#z134162e76d234f83ad7474251f2e13d4)

# Add an Outbound IP Address for Your Domain

Similar to adding outbound IP addresses for your entire company, you can also specify outbound IP addresses for individual domains. All e-mail sent through these outbound IP addresses will be filtered by the outbound FOSE service.

Note

Ensure that all outbound IP addresses added to your domain have been approved to use the FOSE outbound filtering service.

How to add outbound IP addresses to your domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the IP Address Settings section of the center pane, next to Outbound IP Addresses, click Add.4. In the IP Addresses dialog box, enter the outbound IP addresses that you want the domain to use to send e-mail. Separate multiple IP addresses with a comma (,).  |

# Domain Service Settings

Domain Service Settings include the following:

[User List Settings](#z200ed9182d4c4ec3a5151e07284c8e2a)

[Archive Settings](#z8cb1ce9ac1b14f82ac9384b959f43b61)

[Spam Action Settings](#zd9281131e2f142799c3a0691d98c2d17)

[Spam Submission Evaluation](#z243d624d3f034dc1b625103cc943bf7d)

[Additional Spam Filtering Options](#z074002c0d00e4f378225a1f254079562)

[Additional Spam Filtering Test Mode Options](#zbfb3b3d0134a49b1b383c7d964004285)

[Policy Filter Settings](#z70557c5d61b44dcdab2cbb8f977e3b59)

[Configure Quarantine Settings](#z9183386f4cd04385b623ac903aee3da8)

# User List Settings

The User List source is configured in the User List Settings section of the Service Settings on the Domain properties page.
There are four primary methods for adding user accounts to your hosted services:

1. Admin Center

2. Secure FTP

3. Directory Synchronization tool

4. Legacy Directory Synchronization tool

For more information about the User List source see [Add Users](#z08d23df467b54594ac266738d1be4817).

# Specify the User List Source

The User List source is configured in the User List Settings section of the Service Settings on the Domain properties page. There are four primary methods for adding user accounts to your hosted services:

 Admin Center

 Secure FTP

 Directory Synchronization tool

 Legacy Directory Synchronization tool

For more information about the User List source see [Add Users](#z08d23df467b54594ac266738d1be4817).

# Directory-Based Edge Blocking

The Forefront Online Protection for Exchange Filtering service normally processes all of the messages that are sent to any SMTP address within your domain. You can, however, configure your service to validate the messages that come into the domain, before they undergo further processing. This extra option is provided by the Directory-Based Edge Blocking section, available in the center pane on the Domains tab. For more information, see [Directory-Based Edge Blocking](#z10a04ed0c0a54f54b53f7606e1098033).

How to configure Directory-Based Edge Blocking for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains pane, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Service Settings section of the center pane, next to User List Settings, click Edit.4. In the drop-down menu in the Directory-Based Edge Blocking section, select one of the following options: Disabled: Disables Directory-Based Edge Blocking for the domain. Reject: Rejects all messages at the network perimeter that are sent to e-mail addresses that are not part of the domain’s user list. Reject-Test: Redirects all messages that are sent to user accounts that are not on the user list to a specified e-mail address.Note Reject-Test mode is a test function that is specifically designed to be used for a short period of time. Its purpose is to validate the accuracy of the user list. In Reject-Test mode, any message that is received for a recipient who is included on the user list will be processed according to the domain’s settings. All e-mail for recipients who not on the user list is redirected to a separate e-mail address after filtering. Pass-Through: Filters a subset of user accounts through the Hosted Filtering service. E-mail to all other SMTP addresses not on the list will be delivered directly, without passing through the Hosted Filtering service. The e-mail messages for users who are not present in the Pass Through list do not bypass the IP Reputation Blocks on the FOPE network edge. Passive (Virtual Domain Creation Only): Passive mode on a domain allows you to configure Virtual Domains for that domain without needing to provide a User List for the Parent Domain.5. In the \*Error notification address text box, specify the e-mail address that should receive any error notifications that may occur during the User List upload.6. Click Save.  |

After you have added users to your domain and have selected a Directory-Based Edge Blocking option, all e-mail addresses in the Users List for that domain will be used for recipient validation.
If you disable Admin Center as the User List source for Directory-Based Edge Blocking for a domain, then recipient validation will be disabled for all user accounts listed in the Administration Center for that domain. If you choose to re-enable Admin Center as the User List source for Directory-Based Edge Blocking for the domain, then all user accounts in the Administration Center for that domain will be used for recipient validation.

Note

If you are using the legacy Directory Synchronization Tool or Secure FTP upload to add users to your service, then directory-based edge blocking option you selected for those upload modes will be applied; however, the users will not show up in the Administration Center.

# Archive Settings

If you subscribe to the Exchange Hosted Archive service, you will be able to see some of your Archive Settings here. To learn how to edit archive settings, see [Edit Company-Wide Archive Settings](#z1b8ee5374b0447bea80ee2bef04c03f9).

## See Also

[Edit Company-Wide Archive Settings](#z1b8ee5374b0447bea80ee2bef04c03f9)

# Edit Company-Wide Archive Settings

Archive settings can be configured at multiple levels. Company-wide settings are the default settings for all domains and all users. A setting made at the domain level will override the company default. Settings configured at the user level override both the domain and company settings. This allows customization of archive settings down to the user level.

Note

If you wish to create or edit rules that will exclude internal messages, you must do so only from the Company subtab.

How to Edit Company-Wide Archive Settings

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. On the Administration tab, click the Company subtab.2. In the Service Settings section of the center pane, next to Archive Settings, click Edit.3. Set the archive settings and then click Save.The following table summarizes the configuration options that are available:

| **Option** | **Description** |
| --- | --- |
| Administrator alert | Selects whether users can receive Administrator alerts from Hosted Archive services. |
| Exclude users | Selects whether to enable excluding specific users from the archive. |
| Internal messages | Selects whether to automatically mark internal messages as reviewed. Note: If you wish to create or edit rules that will exclude internal messages, you must do so only from the Company sub-tab. |
| Message review | Selects whether to activate daily message harvest to capture messages for review based on sampling rates and keyword lists. |
| Legal hold | Selects whether to suspend message destruction for the entire company. Messages reaching the end of their retention period will not be destroyed while legal hold is enabled. |
| Journaling address | Sets the Journaling address for Envelope Journaling. This setting is configured during service activation. |
| IM copy address | This setting is configured by Technical Support. Contact support if your company will be archiving instant messages. |
| Retention Period | Defines how long messages will be held in the archive before they are destroyed. |
| Tombstone policy | Selects Tombstone policy which defines archive behavior after message expiration. Available options include the following:  Permanent deletion: Message is fully deleted. Minimal: The time, date and recipients are retained, and the rest of the message is deleted. Full headers: The time, date, recipients, subject, attachment, and delivery path are retained, and the rest of the message is deleted. |
| Tombstone retention period | Sets the Retention period for Minimal and Full header tombstones. |

Note To configure archiving for your organization’s Bloomberg messages, contact Technical Support. |

# Spam Action Settings

Spam action settings determine how spam is stored and managed by your Forefront Online Protection for Exchange Filtering service. Spam action settings are applied at the domain level. By default, spam will be directed to the Spam Quarantine for your service. However, you can modify this setting. In the Administration Center, on the Domains tab of the Administration tab, the Spam Action settings for your domains determine how spam e-mail will be stored and managed for your service. The settings appear under Spam Action in the Service Settings section of the center pane, after you select a domain. The possible spam action options are as follows:

 [Spam Quarantine](#ze2a8341bf704460c8bf9ab59e3709854)

 [Spam Redirection](#zb0e39e3725e04dd989f4f80d6e12fec2)

 [Modify Subject](#zd59ade693fb4445985283ca6265577f9)

 [Add X-Header](#z55a2cb35143247848c4b056ff237bfbe)

# Spam Quarantine

Spam Quarantine is the most widely used option for storing spam, because it relieves corporate e-mail servers of the need to process and store this type of e-mail. In addition, the Spam Quarantine option lets users avoid sorting through spam messages, which ultimately improves employee productivity. For this option, e-mail that is identified as spam is redirected to individual users’ Web-based spam mailboxes that are hosted by the FOSE service. Spam messages are stored for 15 days, and then they are automatically purged.

As an administrator, you can set up Spam Quarantine so that you and other administrators can access end users’ Spam Quarantine mailboxes on their behalf. To do so, you must select the Spam Quarantine option as the setting in the Edit Spam Settings dialog box. This allows administrators to view end users’ Spam Quarantine accounts. You can then log on to the Spam Quarantine user interface and view user accounts. To access a specific user’s Quarantine mailbox, the user must be configured with an account in the Administration Center. After the account is configured, with the Spam Quarantine option you can view a spam message, salvage it, or report a false positive back to FOSE for review.

You can also let your end users have access to their own Spam Quarantine mailboxes to review, delete, or retrieve e-mail that has been identified as spam, as well as report a false positive. In addition, end users can be reminded to review their newly filtered spam mail with periodic e-mail reminders. When users have access to Spam Quarantine, the HTML spam notification allows them to salvage messages to their Inbox or report a false positive from within the e-mail message.

When end users do not have permission to access Spam Quarantine, the HTML spam notification allows them to view the message sender, subject, and date, and choose to salvage the message to their Inbox.End user Quick Cards have been created in order to educate end users on how to take advantage of the Spam Quarantine service. The Quick Cards are available for download from the Resource section on the Welcome pane in the Administration Center, and from the [Download Center](http://go.microsoft.com/fwlink/?LinkID=145099).

# Spam Redirection

When you select the Redirect to other address option, e-mail that is identified as spam is redirected to a single SMTP address within the domain. You can then review these messages at your convenience from a single location that is hosted on your mail server.

# Modify Subject

By selecting the Modify subject option as the Spam Action setting, you can add an identifying word or phrase to the subject line of messages that have been identified as spam. If needed, you can then create client-side rules to filter the spam messages.

# Add X-Header

When you select the Add X-Header option as the spam action, you can add customized X-Header comments to messages that have been identified as spam by the service. The X-Header is then added to the Internet header of all subsequent spam messages. The X-Header option gives you a legitimate count of how many e-mail messages were filtered as spam. You can establish mail server rules or client-side rules to filter e-mail messages that are marked with X-Headers, if needed.

How to configure a spam action setting for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Service Settings section of the center pane, next to Spam Action, click Edit.4. In the Spam Action dialog box, do one of the following: To use the Spam Quarantine option, select Spam Quarantine. To use the spam redirection option, select Redirect to other address, and then type the e-mail address where redirected spam messages should be sent. This e-mail address must exist within the domain. To use the subject modification option, select Modify subject, and then type an identifying word or phrase that should be added to all messages that are identified as spam. To use the X-Header option, select Add X-Header, and then type the X-Header information that should be added messages that are identified as spam.5. Click Save.  |

# Spam Submission Evaluation

The Forefront Online Security Exchange (FOSE) spam team receives and reviews spam submissions from all of its customers. The team examines indicators within each submitted message, such as the following:

 From address

 Sending IP address

 Keywords

 Catch-phrases

 Frequency of transmission

 Other trends and patterns

After reviewing this information, the spam team initiates the relevant changes to the FOSE spam filtering layers. The message is then classified as spam in the future.

## The Spam Evaluation Process

Spam evaluation is an ongoing process that is applicable regardless of the originating language or character set. Quite often, because a spam message can be vague, or even lack text in the subject or message body, the spam team relies on all other available message characteristics to perform filtering. This means that after the spam team flags a given message as spam and makes the necessary changes to its rule base, that message will be blocked in the future until its characteristics have been modified in a manner significant enough to evade our filters.

### Spam Rules Deployment Information

Spam submissions are processed seven days per week and new spam rules are deployed continuously. Timeframes for rules on individual submissions vary depending on the quantity and quality of submissions. Because new spam rules are set globally for all customers, be aware that not all individual spam submissions result in a new spam rule.

## How to Report Spam

It is critical that, when you report spam, you include the full Internet headers. You can do this by sending the offending message as an attachment along with the full original Internet header, or by using the [Junk-Email Plug-In](http://go.microsoft.com/fwlink/?LinkID=147248) (which is made available for some Microsoft Office Outlook 2003 and Outlook 2007 users, depending on your organization).If you would like automated spam processing, send each spam submission individually. Do not forward multiple spam messages in one individual message. See [Guidelines for Successful Spam Submissions](#z4f26a65abe1b44fd89dda297f296d021).

# Additional Spam Filtering Options

Additional spam filtering (ASF) options give you as an IT administrator the ability to select various content attributes of a message that either increase the spam score (potential for the message to be quarantined as spam) or absolutely quarantine messages containing specific attributes. The ASF rules target specific message properties such as HTML tags and URL redirection, which are commonly found in spam messages. See below for the full list of ASF Options.

Enabling the ASF options is considered an aggressive approach to spam filtering, and any messages that are filtered by these options cannot be reported as false positives. These messages can be salvaged using Spam Quarantine and the periodic spam notification messages. Administrators can create Allow policy rules that permit messages to bypass all spam filtering, including these ASF options. If a domain is using a Spam Action option, the ASF definition appears in the Internet header section of a message that has been marked as spam.

How to configure ASF options for your domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Service Settings section in the center pane, next to Additional Spam Filtering (ASF) Options, click Edit.4. For each option, do one of the following: Turn the option on or off. When you turn an option on, messages will be actively filtered according to the rule associated with that option. Messages will be marked as spam or will have the spam scores increased, depending on which ASF options you enable. Click Test to run the option in Test mode. Options that enable filters in Test mode do not take action on messages that meet the filter criteria. Test messages are tagged with either an X-Header or a Subject Line insertion before they are delivered to the intended recipient. They are not filtered against the spam filtering rules.5. Click Save.  |

Some ASF options increase the spam score of a message. Other options mark the message as spam and quarantine it. For a description of each ASF option, see the Additional Spam Filtering (ASF) Options table below.

### Additional Spam Filtering (ASF) Options

| **ASF Option** | **Description** | **ID (as displayed in Test Mode, Quarantine, etc.)** |
| --- | --- | --- |
| Increase Spam Score Section  |  |  |
| Image links to remote sites | This option specifies that any messages with image links to remote sites will trigger a code that causes an HTML e-mail message to load a graphic from a remote Web site. Image tags can be used in legitimate newsletters. However, a spammer can also use an image tag to display text or graphics for advertising purposes. Therefore, applying this option increases the score that such a message receives, and therefore increases the likelihood that it will be marked as spam. | 0 |
| Numeric IP in URL | Messages that have with numeric-based URLs (most often in the form of an IP address) will receive an increased spam score. | 10 |
| URL redirect to other port | Messages that contain a hyperlink that redirects the user to ports other than port 80 (regular HTTP protocol port), 8080 (HTTPS port), or 443 (HTP Alternate port) will receive an increased spam score. | 11 |
| URL to .biz or .info Web sites | Messages that contain a .biz or .info extension in the body of a message will receive an increased spam score. | 12 |
| Mark as Spam Section |  |  |
| Empty messages | Any message in which the message body and subject line are both empty and have no message body formatting, and which also has no attachment, will be marked as spam. | 1 |
| JavaScript or VBScript in HTML | Any message that uses JavaScript or Visual Basic Script Edition in HTML will be marked as spam. Both of these scripting languages are used within an HTML e-mail message to automatically cause a specific action to occur. The browser will parse and process the script along with the rest of the document. The presence of either of these tags indicates dynamic content and the possibility of malicious intent. | 2 |
| Frame or IFrame tags in HTML | Any message that uses the <Frame> or <IFrame> HTML tag will be marked as spam. These tags are used on Web sites or in HTML e-mail messages to format the page for displaying text or graphics. | 3 |
| Object tags in HTML | Any message that contains the <Object> HTML tag will be marked as spam. This HTML tag allows plug-ins or applications to run in an HTML window. | 4 |
| Embed tags appear in HTML | Any message that contains the <Embed> HTML tag will be marked as spam. This HTML tag allows different kinds of documents of varying data types to be embedded into an HTML document. Examples include sounds, movies, or pictures. | 5 |
| Form tags appear in HTML | Any message that contains the <Form> HTML tag will be marked as spam. This HTML tag is used to create Web site forms. E-mail advertisements often include this tag in an attempt to solicit information from the recipient. | 6 |
| Web bugs in HTML | Any message that contains a Web bug will be marked as spam. A Web bug is a graphic that is designed to determine whether a Web page or e-mail message has been read. Web bugs are often invisible to the recipient because they are typically added to a message as a graphic that is as small as one pixel by one pixel. Legitimate newsletters may also use this technique, although many consider this an invasion of privacy. | 7 |
| Apply sensitive word list  | Any message that contains a word from the sensitive word list will be marked as spam. Using the sensitive word list allows easy blocking of words that are associated with potentially offensive messages. As administrator, you cannot edit this list. Filtering against the sensitive word list is applied to both the subject and message body of a message. | 8, 9 |
| SPF record Hard Fail | Any message that does not pass an SPF record verification will be marked as spam. The filter determines whether the envelope sender domain of an incoming message publishes an SPF record (v=spf1 TXT record). If the envelope sender domain does not publish an SPF record, this filter will have no impact on mail filtering. If the envelope sender domain does publish an SPF record, the filter will perform an SPF check to verify that the connecting IP is an approved sender IP for that domain. If the connecting IP is not an approved sender for the domain, then the mail is marked as spam. Note n order to avoid false positives (legitimate e-mail incorrectly identified as spam) for mail from your company, make sure that the SPF record is correctly configured for your domains. See SPF Record Settings for Outbound E-mail Filtering in Best Practices to learn how to configure your SPF record. | 13 |
| From: address authentication: Hard fail | Any message that hard fails a “From Address” SPF authentication process will be marked as spam. From Address authentication is a method of authenticating the sender of the message. Specifically, this option uses an SPF check to help protect against message headers that contain forged senders. A regular SPF check authenticates the message by verifying that the envelope sender corresponds to the IP address that sent the message. It does this by looking up the transmitting IP address in the sender’s SPF record. However, in many cases, the envelope sender is not the sender that is displayed to the end user. What the end user sees in the e-mail client are the “message From:” and “message To:” headers. From Address authentication is designed to work with traditional SPF checks. If a regular SPF check returns a value of SPF None, Neutral, TempError, or PermError, then an additional SPF check will be performed against the domain in the Sender field in the message headers, if that field exists. If it does not exist, then the SPF check will be conducted against the domain in the From field in the message headers (the domain that appears in the end user’s e-mail client).  From Address authentication helps identify and prevent an event in which a spammer spoofs both the envelope sender, by sending from a domain with no SPF record, and the domain that the end user sees in the e-mail client. A traditional SPF check will not capture this case because it does not authenticate against domains in the From field, so From address authentication will capture it. If a hard fail occurs, the message is flagged as spam; otherwise, spam points are added. From Address authentication is skipped if the result of the regular SPF check is SPF Pass, Hard Fail, or Soft Fail.Note It is possible for From Address authentication to create false positives (legitimate e-mails misidentified as spam), because in the SMTP protocol it is not illegal to send mail while rewriting the sending organization in the From or Sender fields. This is most likely to occur in newsletters and other bulk mail. In order to avoid the possibility of messages from your company being marked as spam, it is important to make sure that the SPF record is correctly configured for your domains. See SPF Record Settings for Outbound E-mail Filtering in Best Practices to learn how to configure your SPF record. | 14 |
| NDR (non-delivery report) Backscatter | This option marks as spam all messages that match the non-delivery report (NDR) bounce characteristics. Customers with outbound filtering do not need to enable this option, as NDRs that are legitimate bounce messages will be automatically detected as such and delivered to the original sender. At the same time, all illegitimate bounce messages, known as backscatter, are marked as spam. Enabling this option will mark all NDRs as spam, regardless of whether or not the customer is using outbound filtering, and regardless of whether the NDR is legitimate. | 15 |

# Additional Spam Filtering Test Mode Options

Additional Spam Filter (ASF) options can be enabled, individually, to run in Test mode or in Live mode. In Live mode (when an ASF option is turned on) the message filters take action on messages that match the options which are active for the domain. In Test mode, filters do not take action on messages that meet the filter criteria. Test messages are tagged with an X-Header, a BCC address, or a Subject Line insertion, and are then delivered to the original recipient.

How to configure ASF Test mode options

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Service Settings section of the center pane, next to Additional Spam Filtering (ASF) Test Mode Options, click Edit.4. In the Additional Spam Filtering Test Mode Options dialog box, select the options you want to enable. See the Additional Spam Filtering Test Mode Options table below for a description of each Test mode option.5. To send copies of the messages that are filtered in Test mode to a specific e-mail address, type an e-mail address in the Bcc message to box. For example, you can enter the administrator’s e-mail address in this box.6. Click Save. |

### Additional Spam Filtering Test Mode Options

| **ASF Test Mode Option** | **Description** |
| --- | --- |
| Tag message with X-Header | When you select the Tag message with X-Header option, the following text is inserted in the e-mail message: X-CustomSpam: This message was filtered by custom spam filter option - \*specify option\*. |
| Modify message subject | When you select the Modify message subject option, messages that are filtered in Test mode against the ASF options will contain modified subject lines when they are delivered. Modified subject lines indicate that the message has been filtered in Test mode, and provide the ASF option ID. ASF option IDs are described in the Additional Spam Filtering (ASF) Options table in Configure Additional Spam Filtering Options. The following example shows a modified message subject for a message that has been filtered in Test mode: Filter Test: C<custom spam filter number>. |

# Policy Filter Settings

On the Domains tab, you can enable rules that help your organization conform to the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA). If you subscribe to the optional Encryption e-mail service, you have the ability to configure an outbound encryption rule that evaluates outbound e-mail for matches to phrases that, if used in e-mail, require the e-mail to be encrypted, per HIPAA. For more information about how to enable these rules, see [Enable and Disable HIPAA Rules](#ze7cb241eb1514bb8bc27c7115c8fdddd).

You can add plain text and HTML footers to all outbound e-mail messages (including reply messages). Examples of common footers include your company’s name, address, and contact information, or a required legal disclaimer. You can apply this feature at the domain level (Parent Domains or Virtual Domains). For more information about how to add footers, see [Create an E-mail Footer for Outbound E-mail](#ze6ad06056feb4f509adba223b9fe8a8b).

# Enable and Disable HIPAA Rules

On the Domains tab, you can enable rules that help your organization conform to the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA). If you subscribe to the optional Encryption e-mail service, you have the ability to configure an outbound encryption rule that evaluates outbound e-mail for matches to phrases that, if used in e-mail, require the e-mail to be encrypted, per HIPAA.

The HIPAA rule set option will display on the Policy Filter Settings section of the Services pane on the Domains tab.Two sets of keywords are used to determine if a message should be encrypted. When the HIPAA rule set is enabled, when the HIPAA rule set is enabled, if a keyword or pattern from the first rule set is used AND a keyword or phrase from the second set is matched in the same message, the message will be encrypted.

Note

The message subject and body are scanned for matches in both rule sets.

| **Rule Set 1** | **Rule Set 2** |
| --- | --- |
|  Mr. Ms. Mrs. Miss St. Pl. Ave. Ct. ‘PO Box’ ‘P.O. Box’ DOB d.o.b. ‘date of death’ death: ‘release date’ ‘admit date’ ‘date of admission’ Age: ‘(ddd) ddd dddd’ ‘ddd-ddd-dddd’ \*@\*.com \*@\*.net \*@\*.gov \*@\*.biz SSN ‘Social Security Number’ ddd-dd-dddd Account Number: Acct.: Acct. # ‘Certificate Number;’ ‘Certificate #’ ‘License Number:’ ‘License #:’ ‘/~\*’ \*.\*.\*.\* |  insured claimant adjuster ‘date of incident’ ‘claim #’ ‘claim number’ ‘medical record’ ‘subscriber ID’ ‘mammogram’ ‘radiological film’ x-ray xray injury ‘micro film’ ‘ct scan’ MRI mylogram ‘dental film’ ultrasound tommagram ‘cine film’ ‘video film’ ‘body scan’ confidential pathology |

How to enable the HIPAA rule set

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Policy Filter Settings section of the center pane, next to HIPAA rule set, click Enable.4. When prompted, read the disclaimer, and then click OK to confirm your decision and accept the disclaimer. |

How to disable the HIPAA rule set

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Policy Filter Settings section of the center pane, next to HIPAA rule set, click Disable.4. When prompted, click OK to confirm your decision. |

When prompted, click OK to confirm your decision.

## See Also

[Create an E-mail Footer for Outbound E-mail](#ze6ad06056feb4f509adba223b9fe8a8b)

# Create an E-mail Footer for Outbound E-mail

You can add plain text and HTML footers to all outbound e-mail messages (including reply messages). Examples of common footers include your company’s name, address, and contact information, or a required legal disclaimer. You can apply this feature at the domain level (Parent Domains or Virtual Domains).

How to add a message footer to all outbound messages from a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Service Settings section of the center pane, next to Outbound E-mail Footer, click Edit.4. In the Outbound E-mail Footer dialog box, in the Text footer box, type a message footer as plain text without formatting options.5. In the HTML footer box, type an HTML-based message footer. You must add the appropriate HTML tags.6. Click Save.  |

# Edit Archive Settings for a Domain

You can edit the message retention period or legal hold settings for a domain. Domain settings override company default settings.

How to edit archive settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains subtab.2. Click the appropriate domain.3. In the Service Settings section of the center pane, next to Archive Settings, click Edit.4. Select Enable or Disable from the Legal hold box to enable or disable the legal hold function for the domain. Messages reaching the end of their retention period will not be destroyed while legal hold is enabled.5. In the Retention period box, specify how long messages will be held in the archive before they are destroyed.6. Set the archive settings and then click Save. |

# Configure Quarantine Settings

From a domain’s management information on the Domains tab, you can update Spam Quarantine and Policy Quarantine settings, as well as record an e-mail address to which false-positive submissions (legitimate e-mail misidentified as spam) should be sent. In the Quarantine dialog box, you can modify your quarantine settings for an individual domain.
To modify these settings, you must have the Spam Quarantine and Policy Quarantine features enabled for the domain.

Note

It takes approximately 30 to 35 minutes before changes to the Spam Quarantine and Policy Quarantine settings become available for your Hosted Filtering services.

How to edit quarantine settings for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains list, click the name of the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Quarantine pane, click Edit.4. In the Quarantine dialog box, select the quarantine settings you want to use. For a description of each policy setting, see the Quarantine Settings Options table below. |

### Quarantine Settings Options

| **Quarantine Option** | **Description** |
| --- | --- |
| Spam Quarantine Section |  |
| Allow user access | This setting permits users to sign in to the Spam Quarantine user interface. If you do not select this option, Spam Quarantine notifications will still be delivered to the user. |
| Allow Outlook add-in download | This setting allows users to download and use the Microsoft Junk E-Mail Reporting Tool for Microsoft Office Outlook 2003 and Office Outlook 2007. The Junk E-Mail Reporting Tool allows Office Outlook users to report junk e-mail to Microsoft and its affiliates for analysis, to help improve the effectiveness of Microsoft junk e-mail filtering technologies. |
| Policy Quarantine Section |  |
| Allow user access | With this setting, all users are allowed to sign in to the Policy Quarantine user interface and view their Policy Quarantine. This option allows them to access e-mail that has been quarantined because of a domain policy rule. If this option is not selected, then only administrators have access to the Policy Quarantine. |
| Attachment download | This setting specifies whether attachments can be downloaded in messages that have been quarantined because of a policy rule, and whether all users, or only administrators, can take action on the message. |
| Message release | This setting specifies whether messages that are quarantined because of a policy rule can be released and delivered to the original recipient’s Inbox, and whether all users, or only administrators, can take action on the message. |
| False Positive Submission Copy Section |  |
| Copy address | With this setting, you can add an e-mail address to which a copy of the Spam Quarantine false-positive submission is to be sent. The e-mail address you specify can be from any domain within your company. |

# User Account Management

The Users tab on the Administration tab allows you to add and manage users for both the Microsoft Forefront Online Protection for Exchange (FOPE) Filtering and version of the Exchange Hosted Archive services after version 8.1.

Note

Users uploaded through the Administration Center or through the Directory Synchronization Tool (DST) will show up in the User List View. Users uploaded through the Legacy Directory Synchronization Tool or through SFTP will not show up in the User List View and cannot be used to access the Administration Center or the Quarantine web site.

The User properties page allows administrators to update service settings for individual Users. The Import Users From File pop-up from the Users tab in the Administration Center allows service settings to be updated by using the same .csv file that is used for uploading users to the Company, Domain, or Virtual Domain.

# User Settings

From the list view on the Users tab on the Administration tab, you can click on the Primary e-mail address to view and modify the properties for any of the users in your company.

# Preferences

If you use the Administration Center for your User List upload mode, the First Name and Last Name of your user can be updated in the User Settings on the user properties page. If you use the DST for user upload, then these values cannot be edited through the Administration Center. You can edit the user settings to match your user's preferred language and time zone settings. The Language and Time Zone preferences can be configured at the company or domain level also. The most specific setting will be applied. Language preferences are applied to Spam Notifications and the Archive Viewer web pages.

# Domain

You can also view the Domain to which the User belongs. This domain will be the domain of the Primary e-mail address for the user.

# Virtual Domain

Virtual Domains are used for applying specific settings to a subset of users in a domain. If the user has been associated with a Virtual Domain, then this will display under the User Settings. Users may not belong to more than one Virtual Domain. If you want to change the Virtual Domain association, the user should be associated to the new Virtual Domain through the User Upload in the Administration Center. In order to remove all Virtual Domain associations from the user, disable the active Virtual Domain. See [Virtual and Parent Domains](#z643fe906820d42c489cdf1d4e559536f) for more information on Virtual Domains.

# About User Roles and Permissions

For each FOSE service, users are assigned to specific roles. Each role has a unique set of permissions that define access to and rights to use specific functions in the Administration Center. The table below lists each role and its permissions level in the Administration Center.

| **Role** | **Permissions** |
| --- | --- |
| Administrator | The Administrator has full access to all service settings and can do the following: Manage all company settings and properties. Manage all domains (create, modify, and delete). View audit trail information. Manage all user account information (create, modify, and delete). In order to Import Users From File, the permission must be granted at the Company level. Assign FOSE and Exchange Hosted Archive (EHA) permissions and Roles. Assign FOSE and EHA permissions and roles. Manage the DST. Permissions must be granted at the Company level. Create and run reports. Subscribe to RSS feeds. Manage Spam Filtering and Policy Filtering settings for all user accounts. View all quarantined e-mail for all users. |
| Administrator (read-only) | The Read-Only Administrator role has access to company and domain settings and can do the following:  View all company settings and properties. View all domain settings. View audit trail information. View all user account information. Create and run reports. Subscribe to RSS feeds. Run message trace. |
| Reporting User | The Reporting User has access to reporting features and can do the following: Create and run reports. Trace messages. |
| Account Manager | The Account Manager has access to user account management features and can do the following: View all company settings and properties. View all domain settings. Manage all user account information (create, modify, and delete). In order to Import Users From File, the permission must be granted at the Company level. Manage the DST. Permission must be granted at the Company level. Note: this role cannot change passwords for Administrators. |
| Quarantine Administrator | The Quarantine Administrator has access to spam-quarantined and policy-quarantined messages and can do the following: View all quarantined e-mail for all users. |
| Archive Relationship Administrator | The Archive Relationship Administrator has access to user relationships for the hosted archive service and can do the following: View and modify user relationships for hosted archive users. |
| Archive Retention Administrator | The Archive Retention Administrator has access to retention policy settings for the hosted archive service and can do the following: View and modify retention policy settings for the hosted archive service. |
| Archive Roles Administrator | The Archive Roles Administrator can view and modify user roles for EHA Viewer users and do the following: Create custom user roles for the Archive Viewer users. |
| Archive Compliance Administrator | The Archive Compliance Administrator has access to compliance-related settings and can do the following: View and modify compliance-related settings in the Administration Center. |

# Edit Archive Settings for a User

You can enable or disable the Exchange Hosted Archive service for a user, edit the message retention period, or enable or disable legal hold for a user.
If message retention period and legal hold settings are not specified for the user, the default settings configured for your company or for the user’s domain will be applied to the user.

How to edit archive settings for a user

|  |
| --- |
| 1. On the Administration tab, click the Users subtab.2. Click the appropriate user account.3. In the Service Settings section of the center pane, next to Archive Settings, click Edit.4. Select Enable or Disable from the Archive Service box to enable or disable the Exchange Hosted Archive service for the user. Messages reaching the end of their retention period will not be destroyed while legal hold is enabled.5. In the Retention period box, specify how long messages will be held in the archive before they are destroyed.6. Click Save. |

# Assign Archive Roles to User Accounts

You can assign archive roles for a user account. The archive roles define the user’s archive permissions.

How to assign archive roles to user accounts

|  |
| --- |
| 1. On the Administration tab, click the Users subtab.2. Select the check box(es) next to the user account(s) that you want to assign archive roles to, and then click Assign Archive Permissions.3. In the Edit Archive Role Settings dialog box, select archive role(s), and then click Save.  |

The following table summarizes built-in archive roles that are available.

| **Archive Role** | **Permissions** |
| --- | --- |
| Compliance Manager | Can view all user messages and use all Archive Viewer functions. |
| Compliance Officer | Similar to a Supervisor, but can resolve all escalated messages. |
| Compliance Operator | Has most of the rights of the Compliance Manager, but cannot view contents of messages other than their own or messages shared to them. |
| Disaster Recovery Manager | Can view and restore their own messages, send emergency notifications, and run some disaster discovery related reports. In order to allow a Disaster Recovery Manager to restore all messages, a custom role must be set up explicitly allowing the Disaster Recovery Manager to view and export other users’ messages. |
| External Compliance Auditor | An external individual who has access to folders and messages specifically shared to him/her. |
| Human Resources Manager | Can view their own messages and messages shared to them, and view their own folders and folders shared to them. |
| Monitor | Can access the Review tab in the Archive Viewer. |
| Supervisor | Can view and review messages of assigned subordinates, and annotate and escalate messages for further review. |
| Technical Administrator | Can run most reports in addition to having access to their own messages. |
| Worker | Can view and search their own messages, send and receive messages, restore their own messages, create folders for their messages, and export their messages. |

# Manage User Relationships

In the Administration Center, you can manage supervisory relationships for the Hosted Archive service.

 Subordinate: Assigns new subordinates to a supervisor, so that the supervisor can review subordinates’ messages. You can configure message harvest settings for the subordinates.

 Supervisor: Assigns subordinates to compliance officers.

 Supervisor Delegate: Allows another supervisor to act on behalf of a supervisor.

How to add relationship

|  |
| --- |
| 1. On the Administration tab, click the Users subtab.2. Click the user account that you want to manage.3. In the Tasks pane, click Manage User Relationships.4. In the Views pane, click Subordinate, Supervisor, or Supervisor Delegate, and then click Add Relationship in the Actions pane.5. Search for the desired user(s), and then select and move the user(s) to the Candidates box.6. Click Save. |

How to edit message harvest settings for a subordinate

|  |
| --- |
| 1. On the Administration tab, click the Users subtab.2. Click the user account that you want to manage.3. In the Tasks pane, click Manage User Relationships.4. In the Views pane, click Subordinate.5. Select the check box next to the subordinate you want to set review settings for, and then click Edit Relationship in the Actions pane.6. In Edit Relationship pane, in the Review section, select Yes for Needs review. If the user needs NASD 3010 compliance review, select Yes for Needs 3010 review.7. In the Sampling Percentage section, set the sampling percentage for each type of messages. For example, if you want to sample 10 percent of external e-mail messages, type 10 in the External e-mail box.8. Click Save. |

# Edit User Account Settings

After you create a new user account in the Administration Center, you can modify the user settings, including user preferences, service and security settings, password information, and permissions. Additionally, you can enable and disable user account settings. This topic describes how to complete the following tasks:

 Edit settings and preferences for a user account.

 Enable or disable a user account’s Forefront Online Protection for Exchange (FOPE) Filtering settings.

 Enable or disable a user account’s Exchange Hosted Archive settings.

 Add additional e-mail and instant messaging (IM) addresses.

 Edit permissions for a user account.

Note

Service settings for multiple users can be updated through the use of a .csv file. For information on how to do this see [Update Service Settings for Multiple Users](#zc879a458f0c84c288faf1e0d6582c318).

# Edit User Preferences

For each user in your company, you can specify the First Name, Last Name, default language, and time zone.

How to edit user account settings

|  |
| --- |
| 1. On the Administration tab, click the Users tab. 2. Click the name of the user account that you want to edit. The management information for that user account appears on the Users tab.3. In the User Settings pane, next to Preferences, click Edit.4. In the Preferences dialog box, edit user options as needed, and then click Save.  |

# User Service Settings

You can view the current service subscriptions that are available for your users. If you need to disable or enable specific filtering services for the user, Filtering Settings can be changed. The services must be enabled on the domain in order to enable them on the user. If you subscribe to the post-8.1 Archive, users can also be disabled for archiving from the Archive Settings section of the Services Settings pane.

How to enable or disable Hosted Filtering settings for a user account

|  |
| --- |
| 1. On the Administration tab, click the Users tab. 2. Click the name of the user account that you want to edit. The management information for that user account appears on the Users tab.3. In the Service Settings pane, under Filtering Settings, enable or disable the following services: Spam Filtering: Messages sent to and from this user account will be scanned for spam messages. Virus Filtering: Messages to and from this user account will be scanned for viruses. Policy Filtering: Messages to and from this user account will be scanned against Policy Filter rules. Spam Quarantine Notifications: The user account will receive Spam Quarantine notifications. Click Save.  |

How to edit Hosted Archive settings for a user account

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. Click the name of the user account that you want to edit. The management information for that user account appears on the Users tab.3. In the Service Settings pane, under Archive Settings, click Edit.4. In the Archive Settings dialog box, edit the following options: Archive Service: Enables or disables Hosted Archive features for this user account. Legal Hold: Enables or disables the Legal Hold feature for the user account, which allows you to select messages and prevent them from being deleted from the archive, and to override any retention period settings for the selected messages. Retention Period: The amount of time that messages are archived before they are automatically deleted from the Hosted Archive service.  |

# E-mail and IM Addresses

The five types of addresses are as follows:

 Primary e-mail

 Secondary e-mail

 Alternate e-mail

 Bloomberg

 IM

Only one primary e-mail address can exist per user, and it is assigned when the user is created. This primary e-mail address is the User Name used to log on to the Administration Center and Quarantine (based on permissions). The primary e-mail is also used for Directory-Based Edge Blocking when you configure this feature to use Admin Center or Directory Synchronization Tool as the User List Source. A primary e-mail address must be from a domain that you have registered in the Admin Center.

The secondary e-mail address is an additional proxy address associated with the primary e-mail address. As with the primary, if your domain has Directory-Based Edge Blocking enabled and configured to use the Admin Center as the User List Source, then secondary addresses will also be accepted at the inbound filtering edge. The secondary e-mail address can also be used for logging into the Administration Center or the Quarantine. If a user has secondary e-mail addresses and the domain settings for those addresses are configured to allow Quarantine access all Quarantine folders will automatically be displayed when a user logs into the Quarantine Web site. A secondary address must be from a domain that you have registered in the Admin Center.

The alternate e-mail address is used for Emergency Notifications in the post-8.1 Exchange Hosted Archive service. These are addresses that do not belong to the domains you have registered in the Administration Center. Rather, they are out-of-band, and can be used for emergency communications if all of your domains are unable to receive e-mail.

Bloomberg and IM addresses are used for the post-8.1 Exchange Hosted Archive service, and do not apply to the filtering service.

How to add additional e-mail and IM addresses to a user account

|  |
| --- |
| 1. On the Administration tab, click the Users tab. 2. On the Administration tab, click the Users tab. 3. In the center pane, under E-mail Addresses, click Add.4. In the Add Address dialog box, in the Address type box, select the type of address that you want to add to the account.5. In the Address box, type the full e-mail, Bloomberg, or IM address that you want to add.6. Click Save.  |

# Change Your Password

You can change passwords by using the logon page of the Administration Center. To change your password from the sign-in page, you must know your current user name and password.
Additionally, if you have Administrator rights, you can change your password from the Users tab on the Administration tab of the Administration Center. The user properties page will display the last date that the password was updated.

How to change your password from the sign-in page

|  |
| --- |
| 1. Go to the Administration Center, and click Change Password.2. Follow the instructions on the page to enter your new password information.3. Click Change. |

How to change your password from the Users properties page

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. On the users list, search for and select your user account.3. In the Security pane, next to Password, click Change Password.4. In the Change Password dialog box, enter the password for the account you used to sign in to the Administration Center and then type and confirm the new password for your account.5. Click Save.  |

# Change Another User's Password

When a user account is first added to the Administration Center, it is not assigned a password. However, you can create a password in the Administration Center. Users with the Administrator or Account Manager role have the ability to change passwords for other users. The Account Manager cannot change the password for a user with an Administrator role.

After the user account is created in the Administration Center, users can set or reset their password from the Administration Center, Spam Quarantine, or Archive Viewer sign-in pages. Administrators can also update users’ passwords if the passwords need to be changed or reset.

How to change a user password from the Administration Center

|  |
| --- |
| 1. In the Administration Center, click the Administration tab, and then click the Users tab.2. Click the user account whose password you want to change.3. In the Security pane, click Change next to Password.4. Enter the password for the logged on Administrator, then enter the new password for the user and confirm it, and then click Save.5. In the Security pane, under Password, verify the time that the password was last changed.6. Provide the user with the new password.Note We recommend that you use a protected communications channel to provide users with their password information, and instruct users to change their passwords as soon as possible. |

After you successfully reset the user’s password, the Password section of the Security pane on the Users tab will display the time that the password was last changed. You must provide the user with the new password after it has been changed.

# Have Your Password Sent to You

If you forget your password, you can have a tokenized URL sent to any of the SMTP addresses associated with your user account. To do this, you must have access to the mailbox that is associated with the e-mail address.
 If you do not have access to this mailbox, contact your administrator to get your password reset.

To have your password sent to you

|  |
| --- |
| 1. On the sign-in page of the Administration Center, click Need your password?2. Type your primary, secondary, or alternate e-mail address, and then click Send. The system validates your e-mail address, and then sends your password information as a tokenized URL to the e-mail address that you entered. If you enter your primary e-mail address, the tokenized URL will be sent to both the primary e-mail address and the alternate e-mail address. |

Note

The e-mail address you enter must be an SMTP proxy address associated with your user account. If you enter an e-mail address that is not in the Administration Center, or is not one that lets you to log on to any of the associated Web sites, the e-mail validation process will fail. You will not receive the tokenized URL at any e-mail address.

# Assign Hosted Filtering Permissions to a User

You can assign Forefront Online Protection for Exchange filtering permissions to a user by granting specific user roles from the user’s management information on the Users tab of the Administration tab. Roles can be applied at the domain level or the company level, and users can have multiple roles. The highest level of permission will be saved and displayed in the Security pane of the account details for each user.
For more information about user roles and permissions, see [About User Roles and Permissions](#zfca053bd3fc9483b905d10bd56286579).

How to add Hosted Filtering permissions to a user account

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. Click the appropriate user account. The management information for that user account appears on the Users tab.3. In the Security pane, next to Permissions, click Grant.4. In the Edit Filtering Role Settings dialog box, In the Role list, click the role you want to assign to the user. See [About User Roles and Permissions](#zfca053bd3fc9483b905d10bd56286579) for a description of each user role.5. Under Scope, select whether the role should be applied to a specific domain or across the entire company. If you select Company, enter the company name in the text box.6. Click Grant.  |

# Add Users

The user list source is configured in the User List Settings section of the Service Settings on the domain properties page.

## Primary ways to add user accounts to your hosted services

 Use the Directory Synchronization Tool (DST) (recommended): The DST is an on-site application that communicates with your company’s on-site Active Directory Domain Services and Microsoft Exchange Server messaging environment to build a user e-mail address list for your FOSE and EHA services after version 8.1. With this tool, you can manage your user accounts by using your on-site Active Directory Domain Services environment. User accounts that are synchronized with the DST will be automatically added in the Administration Center. For these user accounts, specific service settings can be controlled, quarantine accounts are pre-populated, and DBEB applies, as does the EHA service version 8.1. For more information, see [Directory Synchronization Tool](#zab46365b12a74adfbc36acb619e9094f)

 Use the Administration Center: Through the Administration Center, users can be added individually, or in batches with an uploaded comma-separated values (CSV) file that contains a list of multiple user names and their related service information. After you add users, you can then edit their user account information and assign roles and permissions.

For these user accounts, specific service settings can be controlled within the Administration Center. If you need to configure an account to bypass spam filtering or exempt them from Policy Rules, which can be controlled on the User properties page. Once the accounts are present in the Administration Center, they are automatically available for accessing the Quarantine and Exchange Hosted Archive mailboxes (after version 8.1) for the users based on domain restrictions. The SMTP addresses for the User can also be used for Directory-Based Edge Blocking (DBEB).

 Upload a user list by using Secure FTP (SFTP): You can create a user e-mail address list and upload it to a Secure FTP (SFTP) directory for your domain. The FOSE service first verifies that the user list meets the correct format requirements, and then adds the users to your services. Users who are synchronized through SFTP will not show up in the Administration Center, but can be used for DBEB. In order to remove user accounts from DBEB that have been uploaded through SFTP, an empty SFTP list should be uploaded for the domain.
For more information, see Use SFTP Upload to Add User Accounts.

 Use the Legacy DST: As with the DST, the Legacy DST is an on-site application that communicates with your company’s on-site Active Directory Domain Services and Microsoft Exchange Server messaging environment to build a user e-mail address list for your FOSE or EHA version 8.1 services. With this tool, you can manage your user accounts by using your on-site Active Directory Domain Services environment.

User accounts that are synchronized with the Legacy DST will not show up in the Administration Center, but can be used with DBEB and for the EHA service version 8.1. For more information, see [Legacy Directory Synchronization Tool](#zfbdc6483affe44fbbff6d1f30162377d)

Important

In order for messages (both sent and received) to be associated with a user, the user must be set up as an archive enabled user in the Administration Center.  Primary as well as secondary SMTP address must be configured.
All messages sent to or received by unregistered SMTP address are handled as follows:

 These messages are not available in the user’s My Messages folders  (this specifically applies to messages archived before the user is registered).

 Because these messages are not associated with a user, they will not be selected for supervisory review.

 Search may be affected, depending upon the search criteria used.  Searches performed based on date or keyword criteria will include these messages.  Searches based on the user account(s) will not include these messages.   Searches based on the SMTP address will only include these messages if the unregistered SMTP address matches the search criteria.

For example:  If Mary Smith, who has an Administration Center account with the primary SMTP address of marysmith@contoso.com and an unregistered SMTP address of mary.smith@contoso.com, searches with the text marysmith will return messages to or from marysmith@contoso.com, but not mary.smith@contoso.com.   Similarly, messages sent to msmith@contoso.com, or any other unregistered addresses or alias, may not be included in the search results.

If messages are ingested into the archive prior to the creation of the user’s SMTP addresses, the messages must be linked to the user account.  This can be done by [Technical Support](#zdd85cd8b1bdf4622806eb266280116e0).

How to specify the User List source for a domain

|  |
| --- |
| 1. On the Administration tab, click the Domains tab.2. In the Domains pane, click the domain that you want to modify. You can search for a specific domain name by using the search box.3. In the Service Settings section of the center pane, next to User List Settings, click Edit.4. In the Select the user list source drop down, click one of the following options: Admin Center: Configures the Administration Center as the authoritative source for the User Accounts with Primary SMTP addresses in that domain. These addresses will be visible in the Administration Center. Secure FTP: Configures Secure FTP as the authoritative source for the User Accounts with SMTP addresses in that domain. These addresses will not be visible in the Administration Center. Directory Synchronization Tool: Configures the Directory Synchronization Tool as the authoritative source for the User Accounts with Primary SMTP addresses in that domain. These addresses will be visible in the Administration Center. Legacy Directory Synchronization Tool: Configures the Legacy Directory Synchronization Tool as the authoritative source for the User Accounts with Primary SMTP addresses in that domain. These addresses will not be visible in the Administration Center.5. Specify the Directory-Based Edge Blocking (DBEB) mode if desired. See [Directory-Based Edge Blocking](#z10a04ed0c0a54f54b53f7606e1098033).6. Specify the e-mail address that you want to receive any error notifications which may occur during the User List upload in the \*Error notification address text box. This option will show if the domain is enabled for DBEB unless the User List source is Directory Synchronization Tool.7. Click Save. Note If you select Secure FTP as the user list source for user accounts but then later need to switch to the Admin Center or Directory Synchronization Tool as the list source, you will need to delete the existing list of user accounts from the Secure FTP database. To do so, give a blank file the same name as the one used for your existing list of user accounts in the Secure FTP. Then, upload this blank file using the Secure FTP. That will strip the Secure FTP of the existing user accounts and allow you to switch the user list source to either Admin Center or Directory Synchronization Tool.  |

# Add New Users in the Administration Center

You can add users with the Add User feature of the Administration Center, which adds one user account at a time.

How to add a new user account by using the Administration Center

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. In the Tasks pane, click Add User.3. In the Add New User dialog box, enter the primary e-mail address of the new user, and then click Save.  |

Note

This e-mail address must be part of your company’s domain.The primary e-mail address is also the user name that is used to sign in to your company’s FOSE services.

After you have successfully created the user account, the user’s management information appears on the Users tab. Here you can update user information, assign permissions, and update password information. For information about how to modify user account settings, see [Edit User Account Settings](#za70bf9ea6bd04576914cc28656fb3b84).

# Import Multiple Users

If you need to import multiple user accounts at once, you can create a CSV file by using Microsoft Office Excel to create a list of user names and other information, and then upload that file to the Administration Center. In order to use the Import Users from File functionality in the Administration center, you will need to have the role of Administrator or Account Manager (at the Company level) in the system.

If you need to associate user accounts with a Virtual Domain through the Administration Center, create a CSV file by using Microsoft Office Excel to create a list of user names and other information, then upload that file to the Administration Center. Be sure to specify the target Virtual Domain in the Choose the virtual domain if this is for user grouping: domain dropdown list to associate those users with the virtual domain.

How to create a list of users as a CSV file

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Open Microsoft Office Excel.2. Enter user information as separate values on the same line in your file, following this order:a. \* Primary e-mail address (\* required)b. First namec. Last named. Secondary e-mail address(es)e. Instant message address(es) (Separate the alias part of the IM address from the IM Provider name with a backslash "\". For example, "lukaa\msn" is an IM address.) (For Exchange Hosted Archive)f. Alternate e-mail address(es) (Add the string "alt:" to the beginning of all alternate e-mail addresses for the user. For example, "alt:davidp@hotmail.com" is an alternate e-mail address.) (For Exchange Hosted Continuity)Example: The following example shows a user file with two users. The first user (Luka Arbus) has one secondary e-mail address and one instant message address; the second user (David Pelton) has two alternate e-mail addresses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| luka@contoso.com | Luka | Arbus | lukaarbus@contoso.com |  lukaa\msn |
| david@contoso.com | David | Pelton | alt:davidp@hotmail.com | alt:d.pelton@hotmail.com |

3. Save the file in CSV format.Note For more information regarding user addresses see [E-mail and IM Addresses](#z537cb0cc36b34cefb80998dd3a4da20c).  |

How to import the CSV user file

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. In the Tasks pane, click Import Users From File.3. In the Send status notifications to the following e-mail box, type the e-mail address for where to send upload status information. 4. In the Specify the user list file box, browse to and select the CSV file you created and saved to your own files.5. To add the users to a virtual domain, in the Choose the Virtual Domain if this is for user grouping list, click the domain.6. To disable all the user accounts that are not included in your user file after the user file has been successfully uploaded, select the Disable all users not specified in the file check box.7. Click Save. |

After you begin the upload process, status notifications are sent to the e-mail address you specified. If the new user accounts were not added to your services, then the process did not complete. This may be the result of an improperly formatted CSV file. Recheck the formatting of your CSV file (see formatting example in To create a list of users as a CSV file above), and then retry the upload process in the Administration Center.

# Update Service Settings for Multiple Users

The Import Users From File pop-up from the Users tab in the Administration Center allows service settings to be updated by using the same .csv file that is used for uploading users to the Company, Domain, or Virtual Domain.

# Additional User Upload Information

If a user list is uploaded from the Administration Center and the associated addresses for a primary e-mail address have changed, all previously associated addresses will be attributed to a disabled user account.
For example, the e-mail address wilson@contoso.com is configured as a primary e-mail address for a user’s account. The user account also has an associated secondary e-mail address of wilsonb@contoso.com, another associated secondary e-mail address of wilsonb@woodgrovebank.com, and an alternate e-mail address of wilsonb@alpineskihouse.com.
If a new user list is uploaded by using the Administration Center and the alternate e-mail address (wilsonb@alpineskihouse.com) was not present in the updated list, the alternate address will be removed from the primary user account and split into a separate, disabled user account. In this example, the primary user account, wilson@contoso.com, will remain enabled with the associated secondary addresses of wilsonb@contoso.com and wilsonb@woodgrovebank.com. However, a new user account will be created for the previously associated alternate e-mail address, wilsonb@alpineskihouse.com, and set to disabled.
You will be able to access the disabled user account in order to see which value was missing from the user list that was uploaded. Once you identify the addresses that were excluded during the import process, you can update the user list with the appropriate data, and upload the list again. After you upload the corrected user list, the disabled user account will be automatically merged back into the enabled user account associated with the primary e-mail address.
If you do need to permanently remove the previously created, disabled user accounts, use the Disabled User Accounts View to delete the user accounts.

Note

The delete functionality is only available for customers who do not subscribe to the Hosted Archive service.

# Enable or Disable User Accounts

After a user account is created, it is enabled by default and inherits the service settings from the domain.
If a user account is no longer being used, you can disable the user account, thereby restricting access to Forefront Online Security Exchange (FOSE) for that account.

How to enable or disable a user account

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. On the Views pane, in the All Users list, click the user group that you want to enable.3. In the Tasks pane, do one of the following:  Click Enable User Account to allow the associated user to access the FOSE services and related Web sites. Click Disable User Account to restrict use of the FOSE services and related Web sites. Note When you disable a user account, all roles and permissions are retained, in the event that the user account must later be re-enabled. |

# Delete a User Account

If you need to remove a user’s account, you can delete the user account. When you delete a user account, all account settings are removed.If you want to temporarily restrict a user’s access to your Forefront Online Security (FOSE) services, then you can disable the associated user account. Disabling a user account restricts access to FOSE services, but does not remove the account or its settings.

How to delete a user account

|  |
| --- |
| 1. On the Administration tab, click the Users tab.2. In the All Users pane, select the check boxes next to all user accounts that you want to disable, and then click the Disable button.3. When prompted, click OK to confirm that you want to disable the account.4. On Users tab, in the Views pane, click Disabled User Accounts.5. In the Disabled User Accounts pane, select the check boxes next to all user accounts that you want to delete, and then click Delete.6. When prompted, click OK to confirm your deletion. |

Note

The delete functionality is only available for customers who do not subscribe to the Hosted Archive service. Once a user account has been deleted, it cannot be recovered. All settings and permissions for the user will be deleted from the Administration Center.

# Use Secure FTP to Add User Accounts

The Administration Center allows you to add users by uploading a user list to a Secure FTP (SFTP) site. After you upload the user list to the SFTP site, the contents of the file will be reviewed by the system and changes to the user list will be applied for Directory-Based Edge Blocking and Virtual Domain filtering.
Each Company is allocated a single SFTP user ID, which is used for the entire company. Users must contact Technical Support for password changes. For more information about how to create a user list file, see Secure FTP File Format and About Secure FTP Upload.
Adding users by SFTP allows you to create a user e-mail address list and add it to an SFTP directory. The FOSE system scans this directory for new e-mail addresses, and updates your existing user list with the information from the upload user list.
This topic describes how the SFTP upload method works, and compares this upload method with the Import Users from File method.

# Subdirectory Structure

You can upload, download, and delete files in the allocated Secure FTP (SFTP) directory structure, also termed the subdirectory. You can perform these actions only within the subdirectory, because you are not granted shell access to the SFTP site. You use the SFTP upload method to upload a list of e-mail addresses for any domain in your company, specifying a Directory-Based Edge Blocking option for each domain.
The table below, Comparison of Import Users from File and SFTP-Based Upload Methods, shows the difference between the two upload methods.

## Comparison of Import Users from File and Secure FTP-Based Upload Methods

| **Feature** | **Import Users from File** | **Secure FTP** |
| --- | --- | --- |
| One domain per file | Yes | Yes |
| Multiple domains per file | Yes | Yes |
| Multiple files per domain | Yes | No |
| Multiple options per domain | No | No |
| Specify Directory-Based Edge Blocking option in upload file | No. When you add user accounts from within the Administration Center, whether on a bulk basis with Import Users From File (on the Users tab, in the Tasks pane), or on an individual basis in the Accounts tab, you must select domain-level Directory-Based Edge Blocking options from the Administration Center as well.Note Only one edge blocking option per domain can be specified. Only one of the options (Pass Through, Reject, Reject Test, or Passive) can be used at any given time for any given domain. | Yes. A tag in the upload file allows you to specify the edge blocking type. |

Edge blocking options are not available to Virtual Domains. E-mail for a particular Virtual Domain is processed for all e-mail addresses that are included in an upload list for that Virtual Domain, as specified by the settings in the Administration Center. If e-mail is received for an address that is not listed in the upload list for the given Virtual Domain, it is processed according to the edge blocking settings for the Parent Domain. Domains that use different edge blocking options cannot be combined in the same file.
You can specify only one user list file per domain. Multiple domains can be merged into the same file, if all domains use the same edge blocking option (Pass Through, Reject, or Reject-Test). Multiple files can be placed in each directory.
Avoid inadvertently leaving multiple files in the subdirectories for a single domain.
When you replace a previously uploaded list for a domain, you must do one of the following:

 Reuse the same file name each time for that domain.

 Delete any existing files for that domain before uploading newer versions of those files.

You can upload files as often or as infrequently as you want.

# File Replication Schedule

When you upload a file to the Secure FTP (SFTP) directory, a script automatically validates the file. After the file has been validated, it is parsed and copied to a central location for replication across the network. Replication occurs every 15 minutes; as soon as replication is complete, the user lists are available for mail processing and filtering.

# File Validation Checking

Before any file uploaded via the Secure FTP (SFTP) method is accepted and used within mail processing, the system conducts a number of validation checks.

Note

If the SFTP upload process takes more than five minutes to complete and the #END\_OF\_FILE tag has not appeared within that time, then the file will be not be accepted.

Following a successful file upload (including the appearance of the #END\_OF\_FILE tag), the file may also be rejected if any of the following are included in it:

 Invalid domain: An address whose domain part is not a domain listed in the Administration Center for this organization (note that Directory-Based Edge Blocking does not currently support the “catch-all” feature).

 Duplicate domain: A domain listed twice in the same file.

 Invalid group: A group that is not a valid virtual domain with #GROUP – GROUP-ONLY tag.

 Duplicate group: A virtual domain listed twice in the same file.

 Invalid e-mail address: An e-mail address that is not compliant with RFC standards.

 Address not in domain: An e-mail address that does not belong to the specified domain.

 Non-English characters: An e-mail address that contains non-English characters.

If the validation script encounters any of the above errors, the list will not be processed. In this case, the validation script takes the first domain listed in the upload file, checks for the administrator e-mail address for that domain, as specified in the Error Notification Email Address box on the Directory Services tab in the Administration Center, and sends an error notification e-mail message to the administrator.

# Secure FTP File Format

Your user e-mail address list files should be in simple text format, with one e-mail address per line. File names are not subject to a maximum length restriction. File names must be suffixed with .txt, but otherwise they do not have to follow a specific naming convention.

# Specify the Directory Service Option

The first line of each file must be a tag that specifies which edge blocking option is going to be used: Pass-Through, Reject, or Reject-Test. All e-mail addresses in the file that follow this tag will be subject to the same option. Use the form: #Option.

# Specify Domains and Users

The specified user list must be preceded by a tag that indicates the domain to which these users belong, in the form: #DOMAIN domain name. E-mail addresses should be grouped following the domain that they belong to, on successive lines, with one entry per line.
The domain part of all e-mail addresses that follow the #DOMAIN tag must be the same as the domain specified in the #DOMAIN tag. See the following example:
#DOMAIN alpineskihouse.com
rmohrman@alpineskihouse.com
jarnold@alpineskihouse.com
To specify multiple domains in the same file, you can list them sequentially in any order, each with its corresponding user list immediately following it. See the following example:
#DOMAIN alpineskihouse.com
rmohrman@alpineskihouse.com
jarnold@alpineskihouse.com
 #DOMAIN contoso.com
dribaute@contoso.com
mkhalili@contoso.com
dpelton@contoso.com

# Specify Virtual Domains

User lists in virtual domains must be listed in the same file that contains the parent domain’s information, following the user list of that parent domain. Specify each virtual domain with the tag #GROUP virtual domain name GROUP-ONLY.
Enter each e-mail address that belongs to a virtual domain as an address in the form: local part@domain-part-of-parent-domain. See the following example:
#GROUP marketing.alpineskihouse.com GROUP-ONLY
rmohrman@alpineskihouse.com
jarnold@alpineskihouse.com
Each virtual domain must be explicitly listed as a domain on the Domains tab of the Administration tab in the Administration Center.

# Add End-of-File Tag

The last line of each upload file must use the following special tag to signify the end of the file:
#END\_OF\_FILE

# Add User Accounts by Using Secure FTP

Use the Secure FTP (SFTP) upload site to add user accounts to your service.

Note

To upload user e-mail address files by using SFTP, you first need a valid user ID and password to gain access to the FOSE SFTP site. Because the user ID and password for the SFTP site are different from those used by the Administration Center for authentication, you must request a separate set of user credentials to access the SFTP directory. You can obtain these credentials by contacting technical support.

How to add user accounts by using SFTP

|  |
| --- |
| 1. Go to the [Frontbridge file transfer protocol site](http://go.microsoft.com/fwlink/?LinkId=152780) (http://go.microsoft.com/fwlink/?LinkId=152780).Note You can connect to this site only on port 22, either automatically by using a script, or manually.2. Copy the user list file that you created to the SFTP directory. |

# Directory Synchronization Tool

The Microsoft Directory Synchronization Tool (DST) is an optional, light weight application that communicates with your company’s on-site Active Directory and Microsoft Exchange Server messaging environment to build a user e-mail address list for your Microsoft Forefront Online Protection for Exchange or post-8.1 Exchange Hosted Archive services. With this tool, you can manage your user accounts in your on-site Active Directory environment. In order to use the DST, you will need to have the role of Administrator or Account Manager (at the Company level) in the system.

The DST tool also collects all valid e-mail addresses from the corporate Active Directory and shares these addresses with Microsoft Forefront Online Protection for Exchange (FOPE) and Exchange Hosted Archive (EHA). User accounts synchronized with the DST appear in the Administration Center and can be managed in the same manner as an Administration Center upload.

In this tool, you as the administrator can specify the domains for which e-mail addresses will be synchronized and how often synchronization should take place.
The synchronization service then does the following:

1. Reads the configuration file (XML file) at the interval specified

2. Retrieves all SMTP addresses from Active Directory for the specified domains

3. Sends the list to the Hosted Services network via SSL.

The address list won’t be transferred until the administrator’s login/password have been authenticated. . A web service running on the hosted network accepts the list and feeds the data to the Directory Services infrastructure, which distributes the list to the FOPE data center network every 15 minutes.

The tool also collects and shares safe senders, as defined by end users. This feature helps to further reduce the possibility of false positives (legitimate e-mail misidentified as spam) and ensure minimum affect to legitimate e-mail communication. This feature requires Microsoft Exchange Server 2007, which stores safe-sender information in Active Directory Domain Services, and versions of Microsoft Office Outlook after Office Outlook 2003. Also, Safelist Aggregation must be enabled on your Exchange Server 2007 in order for this feature to operate. For more information on Safelist Aggregation, see http://technet.microsoft.com/en-us/library/bb125168.aspx.

# Administration Center Settings for the Directory Synchronization Tool

The following configuration settings for the Directory Synchronization Tool are managed from the Administration Center:

[Notification address](#z5755db44423d4f6c89cec871b40f3062)

[Domains](#za823e3ebb7e04bc9bd0a9d09b68cb013)

# Notification address

The default user list upload status notification address for the Company is configured in the User List upload notification address in the Filtering Settings section. After you begin the upload process, status notifications are sent to the e-mail address you specified. This address will be read by the Directory Synchronization Tool (DST) and will populate the Administration Center manual User List upload pop-up by default. This address can be overwritten in the Import Users From File pop-up from the Users tab and changed in the User List Settings section of a specific domain through the Administration Center. However, it cannot be changed via the 9.1 DST.

# Domains

In order for the domains to display in the Directory Synchronization Tool (DST), the User List upload mode must be set to Directory Synchronization Tool. See [Specify the User List Source](#zfd3c8b9e7b68448f9cf8a6809804a4da).For more information about the DST, see the [Microsoft Directory Synchronization Tool](http://go.microsoft.com/fwlink/?LinkId=149668).

# Legacy Directory Synchronization Tool

The Microsoft Exchange Hosted Services Directory Synchronization Tool (Legacy DST) is the older version of the 9.1 Directory Synchronization Tool (DST). Also an optional, light weight application, it communicates with your company’s on-site Active Directory Domain Services and Microsoft Exchange Server messaging environment to build a user e-mail address list for your Forefront Online Protection for Exchange (FOPE) or 8.1 Exchange Hosted Archive (EHA) services. The Legacy DST allows you to manage your user accounts by using your on-site Active Directory Domain Services environment. In order to use the DST, you will need to have the role of Administrator or Account Manager (at the Company level) in the system.

The Legacy DST collects all valid e-mail addresses from the corporate Active Directory Domain Services and shares these addresses with FOPE and EHA. It does so in two ways:

1. FOPE can be configured to allow you to use the addresses to apply a Directory-Based user list based on these e-mail addresses. Users synchronized with the Legacy DST do not appear in the Administration Center. E-mail sent to recipients not on the Directory-Based list is rejected by FOPE with a 554 error. You can review the Dir Edge column of the E-mail Traffic Report (available from the Reports section of the Administration Center) to see how much junk e-mail has been rejected due to Directory-Based Edge Blocking.

2. Exchange Hosted Archive can use the Legacy DST to synchronize the users with the Archive MWA for user management.

The tool also provides a user interface in which you can specify the domains for which e-mail addresses will be synchronized, and how often synchronization should take place. The synchronization system does the following:

1. Reads the configuration file (XML file) at the interval specified

2. Retrieves all SMTP addresses from Active Directory for the specified domains

3. Sends the list to the Hosted Services network via SSL.

The address list won’t be transferred until the administrator’s login/password have been authenticated. . A web service running on the hosted network accepts the list and feeds the data to the Directory Services infrastructure, which distributes the list to the FOPE data center network every 15 minutes.

Another notable function of the Legacy DST is its ability to collect and share safe senders, as defined by end users. This feature helps to further reduce the possibility of false positives (legitimate e-mail misidentified as spam) and ensure negligible impact to legitimate e-mail communication. This feature requires Exchange Server 2007, which stores safe-sender information in Active Directory, and Microsoft Outlook 2003 or higher. Also, Safelist Aggregation must be enabled on your Exchange Server 2007 in order for this feature to operate. For more information on Safelist Aggregation, see http://technet.microsoft.com/en-us/library/bb125168.aspx.

For more information on the Legacy DST see [The Microsoft Hosted Services Directory Synchronization Tool 8.1](http://go.microsoft.com/fwlink/?LinkId=137140).

# Policy Rules

In addition to spam and virus filtering, the Administration Center Policy Rules let you enforce specific company regulations and policies by configuring customizable filtering rules. You can create a specific set of rule options that match messages based on specific match expressions or match options and take a specific action against them when they are being processed by the Hosted Filtering service. For example, you can create a policy rule that will reject any incoming e-mails that have a certain word or phrase in the Subject or Body field. You can also create a policy rule that will reject e-mails with certain attachments files or just encrypt e-mails based on specific e-mail headers. Additionally, Policy Rules let you add and manage large lists of values (such as list of IP addresses, domains, e-mail addresses, file names, files extensions and keywords) for multiple policy rules by uploading a file (Dictionary) and linking these files in multiple policy rules.

For e-mail filtering policy rules, you can use one of the following syntax options to identify strings or text such as particular characters, words, numbers or patterns of characters in e-mails:

 Basic (a mixture of CSV and a simple string-wildcard syntax)

 RegEx (a subset of characters of the regular expression syntax)

For more information about policy rules, see the related topics listed in the See Also section.

## See Also

[Policy Rule Match Options](#z09a960727f0045c3ae705ea95f9043b2)

[Policy Rule Settings](#z1ab0f0c58c1a46619f6488fdfa119f4f)

[Create, Edit, or Delete a Policy Rule](#ze0d44821ed434b4883be6e458a5ae70b)

[Policy Rule Syntax](#z1b8c703569504d399d89c48817086112)

# Policy Rule Match Options

Policy rules can be configured to match expressions within the following parts of an e-mail:

 E-mail Header for field name and value

 E-mail Senders for IP addresses, domains, and e-mail addresses

 E-mail Recipients for domains and e-mail addresses

 E-mail Attachments for file names and file extensions

 E-mail Subject and Body for keywords and phrases

 Other e-mail message properties (e.g. e-mail size, number of recipients, character sets, etc.)

The types and capabilities of the policy rules that can be enforced for each e-mail part vary; details are listed below.

## E-Mail Header match options

| **E-mail part** | **Match for** | **Syntax** | **Additional match option(s)** |
| --- | --- | --- | --- |
| Header | Field name | Basic | N/A |
| Field value | Basic/RegEx | Case sensitive match |

Limitations:

 The combined character limitation for field name and field value is 990 characters

 Dictionaries are not available for the Header fields

Sample e-mail header rule using Basic syntax:

| **Header: Basic syntax** |
| --- |
| Name match expression: | Message-ID |
| Value match expression: | <d1234f1869fb3fb83bfd215319beb77c@www.contoso.com> |
| Interpretation: | Match when an e-mail header contains "Message-ID: <d1234f1869fb3fb83bfd215319beb77c@www.contoso.com>" |

Sample e-mail header rule using RegEx syntax:

| **Header: RegEx syntax** |
| --- |
| Name match expression: | X-Mailer |
| Value match expression: | ContosoMailer\s\[version\s1\.73\]|PartnerContosoMailer1234 |
| Interpretation: | Match when an e-mail header contains the header "X-Mailer: ContosoMailer [version 1.73]" including whitespaces OR "X-Mailer: PartnerContosoMailer1234" |

## E-Mail Sender match options

E-mail Sender match options allow you to specify the e-mail addresses, IP addresses, or top-level domains to which the policy rule will apply. If you have many e-mail addresses or domains that you want to use for this match option and don’t want to enter them manually, use the Dictionary in the Filters tab to upload a list of e-mail addresses or domains. This Dictionary can be reused for multiple policy rules. For details about how to use the Dictionary option, see [Filters](#zb6150b63c0b34f08b10bd4a5438356e0).

| **E-mail part** | **Match for** | **Syntax** | **Additional match option(s)** |
| --- | --- | --- | --- |
| Sender | IP addresses | Basic/CIDR | Dictionaries |
| Domains | Basic/RegEx | Dictionaries |
| E-mail addresses | Basic/RegEx | Dictionaries |

Limitations:

 The combined character limitation for field name and field value is 990 characters

 For the Basic syntax, only valid IP addresses, domains and e-mail address formats will be accepted.

 For IP addresses, Classless Inter-Domain Routing (CIDR) notation of IP addresses is not supported in the same rule with wildcard (\*) and question mark (?) metacharacters in Basic syntax. However, the comma as separator is accepted.

Sample e-mail Sender rule using Basic syntax:

| **Sender IP addresses: Basic syntax** |
| --- |
| Match expression: | 88.88.88.?, 99.99.\*.1, |
| Interpretation: | Match the Address Range 88.88.88.0 - 88.88.88.9 OR the Address Range 99.99.0.1 - 99.99.255.1 |

Sample e-mail Sender rule using CIDR syntax:

| **Sender IP addresses: CIDR syntax** |
| --- |
| Match expression: | 99.99.99.0/24, 88.88.88.88/32 |
| Interpretation: | Matching IP addresses equivalent to the subnet mask 255.255.255.0 resulting in match of 256 hosts for the CIDR Address Range 99.99.99.0 - 99.99.99.255 OR matching the CIDR Address Range 88.88.88.88 - 88.88.88.88 consisting of only one host. |

Sample e-mail Sender rule using RegEx syntax:

| **Sender domains: RegEx syntax** |
| --- |
| Match expression: | ^contoso\.com$|test.\*\.partner\.contoso\.com|\.info$ |
| Interpretation: | Matching only the domain "contoso.com" (not any sub domains of this domain) OR the sub domain "test" followed by any characters (e.g. "test1"," test1234", "testabcd" etc.) of the domain "partner.contoso.com". OR matching the Top Level Domain (TLD) “.info” |

Sample e-mail Sender rule using Basic syntax:

| **Sender e-mail address: Basic syntax** |
| --- |
| Match expression: | \*@contoso.com, \*@\*.contoso.org |
| Interpretation: | Any e-mail alias will be matched which have been sent from the domain "contoso.com" OR any e-mail alias sent from the domain "contoso.org" and any sub domain of this domain. |

### E-Mail Sender policy rule actions overview

A variety of policy rule actions apply to the Sender match option. You can use Inbound Policy Allow rules to safe-list an IP address, even if it is listed on the Reputation Block Lists (RBLs) that are used by the service. IP address ranges or Classless Inter-Domain Routing (CIDR) formatted IP ranges will not bypass the RBLs, but will still apply for allowing messages from the IP range to bypass spam filtering.

If you have added a Policy Allow rule for an IP and the mail from that IP is still being rejected, the bounce message being sent back to the sending server has instructions that allow them to request or investigate the de-listing of their IPs. If you would like to follow up on their behalf, please have the sender provide you with a copy of the bounce message that they are receiving and contact Technical Support to have the Support Team investigate the reason for the rejection.

To see a chart outlining the various policy rule actions that apply to this match option, see [Policy Rule Settings](#z1ab0f0c58c1a46619f6488fdfa119f4f). For more information about the Basic and RegEx syntax options, see [Policy Rule Syntax](#z1b8c703569504d399d89c48817086112).

## E-Mail Recipient match options

E-mail Recipient match options allow you to specify the e-mail addresses or top-level domains to which the policy rule will apply.

| **E-mail part** | **Match for** | **Syntax** | **Additional match option(s)** |
| --- | --- | --- | --- |
| Sender | E-mail addresses | Basic/RegEx |  Dictionaries Enable Opportunistic TLS for unspecified recipients Apply rule even if the e-mail message includes other recipients |
| Domains | Basic/RegEx |  Dictionaries Enable Opportunistic TLS for unspecified recipients |
|

Limitations:

 The character limitation for any field is 9,000 characters.

 For the Basic syntax, only valid domain and e-mail address formats will be accepted.

### Additional match options

 Dictionaries: If you have many recipients and/or e-mail addresses that you want to use for this match option and don't want to enter them manually, use the Dictionary option to upload a list. For details about how to use the Dictionary option, see [Filters](#zb6150b63c0b34f08b10bd4a5438356e0).

 Apply rule even if the e-mail message includes other recipients: If an e-mail message contains other recipients besides the ones specified in the policy rule, then the policy rule will not be applied to that message at all; the policy rule will be skipped. However, if this checkbox is selected, the following actions will be performed:

 For Inbound Policy Rules, messages will be bifurcated, and a policy action will be applied for all recipients in the same domain as the recipient specified in the policy rule. All recipients for domains not specified in the policy rule are not affected by the policy rule action.

 For Outbound Policy Rules, messages will not be bifurcated (except for the Force TLS Opportunistic TLS option) and the policy rule action will be applied for all recipients of a message.

| **Policy Rule** | **Apply rule even if the e-mail message includes other recipients** | **E-Mail containing recipients** Note **Example domains contoso.com and alpha.com are domains of the company, but acquisition.com is not.** | **Rule Behavior** |
| --- | --- | --- | --- |
| Traffic Scope: InboundDomain Scope: All domainsAction: RejectRecipient e-mail address: a@contoso.com | Not selected | a@contoso.com | Rule will be applied; message will be rejected. |
| Traffic Scope: InboundDomain Scope: All domainsAction: RejectRecipient e-mail address: a@contoso.com | Not selected | a@contoso.com; b@contoso.com | Rule will be skipped; all recipients will get the message. |
| Traffic Scope: InboundDomain Scope: All domainsAction: RejectRecipient e-mail address: a@contoso.com | Selected | a@contoso.com; e@acquisition.com | Rule will reject message to: a@contoso.com |
| Traffic Scope: InboundDomain Scope: All domainsAction: RejectRecipient e-mail address: a@contoso.com | Selected | a@contoso.com;b@contoso.com;c@alpha.com ;e@acquisition.com | Rule will reject messages to:a@contoso.com;b@contoso.comsince b@contoso.com belongs to the domain specified in the policy rule. |
| Traffic Scope: OutboundDomain Scope: All domainsAction: RejectRecipient e-mail address: e@acquisition.com | Not selected | e@acquisition.com | Rule will be applied; message will be rejected. |
| Traffic Scope: OutboundDomain Scope: All domainsAction: RejectRecipient e-mail address: e@acquisition.com | Not selected | e@acquisition.com; b@contoso.com | Rule will be skipped; all recipients will get the message. |
| Traffic Scope: OutboundDomain Scope: All domainsAction: RejectRecipient e-mail address: e@acquisition.com | Selected | e@acquisition.com; a@contoso.com; b@contoso.com; c@alpha.com | Rule will be applied; message to all recipients will be rejected. |

 Enable Opportunistic TLS for unspecified recipients: If the box is unchecked, then outbound messages will be bifurcated. This means that authenticated Transport Layer Security (TLS) will be enforced for the delivery of all recipients on the message, where any of the recipients match the Policy Filter rule and the recipient mail transfer agent (MTA) is configured to accepting TLS-based connections (including valid public certificates). If one of the recipients has an MTA that does not supporting TLS connections, then the message to this recipient will be rejected. Checking this box will still enforce authenticated TLS on the recipient who matches the rule, but also allows all other recipients to be transmitted using Opportunistic TLS if all attempts to enforce TLS fail. The Forefront Online Protection for Exchange service will always use the highest level of encryption available for transmission of the messages and if not available step down.

Examples:

| **Policy Rule** | **Apply Opportunistic TLS for unspecified recipients** | **Message Containing Recipients**Note **Example domain acquisition.com supports TLS connections, and alpha.com does not.** | **Rule Behavior** |
| --- | --- | --- | --- |
| Traffic Scope: OutboundDomain Scope: contoso.comAction: Force TLSSender domain: acquisition.com | Not selected | c@acquisition.com; d@alpha.com | Message to c@acquisition.com will be transmitted via TLS; message to d@alpha.com will be rejected, since alpha.com does not support TLS connections (or does not have a valid public certificate) |
| Traffic Scope: OutboundDomain Scope: contoso.comAction: Force TLSRecipient domain: acquisition.com | Selected | c@acquisition.com;d@alpha.com | Message to c@acquisition.com will be transmitted via TLS; message to d@alpha.com will be transmitted via SMTP (unencrypted channel) |

To see a chart outlining all the policy rule actions that apply to this match option, see [Policy Rule Settings](#z1ab0f0c58c1a46619f6488fdfa119f4f). For more information about the Basic and RegEx syntax options, see [Policy Rule Syntax](#z1b8c703569504d399d89c48817086112).

## Attachment match options

The Attachment match option gives you the ability to specify e-mail file extensions and names to which the desired policy rule action will apply. If you want to specify multiple file extensions or names for this option and don’t want to enter them manually, use the Dictionary option to upload a list. For details about how to use the Dictionary option, see [Filters](#zb6150b63c0b34f08b10bd4a5438356e0).

| **E-mail part** | **Match for** | **Syntax** | **Additional match option(s)** |
| --- | --- | --- | --- |
| Attachment | File name (and extension) | Basic/RegEx |  Dictionaries Search files in compressed attachments |
| File extension (only) | Basic/RegEx | Dictionaries |
|

Limitations:

 The character limitation for any field is 9,000 characters.

 File extensions are not accepted with periods (.) in the Basic syntax match expressions.

Sample e-mail Attachment rule using Basic syntax:

| **Attachment file extensions: Basic syntax** |
| --- |
| Match expression: | exe, bat, \*gz |
| Interpretation: | All files in e-mail attachments with the extension exe OR bat, OR all files whose extension is ends with gz (e.g. gz OR tar.gz) will be matched. |

Sample e-mail Attachment rule using RegEx syntax:

| **Attachment file name: RegEx syntax** |
| --- |
| Match expression: | test.\*\.tar\.gz |
| Interpretation: | All files in e-mail attachments with the name and extension test.tar,gz OR test123.tar.gz OR testXXXXXX.tar.gz, etc. will be matched.  |

Note

This field can match file name and field extensions.

### Additional match options

Search files in compressed attachments: When you select this option, the Hosted Filtering service scans for specific extensions that may be located in a compressed file that is not password-protected. The service scans the following compressed extensions: amg, arc, arj, ark, b64, bhx, cab, gbz, gz, gzip, ha, jar, lbr, lha, lzh, lzw, pkzip, rar, tar, tgz, uu, z, zip, zlib.

Note

By default, this check box does not apply to password-encrypted files. To permit password-encrypted files to pass through the Hosted Filtering network, you must insert ZIP+ in the Attachment file extensions box. If you do not select this check box, and any file extension that you want filtered by the policy rule is contained in a non-password-protected archive file, the archive file will be scanned for viruses, if your contract includes virus filtering. If no virus is found, the message will not be matched.

To see a chart outlining the various policy rule actions that apply to this match option, see [Policy Rule Settings](#z1ab0f0c58c1a46619f6488fdfa119f4f). For more information about the Basic and RegEx syntax options, see [Policy Rule Syntax](#z1b8c703569504d399d89c48817086112).

## Message Subject and Message Body match options

This match option allows you to match for words, phrases, patterns of letters or numbers in the message subject or message body. If you want to specify multiple words/phrases for this option and don’t want to enter them manually, use the Dictionary option to upload a list. For details about how to use the Dictionary option, see [Filters](#zb6150b63c0b34f08b10bd4a5438356e0).

| **Match for** | **Syntax** | **Additional match option(s)** |
| --- | --- | --- |
| Subject | Basic/RegEx | 1. Dictionaries2. Exact match3. Case sensitive match4. Not match |
| Body | Basic/RegEx | 1. Dictionaries2. Exact match3. Case sensitive match |

Limitations:

 The character limitation for any field is 9,000 characters.

 The Not match exception option is only available for outbound encryption policy actions.

 Outbound Allow rules are not supported for either Message Subject or Message Body.

 Inbound Allow rules are not supported for words or phrases in Message Body.

Sample e-mail Message Subject rule using Basic syntax

| **Message Subject: Basic syntax** |
| --- |
| Match expression: | casino, free, pill\*, vi?gra |
| Interpretation: | All subject lines containing any of the words “casino” OR “free” OR “pill”, “pills”, “pills4free” etc., OR the word “viagra”, “vi@gra”, “vlagra”, etc. will be matched. |

Sample e-mail Message Subject rule using RegEx syntax

| **Message Subject: RegEx syntax** |
| --- |
| Match expression: | ^\d\d\d-\d\d\d\d-\d\d\d$ |
| Interpretation: | This will match 3 digits, a dash, 2 digits, a dash, and 4 digits, which could be a Social Security Number pattern. |

Sample e-mail Body rule using RegEx syntax

| **Message Body: RegEx syntax** |
| --- |
| Match expression: | Starting.\*Satisfaction.\*Guaranteed |
| Interpretation: | This will match “Starting” AND “Satisfaction” AND “Guaranteed” in this exact order within the body of an e-mail. All words needs to be present in an e-mail in order to match. This will match, for example, the following body text: “Watches Starting at $15. Satisfaction Guaranteed” but will not match “Guaranteed Satisfaction, Watches Starting at $15.”Note You can achieve the same effect with the Basic syntax by using the wildcard meta character. |

### Additional match options

1. Case sensitive match: The policy rule engine will perform a case-sensitive match on e-mails based on the match expression specified in a policy rule.

Example: “cAseSensitivE” will not match "CASESENSITIVE" if the Case sensitive match option was selected for this match expression. If Case sensitive match is de-selected, the match expression "cAseSensitivE" will match "CASESENSITIVE".

2. Exact match: The policy filter will match expressions at its boundaries.

Example: “This is a test” will not match “This is a test1234” OR “This is a perfect test” OR “123This is a test”. It will match exactly the phrase specified, but will not treat this expression as case-sensitive. In order to achieve this, both Exact match and Case sensitive match need to be selected.

To see a chart outlining the various policy rule actions that apply to this match option, see [Policy Rule Settings](#z1ab0f0c58c1a46619f6488fdfa119f4f). For more information about the Basic and RegEx syntax options, see [Policy Rule Syntax](#z1b8c703569504d399d89c48817086112).

## Message Properties

Match criteria options for the message properties include the following options:

 Executable content

 Class ID extensions

 Maximum number of recipients

 Maximum size

 Character sets

The Executable content check box blocks any file attachment that contains executable content (e.g. exe), regardless of file name or file type (e.g. if a .com file has renamed to .jpg). The file is analyzed by the virus filtering service to determine whether it is a binary executable type of content or is simply relying on the extension. If this option is selected, no binary executable files of any type will be allowed through the system if those files contain any active content that can be executed.

The Class ID extensions check box is recommended as a virus precaution. The Class ID (CLSID) tag is an extended HTML element that is used to describe the class of a viewable or downloadable document. When used legitimately, it assists the browser in determining which plug-in, active component, or helper application should be used to handle a data object that is accessed over the Web. Attachments with a CLSID extension do not show the actual full extension of the file when they are saved and viewed with Windows Explorer. This characteristic of the CLSID extension allows dangerous file types to look like simple, harmless files (such as JPG or WAV files) that do not need to be blocked. Using the CLSID extension for attachments may also circumvent attachment checking in some e-mail policy filtering solutions that rely only on file name extensions.

The Maximum number of recipients option specifies the maximum number of recipients to which inbound e-mail messages can be sent. This number must be between 2 and 499. Currently, the network-wide recipient limitation for inbound or outbound e-mail is 499 addresses.

The Maximum size option blocks sending and receiving messages over the specified number of megabytes (MB). The current network-wide size limitation on inbound and outbound messages is 150 MB. Therefore, any message that is 150 MB or greater is blocked by default. The overall message size is being managed by the rule, and not just the attachment size. Messages may be larger than expected when received because of encoding or large message bodies. Values should be entered in Kilobinary Bytes (KiB). For example, the setting to block messages larger than 20 MB is entered as 20,480 KiB.

The Character sets option matches character sets other than English. By matching a character set such as Cyrillic, the filter will match any messages sent to your domain that contains Cyrillic characters. If you create a policy rule to block a character set, this will affect all e-mail sent that includes the specified character set, not just spam e-mail. By default, all available character sets are allowed.

# Policy Rule Settings

In the Policy Rule Settings pane, you can set the scope, actions, and parameters to be applied to the specified match expressions for items such as e-mail headers, sender/recipient, or message subject/body.

Policy rule settings include the following:

 Domain Scope, which lets you select the domains to which the policy rules should apply.

 Traffic Scope, which lets you specify whether the rules apply to inbound, outbound, or if the policy rule should be disabled.

 Action, which lets you specify the action that should be applied to the match criteria,, for example header value.

 Policy action related settings:

 Redirect address is an option of the Redirect policy action.

 BCC address is an option of the Deliver with BCC policy action.

 Attachment Download is an option of the Quarantine policy action.

 Message release is an option of the Quarantine policy action.

 Test mode options: Add X-Header and Modify Subject are options of the Test policy action)

 Expiration date, which lets you assign an optional expiration date to any policy rule.

 Description, which lets you add a summary of the rule.

See Policy Filter Actions, Expiration Date, and Description later in this topic for important additional information about these settings.

## Policy Filter Actions

 The following sections describe the options that you can select in the Action area of the Policy Rule Settings pane, both for inbound and outbound policy filters. A rule can perform either inbound policy filter actions or outbound policy filter actions on a message.

### Inbound Policy Filter Actions

Actions for inbound policy rules apply to incoming messages for recipients for a specific domain scope. The table that is shown here describes the options that are available in the Action section of the Policy Rule Settings pane, actions that the Filtering service can take on inbound messages that match any of the expressions or options specified in a policy filtering rule.

| **Action** | **Description** |
| --- | --- |
| Decrypt | Decrypts messages that are replies to encrypted message, which was originally sent from your company using the encryption service. |
| Allow | Ensures that a message will not be blocked as spam or by other policy rules. Messages will still be processed by virus engines and policy decryption filters as applicable. |
| Reject | Rejects all inbound messages that match any of the expressions specified. |
| Quarantine | Moves inbound messages that match any of the expressions specified in the Quarantine. The original recipient will not receive the message. |
| Redirect | Allows inbound messages that match to be redirected to a new e-mail address. The original recipient will not receive the message. If messages are redirected, the new recipient will be able to view the original addressees if they are included in the To line of the message. When you select this action, you are prompted to enter the e-mail address where the message should be redirected. |
| Deliver with Bcc | Allows inbound messages that match to be delivered to the intended recipient, and a blind carbon copy (Bcc) sent to a separate new e-mail address. Any message that uses this Bcc option will add one message to the delivery report. |
| Test | Allows the administrator to test individual policy reject rules. If a policy rule action is set to “Test”, all e-mail messages that are matched by the policy rule will be marked with a non-customizable X-Header or a Subject line. The X-Header option adds the default X-Header that displays X-PolicyTest: This message was filtered by <RuleID>. The subject line option adds [Filter Test: P<Rule ID>] to the beginning of the message subject line. Rule ID is correlated with the policy rule ID that you have created for the Test policy. |

### Outbound Policy Filter Actions

Actions for outbound policy rules apply to outgoing messages from senders for a specific domain scope. The table that is shown here describes the options that are available in the Action section of the Policy Rule Settings pane, actions that the Hosted Filtering service can take on outbound messages that match any of the expressions or options specified in a policy filtering rule.

| **Action** | **Description** |
| --- | --- |
| Reject | Rejects all outbound messages that match the policy rule options. |
| Redirect | Allows outbound messages that match to be redirected to a new e-mail address. The original recipient will not receive the message. If messages are redirected, the new recipient will be able to view the original addressees if they are included in the To line of the message. When you select this action, you are prompted to enter the e-mail address where the message should be redirected. |
| Deliver | Allows outbound messages that match to be delivered to the intended recipient, with a Bcc sent to a separate new e-mail address. Any message that uses this Bcc option will add one message to the delivery report. Note In the Administration Center, you can create detailed Bcc policy rules. When using the Bcc action for outbound policy rules, you can specify originating IP addresses, sender domains, and sender e-mail addresses as options. |
| Encrypt | Encrypts messages upon sending. Rules can be set to encrypt outbound mail based on subject keywords, message keywords, or common expressions in addition to sender IP address, sender and recipient domain, or e-mail address. |
| Force TLS | Enforces transport layer security (TLS) between your outbound mail transfer agent (MTA) and your recipient’s MTA. When you configure this Policy Rule, the Force TLS restrictions are applied to matching outgoing e-mails and are enforced across your whole domain. |

Important

If the recipient server certificate is expired, self-signed, or not valid, the TLS connection will not be established and the message will be deferred.

If a TLS connection cannot be established between your outbound services and the recipient’s messaging environment, the message will be deferred for 24 hours. If message delivery fails, a bounce message will be sent to the sender. In order to receive the bounce message, your server must have a valid, known certificate.

If the Enable Opportunistic TLS for unspecified recipients box is unchecked, then outbound messages will be bifurcated. This means that authenticated Transport Layer Security (TLS) will be enforced for the delivery of all recipients on the message, where any of the recipients match the Policy Filter rule and the recipient mail transfer agent (MTA) is configured to accepting TLS-based connections (including valid public certificates). If one of the recipients has an MTA that does not supporting TLS connections, then the message to this recipient will be rejected. Checking this box will still enforce authenticated TLS on the recipient who matches the rule, but also allows all other recipients to be transmitted using Opportunistic TLS if all attempts to enforce TLS fail. The Forefront Online Protection for Exchange service will always use the highest level of encryption available for transmission of the messages and if not available step down.

# Policy Rule Syntax

When creating policy rules, you have two options for the syntax of the rule. First, you can use comma-separated values (CSV) mixed with the string-wildcard syntax, which is listed as Basic in the Administration Center Policy Rules editor. Second, you can use a subset of characters specified in the Regular Expression syntax, which is listed as RegEx in the Administration Center Policy Rules editor, for more complex rules.

If you are not familiar with RegEx syntax, you can select the Basic option, which will allow you to create simple expressions for content filtering and help you write correct matching expressions format by evaluating your match expressions based on the context they are defined within. For example, only correct IP addresses will be accepted in the IP address field. If the rules you wish to create require more complexity, such as matching patterns of numbers and patterns of words, you can use a subset of RegEx syntax characters by selecting the RegEx option. With this option, context-based validations are not available; only syntax-specific validations will apply.

## Basic syntax

When you select Basic in the Policy Rules editor, you will be able to list expressions using a CSV syntax separating the match expressions with commas. Additionally, you will be able to enhance match expressions with simple string-wildcard metacharacters. The same syntax applies to dictionary files uploaded through Filters.

### Definition of basic syntax

| **Metacharacter** | **Description** | **Example** |
| --- | --- | --- |
| , | A comma is the choice metacharacter, also known as an alternation or a separator, and it matches the expression listed either before or after the comma. | abc, def, xyz matches abc or def or xyz |
| \* | An asterisk is the wildcard metacharacter and it represents zero or more characters.Note This character is equivalent to the (.\*) in the RegEx syntax. | ab\* matches aba or abaa or abaaa or ab12345667, etc. |
| ? | The question mark represents any single character.Note This character is equivalent to the (.) in the RegEx syntax. | ab? matches aba or abb or abc or ab1 or ab2, etc. |
| \ | A backslash is the escape operator. In order to match the literals (,) (\*) (?) or (\) and to suppress their special meaning in the basic syntax, the escape operator needs to be placed in front of the basic syntax operators. Note This character is equivalent to the (\) in the RegEx syntax. | \\*a\\bc\? matches \*a\bc? |
| /0 up to /23 | A slash mark indicates Classless Inter-Domain Routing (CIDR) notation. This can be expressed by adding a slash mark (/) followed by a number from 0 up to 23 after the last octet of an IP address. Note CIDR notation applies only to IP address expressions and cannot be used in other contexts. | 99.99.98.0/23 matches IP ranges from 99.99.98.0 up to 99.99.99.255 |

Note

The total number of characters inserted into any Policy Rule field or dictionary cannot exceed 9,000. Dictionary file size limit is 2 MB.

## RegEx syntax

When you select RegEx in the Policy Rules editor, you can specify more complex expressions that match patterns of text, numbers, or special characters. For example, you can match many different variations of a word such as viagra, vi@gra, vlagra using a subset of RegEx characters. This will allow you to minimize the number of rules needed and to create powerful matching expressions, such as scanning for credit card numbers, social security numbers, e-mail addresses, and similar strings of sensitive words or numbers.

### Definition of RegEx syntax

The RegEx option in the Policy Rules editor is a subset of the POSIX Basic and Extended Regular Expressions syntax, expressed in the following table.

| **Character type** | **Character** | **Description** | **Example** |
| --- | --- | --- | --- |
| Meta | ^ | The caret metacharacter matches the starting position within the string.Note Used in combination with the dollar sign character, the caret has the same functionality as the exact match option. | ^abc matches abc1234, but will not match 1234abc |
| Meta | $ | The dollar sign metacharacter matches the ending position of the string, or the position just before a string-ending newline.Note In combination with the caret character, the dollar sign offers the same functionality as the exact match option. | abc$ matches 1234abc, but will not match abc1234 |
| Meta | \* | The star matches the preceding element zero or more times.Important This character should be used with caution; match expressions using this character might match more than intended. | ab\*x matches abx or abbx or abbbx or abbbbx, etc. |
| Meta | + | The plus metacharacter matches the preceding element one or more times.This character should be used with caution; match expressions using this character might match more than intended. | ab+x matches abbx or abbbx or abbbbx or abbbbbx, etc. |
| Meta | . | The period metacharacter matches any single character except new line. | ab.x matches ab1x or ab2x or ab3x or ab4x, etc. |
| Meta | ? | The question mark matches the preceding element zero or one times. | ab? matches a or ab |
| Meta | | | The pipe is a choice, or alternation, character, which matches the expression either before or after the operator, starting from the first (left) string and stopping when a match is found. | abc|def|xyz matches abc or def or xyz or abc12345, but will not match a123c or axm |
| Meta | \ | The backslash causes RegEx metacharacters to be treated as literal characters in the context of the rule. | x\\*1\.5\+9\\x=y matches x\*1.5+9\x=y |
| Class | \w | The backslash with lowercase w matches any word character, including alphanumeric characters with "\_". | \w123 matches a123 or bbb123 or c\_c123xxx, but will not match @123 |
| Class | \d | The backslash with lowercase d matches any decimal digit. | \dabc matches 123abc or 12345abcxxx or 1abc1, but will not match abc123 or @abc123 |
| Class | \s | The backslash with lowercase s matches any white-space character.  | abc\sdef matches abc def |

Important

If you are unfamiliar with RegEx syntax, we recommend that you use the Basic option or test rules by using the Test policy rule action before using them with policy rule actions such as Reject, Encrypt, Redirect. The Administration Center Policy Rules support only a subset of RegEx characters.

The total number of RegEx characters inserted into any Policy Rule field cannot exceed 9,000.

### More examples for creating match expressions with RegEx

The following are examples of RegEx expressions matching different parts of a message:

 A period used to match file extensions will match any single character after your expression. For example, r. would match any file name that begins with the letter r and any single character following it. For example, the match expression r. would match extensions such as r1 or another two-character combination.

 In order to be matched as literal, all RegEx metacharacters need to be accompanied by the escape operator. Non-RegEx metacharacters are matched literally and do not need to have the escape operator added. If you want to match the period in a domain name, this period needs to have the escape character added by listing \.. The match expression contoso\.com will match contoso.com.

 For Domain options, the domain matching acts on the presence of the sender or recipient domain in an e-mail header. For example, a rule to take action on contoso.com will also affect messages for the sub domain 123.contoso.com. If you want to match only the domain name without any subdomains, then you can configure the rule by using the carat metacharacter ^contoso.com. The rule configured in this manner would match only e-mails sent to or received from contoso.com and not 123.contoso.com.

 If you want to search for terms, for example, in the subject, body, or attachment file name of an e-mail that ended with the string “ness”, combine the asterisk and the period to perform your match. For example, the search term .\*ness will return results such as “wilderness” or “happiness”.

 A period . followed by an asterisk \* represent zero or more characters. For example, the match expression contoso\..\* would match “contoso.com” but would also match “contoso.microsoft.com” or “contoso.mydomain.ca”, etc. In order to match only the Top Level Domain (TLD) of a domain, a more precise match expression is required. contoso\.\w\w\w$ will match “contoso.com” or “contoso.org” or “contoso.tv1”, but will not match any domains with more or less than 3 alphanumeric characters after the period.

### About Regular Expressions

Regular expressions, abbreviated as RegEx, are a standard formal language used in many systems and programming languages. Regular expressions can be powerful if used in a proper way. You can find more information, including syntax definition, examples, and tutorials, on many Web sites, such as the following:

MSDN [Introduction to Regular Expressions](http://go.microsoft.com/fwlink/?LinkId=168417) (http://go.microsoft.com/fwlink/?LinkId=168417)

[The Regular Expressions.Info Web site](http://go.microsoft.com/fwlink/?LinkID=168418) (http://go.microsoft.com/fwlink/?LinkID=168418)

[The Regular Expression Library Web site](http://go.microsoft.com/fwlink/?LinkId=168419)

# Create, Edit, or Delete a Policy Rule

In the Policy Rule tab, which is in the Administration tab you can create, edit, and delete custom policy rules for your domains and your service. For more information about policy rule options, see [Policy Rules](#zd43d92b98b8c43a3869b6bb4ca4e0682).

How to create a new policy rule

|  |
| --- |
| 1. On the Administration tab, click the Policy Rule tab.2. In the Tasks pane, click New Policy Rule.3. Select the options you want to use for your policy rule. See [Policy Rule Settings](#z1ab0f0c58c1a46619f6488fdfa119f4f) for a complete description of all options and parameters.4. Select the syntax type (Basic or RegEx) that you want to use. For more information about the syntax types, see [Policy Rule Syntax](#z1b8c703569504d399d89c48817086112). 5. In the appropriate text fields, such as Message Body, for the desired match criteria, such as e-mail part, use the appropriate syntax characters to enter the values for which you want to scan. To add values using the Dictionary option, see [Filters](#zb6150b63c0b34f08b10bd4a5438356e0).6. In the Actions pane, click Save Policy Rule. The following is a view of the New Policy Rule dialog box. |

How to edit a policy rule

|  |
| --- |
| 1. On the Administration tab, click the Policy Rule tab.2. In the All Policy Rules pane, click the rule ID of the policy rule you want to modify. The management information for that policy rule appears in the Policy Rule tab.3. Modify the options and parameters as needed.4. In the Actions pane, click Save Policy Rule.  |

How to delete a policy rule

|  |
| --- |
| 1. On the Administration tab, click the Policy Rule tab.2. In the All Policy Rules pane, click the rule ID of the policy rule you want to modify. The management information for that policy rule appears in the Policy Rule tab.3. In the Actions pane, click Delete Policy Rule. |

# Set Compliance Policy Rules

The Hosted Archive supports two special configuration settings:

1. Exclude Attorney Client Conversations This policy rule excludes attorney-client privileged messages from review, thus protecting the confidentiality of the conversation. This exclusion can be applied at the individual user or domain level and the exclusion can be permanent or set to expire on a specified date. Multiple instances of this policy rule can be set simultaneously if you have several business requirements.

2. Implicitly Review This policy rule allows messages that are sent to or from specific e-mail addresses or domains, or messages that contain specific words in subjects to always be marked as implicitly reviewed. Multiple instances of this policy rule can be set simultaneously if you have several business requirements.

How to add Exclude Attorney Client Conversations rule

|  |
| --- |
| 1. On the Administration tab, click the Policy Rules tab.2. In the General pane, select Exclude Attorney Client Conversations from the Action area.3. Set a specific date in the Expiration date box if the rule is temporary. Otherwise, keep the box blank to make the rule permanent.4. In the New Compliance Policy Rules pane, do one of the following: If you want to protect message to or from a specific e-mail address, select E-mail, and then enter the e-mail address. If you want to protect messages to or from a specific domain, select Domain, and then enter the domain name.5. Click Save Policy Rule. |

How to add Implicitly Review rule

|  |
| --- |
| 1. On the Administration tab, click the Policy Rules tab.2. In the General pane, select Implicitly review from the Action box.3. In the New Compliance Policy Rules pane, do one of the following: If you want to apply the policy to messages to or from a specific e-mail address, select E-mail, and then enter the e-mail address. If you want to apply the policy to or from a specific domain, select Domain, and then enter the domain name. If you want to apply the policy to messages containing specific words in the subject, select Subject, and then enter the desired words.4. Click Save Policy Rule. |

# Policy Rule Processing

The following table shows the available combinations of policy rule actions.

| **Policy Action** | **Inbound** | **Outbound** |
| --- | --- | --- |
| Reject | Action/combination available | Action/combination available |
| Allow | Action/combination available | Not available because of the potential for SPAM override |
| Quarantine | Action/combination available | Not available |
| Redirect | Action/combination available | Action/combination available |
| Deliver with Bcc | Action/combination available | Action/combination available |
| Force TLS | Not available | Action/combination available |
| Test | Action/combination available | Not available |
| Encrypt | Not available | Action/combination available |
| Decrypt | Action/combination available | Not available |

As a general guideline, the most permissive policy rule should be the one that takes action on the messages being processed through the Policy Filter. If a message matches both an inbound policy rule and an outbound policy rule, then the outbound policy rule takes precedence. For every policy rule with the same Action and Domain Scope, the policy rule that was created first will be applied first. So, if multiple policy rules could be applied to the message (equal rule settings), the rule with the lowest Rule ID (the one created first) will be processed first.

For inbound policy rules, the general expectation for processing should follow this formula:

1. Company-Wide Decrypt

2. Company-Wide Inbound Allow

3. Company-Wide Inbound Reject

4. Company-Wide Inbound Quarantine

5. Company-Wide Inbound Redirect

6. Company-Wide Inbound Bcc

7. Domain Wide Decrypt

8. Domain Wide Inbound Allow

9. Domain Wide Inbound Reject

10. Domain Wide Inbound Quarantine

11. Domain Wide Inbound Redirect

12. Domain Wide Inbound Bcc

For outbound policy rules, the general expectation for processing should follow this formula:

1. Company-Wide Outbound Reject

2. Company-Wide Outbound Redirect

3. Company-Wide Outbound Bcc

4. Company-Wide Outbound Encrypt

5. Company-Wide Outbound ForceTLS

6. Domain Wide Inbound Reject

7. Domain Wide Inbound Redirect

8. Domain Wide Inbound Bcc

9. Domain Wide Inbound Encrypt

10. Domain Wide Inbound ForceTLS

The table in this section provides more details about how policy rules are processed. In the table, the following three options indicate the status of each rule:

 Skip indicates that the rule will not been processed.

 Match indicates that the rule action will be applied to policy rule.

 Check indicates that the rule will be processed and applied if it matches.

Outbound only

| Outbound only |
| --- |
| Reject | Match | No match | No match | No match | No match | No match |
| Redirect | Skip | Match | No match | No match | No match | No match |
| Deliver w/BCC | Skip | Skip | Match | No match | No match | No match |
| Encrypt | Skip | Skip | Check | Match | No match  | No match |
| TLS | Skip | Skip | Check | Skip | Match | No match |

Inbound only

| **Inbound only** |
| --- |
| Decrypt | Match | No match | No match | No match | No match | No match |
| Allow | Skip | Match | No match | No match | No match | No match |
| Reject | Skip | Skip | Match | No match | No match | No match |
| Quarantine | Skip | Skip | Skip | Match | No match | No match |
| Redirect | Skip | Skip | Skip | Skip | Skip | Match |
| Bcc | Skip | Skip | Skip | Skip | Skip | Match |

Outbound + Inbound

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Outbound Reject | Match | No match | No match | No match | No match | No match | No match | No match | No match | No match | No match |
| Outbound Redirect | Skip | Match | No match | No match | No match | No match | No match | No match | No match | No match | No match |
| Outbound Bcc | Skip | Skip | Match | No match | No match | No match | No match | No match | No match | No match | No match |
| Outbound Encrypt | Skip | Skip | Check | Match | No match | No match | No match | No match | No match | No match | No match |
| Outbound TLS | Skip | Skip | Check | Can’t Match | Match | No match | No match | No match | No match | No match | No match |
| Inbound Decrypt | Skip | Skip | Check | Check | Can’t match | Can’t match | No match | No match | No match | No match | No match |
| Inbound Allow | Skip | Check | Check | Check | Check | Skip | Match | No match | No match | No match | No match |
| Inbound Reject | Skip | Check | Check | Check | Check | Skip | Skip | Match | No match | No match | No match |
| Inbound Quarantine | Skip | Check | Check | Check | Check | Skip | Skip | Skip | Match | No match | No match |
| Inbound Redirect | Skip | Check | Check | Check | Check | Skip | Skip | Skip | Skip | Match | No match |
| Inbound Bcc | Skip | Check | Check | Check | Check | Skip | Skip | Skip | Skip | Skip | Match |

## Additional Policy Rule settings

### Expiration Date

You can assign an optional expiration date to any custom policy rule. If no date is assigned, the rule is in force until it is deleted. When a rule expires, it is no longer active, but will still appear on the policy rules list.

### Description

A description field is available for each rule and is displayed with the rule in the Policy Rule Settings pane. The maximum length of the comment is 128 characters. Comments are helpful when there are multiple administrators creating rules, or when rules are created in response to a specific issue.

### Notifications

In the Notifications pane, you can set notification messages that will be sent by the system if a message violates a policy rule. Notification messages can be sent to the intended recipient, as well as to the sender of the message and the administrator. When you enable this option, a default message will be sent; you can customize the subject line and message body of this message on a per-rule basis.

The following examples describe sample notifications for the policy reject rules.

Policy Rule Reject Notification to Message Sender
From: Policy Filter <> OR <CUSTOM DISPLAY NAME> <CUSTOM FROM ADDRESS>
 Sent: <DATE>
 To: <SENDER>
 Subject: Undeliverable message returned to sender OR <CUSTOM SUBJECT>
 This message was created automatically by mail delivery software.
 Message violated a policy rule set up by the domain administrator OR <CUSTOM MESSAGE BODY>
 Delivery failed for the following recipient(s):
 <RECIPIENT>
 ----- Original Message Header -----
 <FULL INTERNET HEADERS OF THE MESSAGE>

Policy Rule Reject Notification to Message Recipient
From: Policy Filter <> OR <CUSTOM DISPLAY NAME> <CUSTOM FROM ADDRESS>
 Sent: <DATE>
 To: <RECIPIENT>
 Subject: [NOTIFICATION] message rejected due to policy rule OR <CUSTOM SUBJECT>
 This message was created automatically by mail delivery software.
 A message sent to you by <SENDER> was rejected because:
 Message violated a policy rule set up by the domain administrator OR <CUSTOM MESSAGE BODY>
 ----- Original Message Header -----
 <FULL INTERNET HEADERS OF THE MESSAGE>

Policy Rule Reject Administrator Copy Notification
 From: Policy Filter <> OR <CUSTOM DISPLAY NAME> <CUSTOM FROM ADDRESS>
 Sent: <DATE>
 To: <ADMINISTRATOR>
 Subject: [NOTIFICATION] Policy Rule Matched OR <CUSTOM SUBJECT>
 This message was created automatically by mail delivery software.
 The following rule was matched:
 Rule ID: <RULE ID>

Inbound Reject Rule
 File Attachment Extensions:
 <ALL EXTENSIONS LISTED AS CONFIGURED IN THE RULE>
 File Attachment Extensions/File Names Examine Archive:
 ON
 ----- Original Message Header -----
 <FULL INTERNET HEADERS OF THE MESSAGE>

# Filters

The Filters repository lets you add and manage large lists of values for multiple policy rules. This includes the following:

 Upload large lists. Called Dictionaries, these lists can contain IP addresses, domains, e-mail addresses, keywords, and file names and extensions that you want to quickly use in various policy rules. Utilizing these lists can be faster than manually entering hundreds of keywords or e-mail addresses in the policy rule editor.

 Download dictionaries. Dictionaries can be downloaded from within the Filters tab by clicking the dictionary name.

 Replace dictionaries. Any dictionary can be replaced, even if it is currently associated with a policy rule. In this case, all policy rules using the dictionary that is replaced will be updated with the new values.

 Delete dictionaries. Dictionaries can be used in multiple policy rules. Therefore, deleting them from the Filters repository would cause a change of behavior in the associated policy rules and a potentially undesirable impact on the message flow. Therefore, dictionaries that are currently associated with any policy rule cannot be deleted from the Filters repository (see the Usage column on the Filters tab). To safely delete dictionaries, browse all policy rules using the dictionaries by navigating to the specific policy rules via the link on the Usage column, and unlink the dictionaries from the appropriate policy rules. Only then can the dictionaries be deleted from the Filters tab.

 Audit dictionary actions. Any time a dictionary is added, deleted, or moved, a record of the action will be saved in the Audit Trail. This will ensure that any outcomes associated with adding, deleting, or moving a dictionary can be tracked to the root cause.

Note

The maximum permissible file size for dictionaries is 2 MB and each file can support 9,000 characters. Additionally, dictionary files support only Basic syntax. For more information about the supported syntax, see Basic Syntax in [Policy Rule Syntax](#z1b8c703569504d399d89c48817086112).

How to import a dictionary

|  |
| --- |
| 1. From the Administration tab, click the Filters tab.2. In the Tasks pane, click Import Dictionary.3. In the Import Dictionary box, select Browse.4. Find and select the file and then click Open.5. If desired, change the name of the dictionary file in the Dictionary name: field; otherwise, whatever name you gave the file when you saved it to your own files will be used in this dialog box and once the dictionary has been uploaded.6. Select the appropriate type of content that your dictionary contains, for example domain names or e-mail addresses, from the Dictionary contents menu. 7. If desired, add any comments about the dictionary in the Comments field. 8. Select Import.  |

How to replace a dictionary

|  |
| --- |
| 1. From the Administration tab, select the Filters tab.2. In the Tasks pane, select Import Dictionary.3. In the Import Dictionary box, click Browse.4. Find and select the file and then click Open.5. Change the name of the dictionary file in the Dictionary name: field to match the file name of the dictionary you want to replace.6. Select the check box Replace Dictionary if exists.7. Select the appropriate type of content that your dictionary contains; for example, domain names or e-mail addresses from the Dictionary contents menu. This content type needs to match the content of the dictionary you want to replace.8. If desired, add any comments about the dictionary in the Comments field. 9. Select Import.  |

How to add a dictionary to a rule

|  |
| --- |
| 1. Select the Policy Rules tab.2. Select the rule you want to apply the dictionary to by clicking the appropriate rule ID, or create a new rule.3. Expand the policy editor fields for the appropriate message component, for example Body, by selecting the down-arrow icon next to the component title. 4. Select your uploaded dictionary from the Dictionary combo box.Note You can either have a match expression in the textbox, or select Dictionary. If you select Dictionary, the textbox will be de-activated, and any match expressions entered in this textbox will be deleted upon saving of the policy rule. 5. Add additional settings to the policy rule and click Save.  |

How to delete a dictionary

|  |
| --- |
| 1. Select the Filters tab.2. Select the dictionary you want to delete by clicking the checkbox next to the name of the appropriate dictionary. Important If the dictionary you wish to delete is currently in use by any policy rules, browse all policy rules associated with this dictionary by navigating to the specific policy rule by selecting Usage within the Filters tab, and unlink the dictionary from these policy rules. Then you can return to the Filters tab and delete the dictionary.3. Select the appropriate dictionary and click Delete.  |

How to audit a dictionary-related action

|  |
| --- |
| 1. Select the Tools tab.2. Select the Audit Trail tab.3. Browse the Audit Trail for the PatternFiles events. Information related to the creation, replacement, and deletion of dictionaries is recorded here.  |

# My Reports Tab

From the My Reports tab, you can access reporting data within an hour of a message being processed by the Forefront Forefront Online Protection for Exchange (FOPE) Filtering service. You can view reports on all domains, or on specific domains, using a variety of options to filter the information.
Reports provide customers with access to historical message filtering summaries. This reporting data is made available to customers for informational purposes only. It is not a representation of all the data that is stored by the Hosted Filtering service.

# About Reports

The My Reports tab of the Administration Center provides customers with access to reports that contain historical message filtering summaries. This reporting data is made available to customers for informational purposes only. It is not a representation of all the data that is stored by the Microsoft Forefront Online Protection for Exchange service.

# Reports Overview

The report is separated into two sections: E-mail Traffic Count and E-mail Traffic Volume. Each section displays a summary of the returned results, which are categorized into percentages, a pie graph, and a line graph. Some of the values in the report show information in greater detail as well. To view the hourly summary from the daily summary, expand each entry to see more details. Details for a specific traffic type are available from the E-mail Traffic Count section only.
Also, you can modify a report from the My Reports tab after the report has been run. From here you can make quick changes to your report settings based on the information you receive from the report.

# Saved Reports

When you save a report, all of the settings that you have configured for that report are saved so that you can view or modify saved reports in the future without needing to specify the domains or traffic types. The date specified is also saved and can be modified when you return to the report.
You can save multiple reports and reuse them the next time you log on to the Administration Center. Saved reports are specific to your account. Each Administration Center logon account has its own set of saved reports. You can reach saved reports from the My Reports tab, where you can view updated data, modify the report settings, or delete a report.

# Scheduled Report Delivery

Reports can be scheduled for e-mail delivery. In order to configure the e-mail delivery settings check Enable scheduled report delivery on the report settings page.
 The e-mail message will be sent with the From: address of support@messaging.microsoft.com. The e-mail message can be configured with a custom E-mail subject and Reply-To: address. If a custom Reply-To: address is used, it must be an address from a domain that belongs to the company that the logged-on user belongs to. The reports can be sent in either Excel or PDF format, and can be scheduled for One-time only, Weekly, or Monthly delivery.
A maximum of 20 scheduled reports can be configured for any single company.

# Create, Modify, or Delete a Report

On the My Reports tab, you can view saved reports or create new reports for your service. After you have saved a report, you can modify its settings when you need to change the type of information that the report should return. You can delete the report if it is no longer being used.

How to create a new report

|  |
| --- |
| 1. On the My Reports tab, in the Tasks pane, click New Report. The New Report pane appears.2. In the New Report pane, under Report Name, type a unique name for the report you want to create. You can later search for this report by the report name.3. Under Report Type, select the type of report you want to create: E-mail Traffic Report: Returns the number and volume of messages for each traffic type that you select. The available traffic types are: Inbound delivery: Legitimate messages that are delivered to this organization or domain. Reports that include this traffic type do not include messages that are allowed by policy filter rules. Spam: Inbound messages that are filtered as spam. This traffic type also includes the requests that are sent to the e-mail abuse and false-positive submission e-mail aliases, and, if applicable, any salvaged messages that are requested from the Spam Quarantine or Spam Notification e-mail messages. Inbound virus: Inbound mail and virus-infected file attachments that are scanned, as well as viruses that are blocked and cleaned. Inbound policy filter: Inbound messages that are filtered by the policy filter. (The report breaks down these messages into each different filter type.) Outbound delivery: All messages that are sent from this organization or domain. This traffic type includes successfully sent outbound messages and outbound messages that are blocked due to a policy filter. Outbound virus: Outbound mail and virus-infected file attachments that are scanned, as well as viruses that are blocked and cleaned. Outbound policy filtering: Outbound messages that are filtered by policy filter. (The report breaks down these messages into each different filter type.) Top Viruses Report: Returns a list of the top 10 viruses that have been caught by the virus filters for your domain or set of domains. Deferral Report: Returns a list of messages that have been deferred by the service. It includes the message and the reason for deferral. Top Users: Returns a list of the top 10 users of the service.Note This report displays only users that belong to domains that have Directory-Based Edge Blocking enabled. Doing this helps decrease the number of invalid user accounts from being recorded in this report.4. Under Report Scope, do one of the following: To gather data for all domains in your company, enter your company name in the Company name box. To run the report for only a subset of domains, select the Run report on selected domains check box, click Sync to retrieve a list of domains, and then select the domains that you want to include in the report.5. Under Report Date Range, select the date range and time zone setting that you want the service to use when creating the report.Note The date range feature has several constraints. Predefined date ranges are relative to the current date. When you specify a date range for a traffic summary report, it cannot exceed 62 days. Top reports are limited to a seven-day range. Data for messages that are processed through Microsoft Forefront Online Protection for Exchange. Filtering is available for 24 months.6. In the Actions pane, do one of the following: To add the report to your Saved Reports pane, click Save Report. To generate the report, click View Report. Generating the report will not automatically save the report to your Saved Reports pane.  |

How to modify a saved report

|  |
| --- |
| 1. On the My Reports tab, in the Saved Reports pane, open the report that you want to modify.2. Click Edit. The report’s management information appears in the My Reports tab.3. Modify the report settings as needed.4. In the Actions pane, click Save Report. |

How to delete a saved report

|  |
| --- |
| 1. On the My Reports tab, in the Saved Reports pane, open the report that you want to modify.2. Click Delete. |

# View and Export Results for Saved Reports

For all saved reports, you can view updated report information from the Saved Reports pane on the My Reports tab. You can also export the report data to a separate file, such as a Microsoft Office Excel spreadsheet or a PDF file.

Important

Reports are exported in English only, even if the Administration Center pages have been translated into your local language.

How to view data from saved report

|  |
| --- |
| 1. On the My Reports tab, click the name of the report that you want to view. The report appears in a new browser window. |

To export report data

|  |
| --- |
| 1. On the My Reports tab, click the name of the report from which you want to export data. The report appears in a new browser window.2. On the navigation toolbar above the report, in the Select a format list, click the output format for your report results.Note Some common supported export formats include XLS, CSV, MHTML (Web archive), TIF, and PDF.3. Click Export. The report is generated in the format you selected.4. When prompted, open the file or save it a new location. |

# Run Archive Report

As a compliance manager, technical administrator, or supervisor, you can run archive reports from the Administration Center. You can run a report immediately, or schedule reports to be run at regular intervals and delivered to you and other administrators.

You can view a report as a Web page, as a PDF file (requires Adobe Acrobat 5.0 or later with inline PDF viewing enabled), or as a Microsoft Excel (XLS) file.

To run an archive report

|  |
| --- |
| 1. In the Administration Center, on the My Reports tab, in the Tasks pane, click Run Archive Report. 2. On the Report List page, click the type of archive report you want to run.3. On the Report Execution page, set the report criteria.4. Select an output format for the report, and then do one of the following:a. To run a report immediately, click Run.b. To run regular reports, click Subscribe. In the Send box, type the e-mail addresses to send the reports to, choose the interval, and then click Apply. |

Tip

To change your archive report subscriptions, on the Report List page, click Subscriptions in the upper right.

The following sections describe the available archive reports.

### Activity Summary Report

The Activity Summary report provides an overview of how many internal and external messages were sent and received for e-mail, instant messages, and other files and documents. This report also provides the overall and average size for each category of messages. The report counts real messages and removes embedded messages.

### Archive Summary Report

The Archive Summary report displays archive statistics for the organization. Statistics are included for e-mail messages, instant messages, and other files and documents that include Bloomberg reports, faxes, and uploaded documents.

Statistical breakdowns include count, basic size, size of attachments, total size, and average size. Totals are given for all data categories.

### Attachment Summary Report

The Attachment Summary report presents the data in a table and in a three-dimensional column chart, showing top attachment types found in the archived message traffic. Data includes file extension, document type, quantity, total size, and average size.

### Audit Events Report

The Audit Events report gives details of all the user-related granular actions which they have performed. These activities include viewing e-mail messages, export/restore messages, log in/log out of users. This report can provide overall and for each category individually.

### Daily Statistics Report

The Daily Statistics report shows the daily statistics for all messages (e-mail, instant messages, and other files and documents) archived for a particular day. Totals and size are given for all data columns.

### Destruction Report

The Destruction report validates and lists messages that have been destroyed because of the retention period expiration date. Details about each individual message include Date Destroyed, Date Sent/Received, Age When Destroyed, From, To, and Subject.

Messages older than their retention period are destroyed in all data centers (production and disaster recovery) once a day starting at 6:00 P.M. PST. If a message is on destruction hold, the message will not be destroyed.

Any e-mail message, instant message, Bloomberg transcript, or uploaded document is destroyed when the retention period expires. The header information of a message is kept, but bodies of messages or attachments are destroyed.

### Email Summary Report

This report generates a summary for all users or individuals. Statistics include summaries of internal and external messages sent and received, size, and average size, along with totals.

### Employee Roster Report

The Employee Roster report displays a complete list of users who have archive accounts, as well as what roles they have been assigned, who is their supervisor, dates of their last logon, an individual’s retention period settings, last sent messages, and last received messages. Totals are included for all data columns, as well as a breakdown of totals by assigned roles.

### Privileged Roles Report

The Privileged Roles report includes a category for each role with privileges — Compliance Manager, Compliance Operator, External Compliance Auditor, HR Manager, Monitor, Monitor Operator, Role Manager, Supervisor, Technical Administrator, and Technical Operator. In each category, the users with that role are listed, as well as the date the role was assigned to them. Totals are given for each category.

### SEC 17a-4 Report

The SEC 17 a-4 report demonstrates evidence of complete, serialized, and archived e-mail for your organization. It identifies the first message archived and the most recent message archived, as well as Date, Time, To, From, Subject, and the Message ID number for serialization.

This report also includes the number of messages captured, messages certifiably destroyed, messages on destruction hold, and voided message IDs. In the event that an ID number is not issued sequentially, it will not be used at all (these are voided IDs).

### Supervisory Review Evidentiary Report

The Supervisory Review Evidentiary report is useful for audits. It not only provides compliance managers with the numbers and percentages of communications being reviewed for NASD 3010 compliance, but also provides the same metrics for those subordinates who are having mail reviewed for general purposes.

Tip

To select all supervisors, leave the Supervisor box blank.

When choosing who to include in the report, you can choose one or both of these options: Include Individuals requiring NASD 3010 review and Include individuals requiring review. If you only select the Include Individuals requiring NASD 3010 review option, the report title is a NASD 3010 Evidentiary Report. With any other combination, the report title is Supervisory Review Evidentiary Report. When you select the both options, names that are being reviewed for NASD 3010 compliance are displayed in bold red type.

If you are a compliance manager, you can run this report on a regular basis to make sure that individuals in the Supervisor role are performing their supervisory duties. The report is broken down by supervisor and shows how many messages have been captured and reviewed for each subordinate, as well as the last time the supervisor performed regular message sampling (in the Last Sampling field).

### System Statistics Report

The System Statistics report provides a view of the complete system for the date range that you specify. Statistics cover the number of mailboxes, recipients, senders, volume, and archive statistics. Data breakdown includes quantity, size, average size, and totals for all data categories.

# Tools Tab

From the Tools tab, Administrators can trace messages and view service events by using the Audit Trail feature. The Tools tab includes two tabs:

1. Message Trace—Run message traces from this tab as you did in previous versions of the Administration Center.

2. Audit Trail—The Audit Trail feature helps you track important events that have occurred in your service. From the Audit Trail tab, you can view user- and service-related events. Events can be sorted by e-mail address, company, domain, activity, or date and time.

# Run a Message Trace

The Message Trace feature of the Administration Center enables you to search for a specific message using basic information, such as the sender, recipient, date, and message ID, to obtain the status of that message. E-mail status information helps you see if and when a message was received by the Forefront Online Protection for Exchange filtering service; whether it was scanned, blocked, or deleted; or whether it was delivered successfully within the last month. To begin searching for specific messages in the Administration Center, use the Message Trace tab on the Tools tab to define your search criteria.

How to run a message trace

|  |
| --- |
| 1. On the Tools tab, click the Message Trace tab.2. On the Message Trace pane, under Search Parameters, enter the sender and recipient address information. Important Both sender and recipient e-mail addresses are required when you perform a message trace, and at least one of the search boxes must contain a complete e-mail address, such as recipient@contoso.com. If you want to broaden your search, you may add either a full e-mail address or just a domain name, such as @nwtraders.com, in the other search box. 3. In the Start date and End date boxes, select a date range for your message trace. The default date range is set to 48 hours prior to the current date and time. The maximum date range for a single search is 30 days.4. In the Time zone list, click the time zone that should be used when processing your message trace.5. In the Message ID box, type the message ID of the message that you want to trace. The message ID is a unique ID that is generated by a sending e-mail server. This information is optional when you run a message trace.6. Click Search. A Results pane appears below the Message Trace pane, displaying the message count and list of messages that match the search criteria that you entered in the Message Trace pane.7. To have fewer messages returned from the search, click Refine Search and redefine the search criteria.8. To view more detailed information about a specific e-mail message, click Details. A new browser window will open showing the Message Trace Summary for that message.  |

# Message Trace Tool Known Limitations

There are some known limitations of the Message Trace tool. Improvements to the tool are ongoing.

## Voltage Encryption:

Mail that goes through the Voltage Encryption Gateway ceases to be traceable once it moves to the Encryption systems. The Filtering Result will show "Delivered to Encryption Gateway" but is unable to trace the message beyond that point. Similarly, messages that are to be decrypted will show "Delivered to Decryption Gateway" for the filtering results, but delivery to the destination server is not traceable at this time.

## IP Edge Blocks:

Messages blocked by reputation block lists will be included in the Spam data in the Real Time Reports, but you will not be able to perform a message trace on a message that was edge-blocked.

## Redirected messages:

If a recipient is rewritten by a Policy Filter rule, or because the spam action for the domain is set to Redirect to other address, the message is not traceable in a single search. The original message will be traceable up to the point when the recipient is changed. After that we are not able to trace the message under the original recipient. You will be able to trace the message again using the new recipient.

## Deferred message:

If a message was deferred during delivery it is possible that the delivery results returned by the Message Trace Tool may not be accurate. Not all deferred messages will have inaccurate results. If the message you are trying to trace is affected by this issue, the Delivery Result will read "In Deferral,” even though the message was successfully handed off to the recipient server. We are currently working to solve this problem.

## Directory Services:

 Reject: Similar to any other edge block, Rejects are not traceable.

 Reject Test: Reject Tests are treated much as redirected messages are. The original recipient addresses are re-written in Postfix1 to the "catch all" address.

 Pass Through: Messages destined for a recipient not on the Pass Through list can be traced. The message summary will contain delivery information, but Filtering Results will not be available.

## Virus Cleaned:

Viruses that are cleaned will give no indication in the message trace results. These will appear as "passed filtering" messages delivered to the customer.

## Messages that travel between data centers:

Any message that goes from one data center to another will not be completely traceable.

## Virtual Domains:

 Without Parent Domain address rewrite: These messages will be traceable as long as the recipient address used is the Virtual Domain address. If the original To: address is used, there will be no results returned.

 With Parent domain address rewrite: These messages will also be traceable as long as the recipient address used is the Virtual Domain address.

## MAIL FROM:

The Message Trace Tool uses the MAIL FROM value presented at the initiation of the SMTP conversation as the Sender in the search, regardless of what the DATA section of the message shows. The message may show a Reply-to address or different From: or Sender values. If the e-mail was sent by a process and not by an e-mail client, there is an increased likelihood that the sender in the MAIL FROM doesn't match the sender in the actual e-mail message.

## Policy Rule Updates:

When a message hits a policy rule, the Policy Filter rule ID is stored in the Message Trace and Real Time Reporting databases. If you trace one of these messages, or drill down on policy details in a report, the Message Trace and Real Time Reporting UI dynamically pulls the current rule information from the Hosted Services network based on the Policy Filter Rule ID in the reporting database. If you have changed the attributes of that particular rule since the message was processed (changed it from Reject to Allow, for example), the rule ID stays the same in the Message Trace and Real Time Reporting returned results, but the Admin Center will show the new rule.

# View the Audit Trail

In the Administration Center, the Audit Trail tab on the Tools tab helps you track important events that have occurred in your FOSE service. From the Audit Trail tab, you can view both user-related and service-related events. Events can be sorted by the e-mail address of the logged on user, Company, Domain, activity, or Date and time. You can filter results by clicking a view on the Views pane and by specifying a specific date range for your search. You can search for events that relate to a specific Company or Domain by using the Search box.

The Audit Trail tool tracks changes to an object based on the object ID numbers. Each Company, Domain, User, and Policy Filter Rule has a unique object ID. When investigating changes to an object, make it easier to filter the Audit Trail information by using use the Track Changes feature from the properties of that object In order to narrow the returned results, you can specify the Date Range without changing the Search criteria. To clear the Track Changes search criteria from the Search box, click Clear.

# Technical Support

As an administrator, you can use the Support Incident tracking system to view and search a messaging knowledge base, create new support incidents, update existing support incidents, and track the current status of your support incidents using a Web browser. The Technical Support Service Level Objectives and the Technical Support Escalation Path are posted on the Resource tab of the Welcome pane in the Administration Center.

## The four ways to contact Technical Support to open a support incident

1. Microsoft Premier Support: For more information about accessing Premier Support, go to the Microsoft Premier Support Online Portal or the Microsoft Premier Support Web site.

2. [Technical Support Web site](http://go.microsoft.com/fwlink/?LinkID=149248) (http://go.microsoft.com/fwlink/?LinkID=149248)

3. Technical Support e-mail: support@messaging.microsoft.com

4. Phone: Toll-free: 866.291.7726
Direct: +1.204.927.2299

# International Support and Dialing Codes

Support and help documentation is available in Chinese, Dutch, French, German, Italian, Japanese, Korean, Portuguese, and Spanish. Local language telephone support is also available for these languages. To receive telephone support in one of these languages, follow the instructions for using translation services when you call Microsoft technical support at (866) 291-7726.

When using the UIFN phone number (800-0000-0060), use the following dialing codes for countries and regions that have UIFN support:Australia 0011
Austria 00
Costa Rica 00
Denmark 00
Finland 00
France 00
Germany 00
Hong Kong SAR 001
Italy 00
Japan: 0061-010, for IDC and 041 010, for Japan Telecom
Luxembourg 00
Netherlands 00
Norway 00
Switzerland 00
Use the following individual telephone numbers for countries and regions that do not support UIFN:
Mexico 001-8885086467
Belgium 0800-75013

# Messaging Knowledge Base

From the Web, visit the messaging knowledge base for additional support information. You can search for known issues, submit feedback on the solutions, and subscribe to the support RSS feed to be notified when they are updated. To access the messaging knowledge base, go to the [Support Incident tracking system](http://go.microsoft.com/fwlink/?LinkID=149248), and then click the Knowledge Base tab. Click Search Tips for information about the best keyword syntax to use.

# Submit a Service Request on the Web

You can generate a new support incident by visiting the [Support Incident tracking system](http://go.microsoft.com/fwlink/?LinkID=149248) and clicking the New Incident tab. When you complete the Web form, you are given a 12-digit incident reference number that you can use to update and obtain status on your incident.

# Checking Incident Status

From the [Support Incident tracking system](http://go.microsoft.com/fwlink/?LinkID=149248), you can check the status of a support incident by clicking the Incident Status tab. You can filter incidents based on whether they are opened or closed, and by the words they contain.

# Guidelines for Successful Spam Submissions

FOSE receives spam submissions from all of its customers. The spam team examines indicators within each submitted message, such as the From address, the sending IP address, keywords, catch-phrases, frequency of transmission, and other trends and patterns. After reviewing this information, the spam team initiates the relevant changes to the FOSE spam filtering layers. The message is then classified as spam in the future.

Spam evaluation is an ongoing process that applies regardless of the originating language or character set. Quite often, because a spam message can be vague or even lack text in the subject or message body, the spam team relies on all other available message characteristics to perform filtering. This means that after the spam team flags a given message as spam and makes the necessary changes to its rule base, that message will be blocked in the future until its characteristics have been modified in a manner significant enough to evade our filters.

Spam submissions are processed seven days per week, and new spam rules are deployed continuously. Timeframes for rules on individual submissions vary depending on the quantity and quality of submissions. Because new spam rules are set globally for all customers, be aware that not all individual spam submissions result in a new spam rule.

If Users reports that they are receiving spam in their Inboxes, do the following:

 Ensure that your mail exchange (MX) record is pointed to the filtering network.

 Ensure that your firewall is set to only allow mail from the filtering network.

 If you are using Directory Services Pass Through mode, ensure that users receiving the Spam are added to the Directory Services list.

 If you are using Directory Services Reject Test mode, note that the last user on the list will receive high amounts of spam.

Once you have configured the firewall settings to accept e-mail only from your Hosted E-mail Filtering Service data centers, the best way to submit unfiltered spam messages to the Spam Analysis Team is to send the unfiltered spam message, with the full Internet headers intact, to abuse@messaging.microsoft.com. When submitting to the abuse alias, remember to do the following:

 Submit full Internet headers with the original unfiltered spam message. Do not simply forward the unfiltered spam message, as this process drops the Internet headers.

 Submit the original spam message to the spam evaluation team at abuse@messaging.microsoft.com. Do not modify the spam message or subject line in any way.

 Submit unfiltered spam in a timely manner to ensure the most benefit from your services. Spam messages that are to the evaluation team several days after they were originally received are often too late, as these spam messages may have already been triaged.

To increase submission success, submit only one spam sample per e-mail message. Also, note that it is critical to include the full Internet headers. Do this by sending the offending message as an attachment, along with the full original Internet header, or by using the [Junk-Email Plug-In](http://go.microsoft.com/fwlink/?LinkID=147248) (which is made available for some Microsoft Office Outlook 2003 and Outlook 2007 users, depending on your organization).

Submit the unfiltered spam message with the Internet headers of that message passed in the top portion of the message to abuse@messaging.microsoft.com. For instructions on how to extract the headers manually from many popular e-mail clients, search for the "How do I report spam in the Inbox?" knowledge base article in the [Support Incident tracking system](http://go.microsoft.com/fwlink/?LinkID=149248).