Microsoft

Enabling Office 365 Services

SECOND EDITION

Exam Ref 70-347

Orin Thomas

Microsoft

Exam Ref 70-347 Enabling Office 365 Services

2nd Edition

Orin Thomas

Exam Ref 70-347 Enabling Office 365 Services, Second Edition

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

ISBN-13: 978-1-5093-0478-3
ISBN-10: 1-5093-0478-9

Library of Congress Control Number: 2017963302
1 18

Trademarks

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief	Greg Wiegand
Acquisitions Editor	Laura Norman
Development Editor	Troy Mott
Managing Editor	Sandra Schroeder
Senior Project Editor	Tracey Croom
Editorial Production	Backstop Media
Copy Editor	Christina Rudloff
Indexer	Julie Grady
Proofreader	Christina Rudloff
Technical Editor	Tim Warner
Cover Designer	Twist Creative, Seattle

Contents at a glance

This page intentionally left blank

Contents

Introduction

The 70-347 exam deals with advanced topics that require candidates to have an excellent working knowledge of Office 365, Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business Online, and Office 365 Security and Compliance. Some of the exam comprises topics that even experienced Office 365, Exchange Online, SharePoint Online, and Skype for Business Online administrators may rarely encounter unless they are consultants who deploy new Office 365 tenancies on a regular basis.

Candidates for this exam are Information Technology (IT) Professionals who want to validate their advanced Office 365, Exchange Online, SharePoint Online, Skype for Business Online, OneDrive for Business management skills, configuration skills, and knowledge. To pass this exam, candidates require a strong understanding of how manage and configure Office 365 clients and end user devices, provision SharePoint Online site collections, configure Exchange Online, OneDrive for Business, and Skype for Business Online for end users and manage, migrate to, and administer Exchange Online, OneDrive for Business Online and Skype for Business Online. To pass, candidates require a thorough theoretical understanding as well as meaningful practical experience implementing the technologies involved.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the "Need more review?" links you'll find in the text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learning website: *https://aka.ms/examlist*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

> ***MORE INFO*** **ALL MICROSOFT CERTIFICATIONS**
>
> **For information about Microsoft certifications, including a full list of available certifications, go to *https://www.microsoft.com/learning*.**

Microsoft Virtual Academy

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You'll find what you need here:

https://www.microsoftvirtualacademy.com

Quick access to online references

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these addresses (also known as URLs) can be painstaking to type into a web browser, so we've compiled all of them into a single list that readers of the print edition can refer to while they read.

Download the list at *https://aka.ms/examref3472E/downloads*.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

https://aka.ms/examref3472E/errata

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to https://support.microsoft.com.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

https://aka.ms/tellpress

We know you're busy, so we've kept it short with just a few questions. Your answers go directly to the editors at Microsoft Press. (No personal information will be requested.) Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

This page intentionally left blank

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam ref and another study guide for your ”at home” preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

Note that this Exam Ref is based on publicly available information about the exam and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

This page intentionally left blank

CHAPTER 4

Plan for Exchange Online and Skype for Business Online

For many organizations, the default settings for Exchange Online and Skype for Business Online within an Office 365 tenancy don't require much attention or modification. This is because the default configuration of these services does what the tenants needs them to do. For other users, it is necessary to tune the settings on these services to better meet organizational requirements. In this chapter, you'll read about configuring anti-spam and anti-malware policies, determining an appropriate mailbox migration strategy, performing compliance operations, and managing settings at a tenancy level for Skype for Business Online.

Skills in this chapter:

- Skill 4.1: Manage anti-malware and anti-spam policies
- Skill 4.2: Recommend a mailbox migration strategy
- Skill 4.3: Plan for Exchange Online
- Skill 4.4: Manage Skype for Business global external communications settings

Skill 4.1: Manage anti-malware and anti-spam policies

This skill deals with the Exchange Online anti-malware and anti-spam functionality. You manage this functionality through the configuration of anti-malware and spam filter policies. These policies determine what action Exchange Online will take with spam and malware as it passes through the service.

This skill covers the following topics:

- Anti-malware policies
- Spam filter policies
- Outbound spam policy
- Release quarantine
- Advanced threat protection

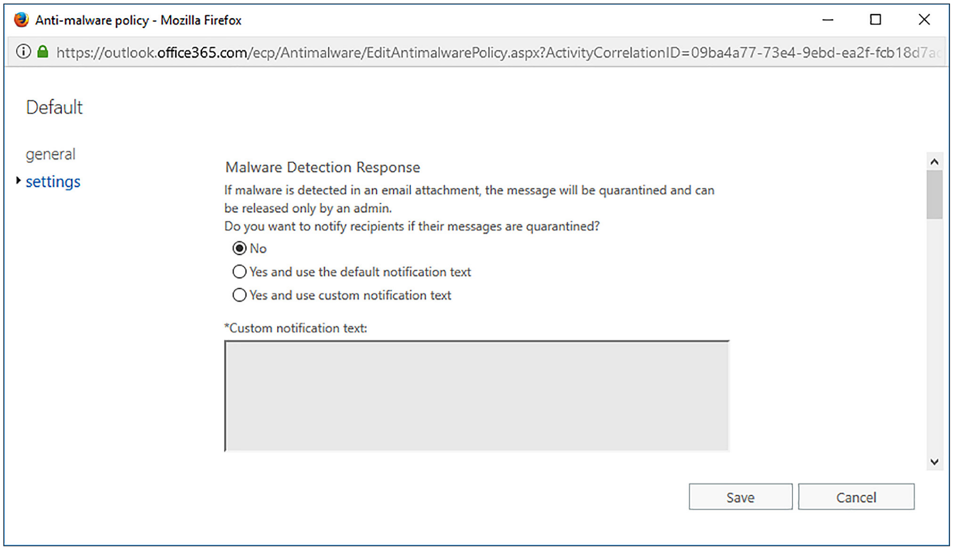
Anti-malware policies

Anti-malware policies allow you to block incoming malware from reaching user inboxes. Anti-malware policies also allow you to stop your own users from inadvertently sending malware to other people in your organization or others on the Internet. Anti-malware policies are part of an in-depth defense strategy. Users in your organization are far less likely to be infected by malware transmitted through email messages if malware is being purged by Exchange Online, as well as by an anti-malware solution installed on the client computer.

> ***MORE INFO*** **ANTI-MALWARE POLICIES**
>
> **You can learn more about anti-malware policies at *https://technet.microsoft.com/en-us/library/jj200745(v=exchg.150).aspx*.**

Malware detection response

The malware detection response settings determine what happens when malware is detected in a message attachment on inbound and outbound messages. When malware is detected, the message is automatically quarantined. Only an administrator can release a message from quarantine. Because the malware engine occasionally generates false positives, you may wish to notify users if a message sent to them is flagged as containing malware. You can do this with the Malware Detection Response settings shown in Figure 4-1.


Anti-malware policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antimalware/EditAntimalwarePolicy.aspx?ActivityCorrelationID=09ba4a77-73e4-9ebd-ea2f-fcb18d7a
Default
general
settings
Save
Cancel

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

● No

○ Yes and use the default notification text

○ Yes and use custom notification text

*Custom notification text:

FIGURE 4-1 Malware Detection Response

You can configure the following options:

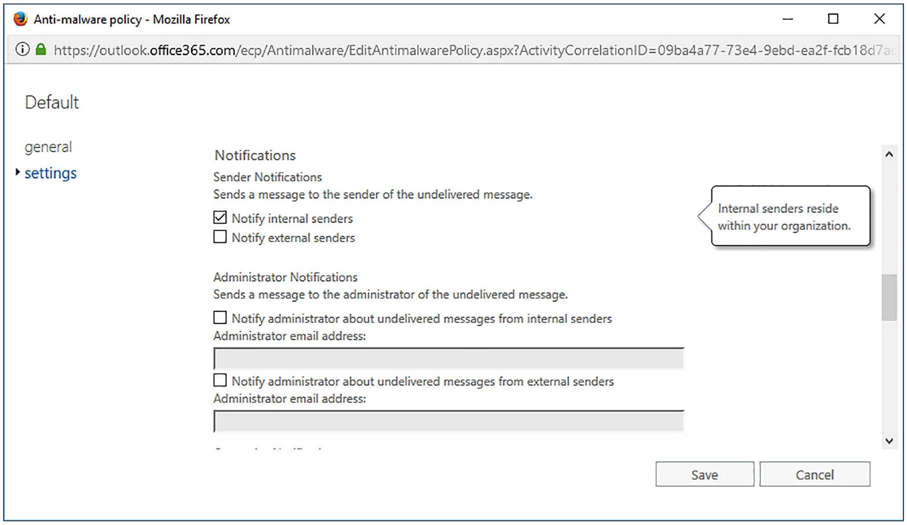
- **No** No notification is sent to the recipient.

- **Yes And Use The Default Notification Text** A notification using the default notification text is sent to the recipient.
- **Yes And Use Custom Notification Text** A notification using custom notification text is sent to the recipient.

Anti-malware notifications

Notifications allow you to configure whether the sender of the message in which malware is detected is notified and whether administrators are notified. Notifications are only sent when the entire message is deleted. The notification language is dependent on the location of the message being processed. You can choose the following options, shown in Figure 4-2:

- **Notify Internal Senders** Sends a message to a sender from within your organization who sends a message in which malware is detected.
- **Notify External Senders** Sends a message to a sender external to your organization who sends a message to someone inside your organization in which malware is detected.
- **Notify Administrators About Undelivered Messages From Internal Senders** Allows you to have an administrator sent a message about messages from internal senders in which malware is detected. You need to provide the administrator email address.
- **Notify Administrators About Undelivered Messages From External Senders** Allows you to have an administrator sent a message about messages from external senders in which malware is detected. You need to provide the administrator email address.



Anti-malware policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antimalware/EditAntimalwarePolicy.aspx?ActivityCorrelationID=09ba4a77-73e4-9ebd-ea2f-fcb18d7a

Default

general

settings

Notifications

Sender Notifications

Sends a message to the sender of the undelivered message.

☑ Notify internal senders

□ Notify external senders

Internal senders reside within your organization.

Administrator Notifications

Sends a message to the administrator of the undelivered message.

□ Notify administrator about undelivered messages from internal senders

Administrator email address:

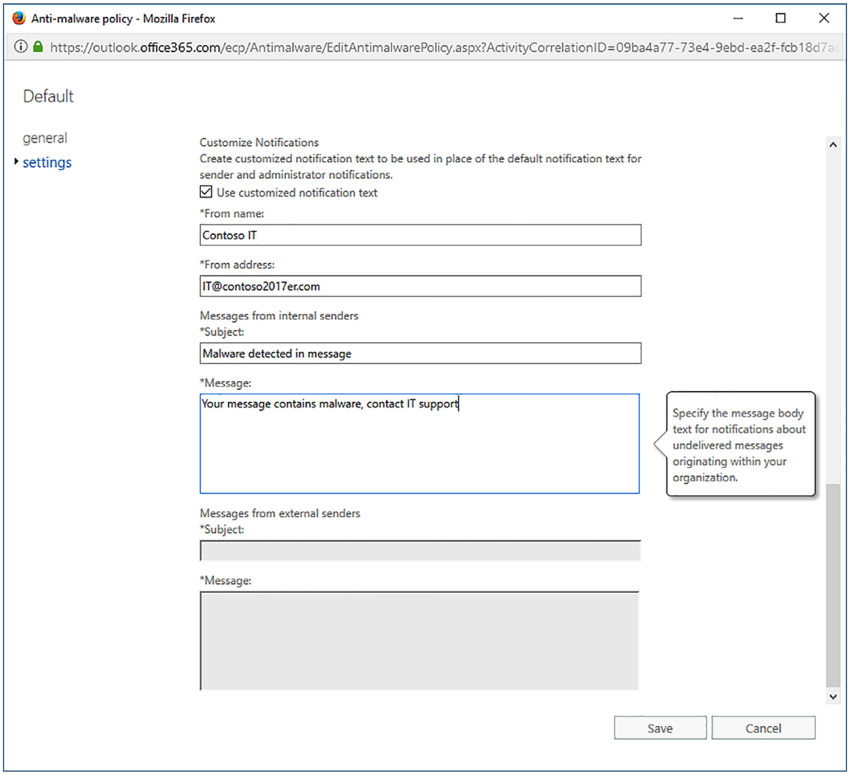
□ Notify administrator about undelivered messages from external senders

Administrator email address:

FIGURE 4-2 Notifications Settings

The default notification text is as follows "This message was created automatically by mail delivery software. Your email message was not delivered to the intended recipients because malware was detected." If you don't want to use the default notification text, you can create your own custom notification text by configuring the following settings, shown in Figure 4-3. These settings are only available if the relevant notifications are configured.

- **From Name** The name that the email message appears to be from.
- **From Address** The email address the message appears to originate from.
- **Messages From Internal Senders** The subject and the message sent to internal senders who have messages deleted by the anti-malware policy.
- **Messages From External Senders** The subject and the message sent to external senders who have messages deleted by the anti-malware policy.



Anti-malware policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antimalware/EditAntimalwarePolicy.aspx?ActivityCorrelationID=09ba4a77-73e4-9ebd-ea2f-fcb18d7a
Default
general
settings
Save
Cancel

Customize Notifications

Create customized notification text to be used in place of the default notification text for sender and administrator notifications.

☑ Use customized notification text

*From name: Contoso IT

*From address: IT@contoso2017er.com

Messages from internal senders

*Subject: Malware detected in message

*Message: Your message contains malware, contact IT support

Specify the message body text for notifications about undelivered messages originating within your organization.

Messages from external senders

*Subject:

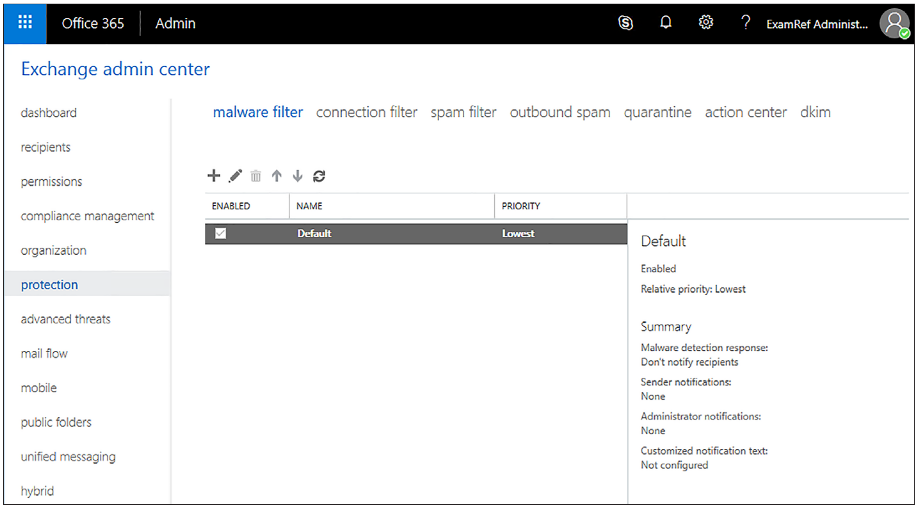
*Message:

FIGURE 4-3 Customized notifications

Review default anti-malware policy

To review the default anti-malware policy, perform the following steps:

1. In the Office 365 Admin Center, click Exchange under Admin Centers.
2. In Exchange Admin Center, click Protection, and then click Malware Filter. Figure 4-4 shows the Default anti-malware policy selected.



ENABLED	NAME	PRIORITY
☑	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

Malware detection response:
Don't notify recipients

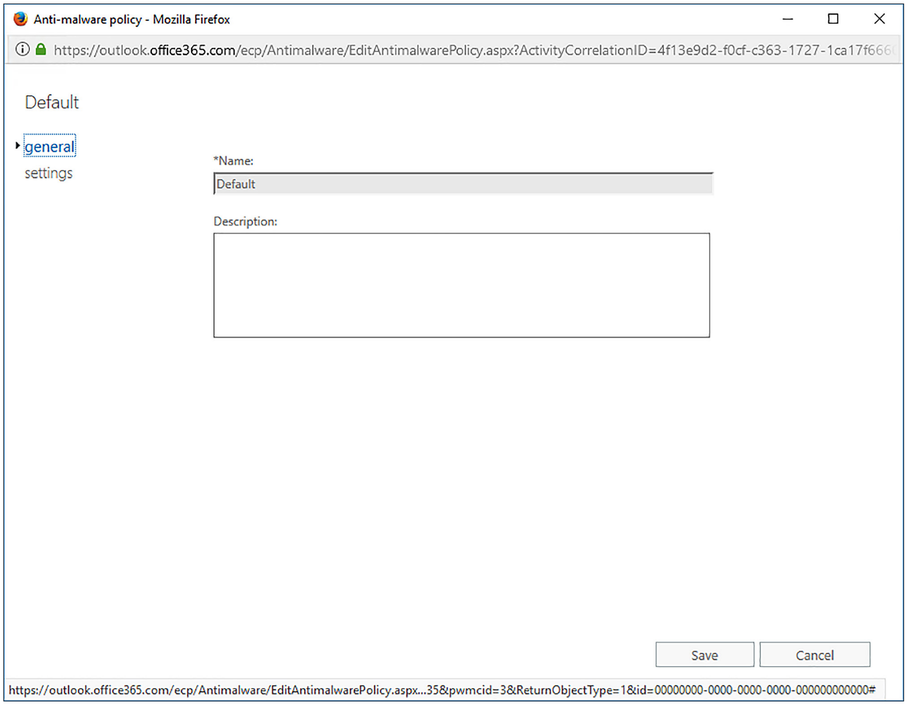
Sender notifications:
None

Administrator notifications:
None

Customized notification text:
Not configured

FIGURE 4-4 Default Malware Filter policies

3. With the Default policy selected, click the edit (Pencil) icon on the toolbar. This opens the Anti-Malware Policy properties page. The General section, shown in Figure 4-5, shows the policy Name and Description.



Anti-malware policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antimalware/EditAntimalwarePolicy.aspx?ActivityCorrelationID=4f13e9d2-f0cf-c363-1727-1ca17f666

Default

*Name: Default

Description:

https://outlook.office365.com/ecp/Antimalware/EditAntimalwarePolicy.aspx...35&pwmcid=3&ReturnObjectType=1&id=00000000-0000-0000-0000-000000000000#

FIGURE 4-5 Default Policy

4. On the Settings page, you can configure the following settings:
   - Malware Detection Response
   - Notifications
   - Administrator Notifications
   - Customize Notifications

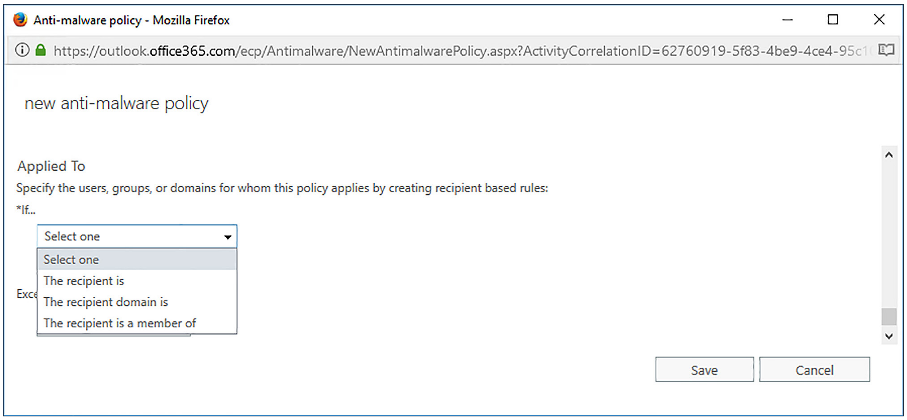
Create an anti-malware policy

You can create different anti-malware policies and then apply them to different groups of mail users. For example, you might wish to have an anti-malware policy for one group of users that provides notifications to the user if malware is detected and a message is purged, and another policy that sends notifications to an administrator if malware is detected and the message purged.

When creating a new custom anti-malware policy, you need to configure the Applied To setting. This setting takes the form of an If statement with a condition and exceptions. As Figure 4-6 shows, the If conditions can include:

- **The Recipient Is** Use this to specify a specific recipient.
- **The Recipient Domain Is** Use this to specify the recipient's mail domain.

- **The Recipient IS A Member Of** Use this to specify a recipient group.



Anti-malware policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antimalware/NewAntimalwarePolicy.aspx?ActivityCorrelationID=62760919-5f83-4be9-4ce4-95c1

new anti-malware policy

Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

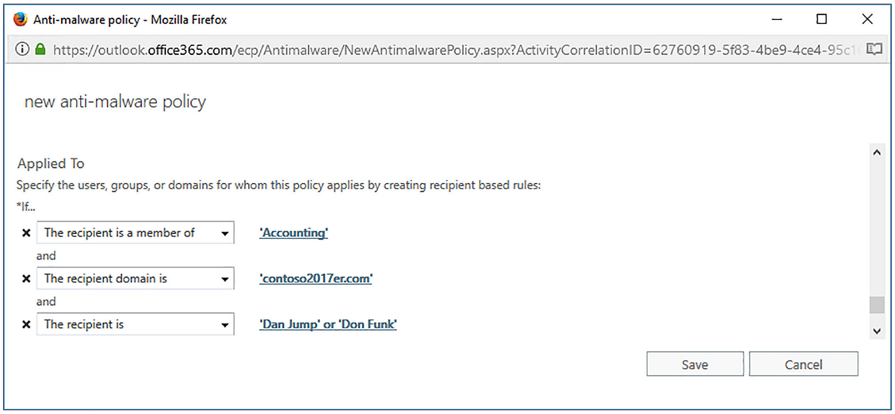
*If...

FIGURE 4-6 Select condition

The exceptions are the same and include:

- **The Recipient Is** Use this to specify a specific recipient.
- **The Recipient Domain Is** Use this to specify the recipient's mail domain.
- **The Recipient Is A Member Of** Use this to specify a recipient group.

You can create as many conditions as you want, as long as those conditions are unique. For example, Figure 4-7 shows a set of conditions that apply if the recipient is a member of the Accounting group, the recipient domain is contoso2017er.com, and if the recipient is Dan Jump or Don Funk.



Anti-malware policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antimalware/NewAntimalwarePolicy.aspx?ActivityCorrelationID=62760919-5f83-4be9-4ce4-95c1

new anti-malware policy

Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

× The recipient is a member of 'Accounting'

and

× The recipient domain is 'contoso2017er.com'

and

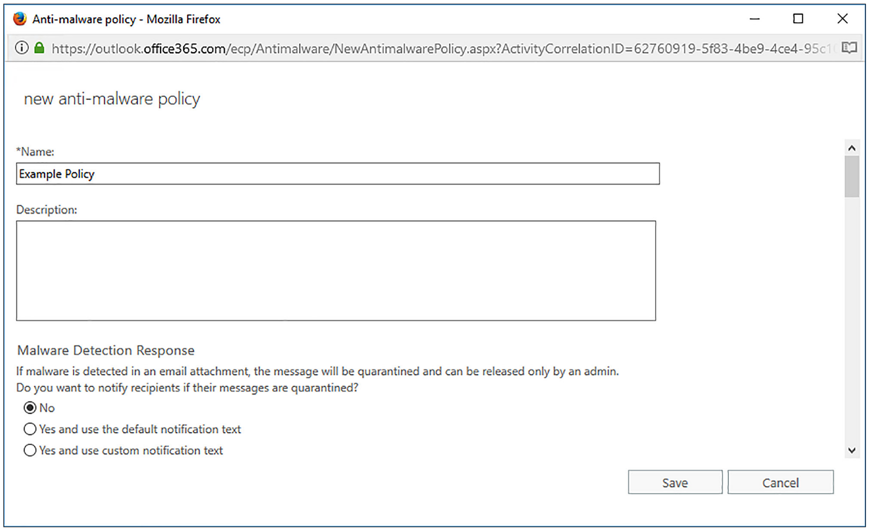
× The recipient is 'Dan Jump' or 'Don Funk'

FIGURE 4-7 Policy conditions

To create a new anti-malware policy, perform the following steps:

1. In the Office 365 Admin Center, click Exchange under Admin Centers.
2. In Exchange Admin Center, click Protection, and then click Malware Filter.

3. Click the Plus (+) icon. This opens the New Anti-Malware Policy page, shown in Figure 4-8. Provide the following information:
   - Policy Name
   - Policy Description
   - Malware Detection Response
   - Notification Settings
   - Applies To Settings



Anti-malware policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antimalware/NewAntimalwarePolicy.aspx?ActivityCorrelationID=62760919-5f83-4be9-4ce4-95c1

new anti-malware policy

*Name: Example Policy

Description:

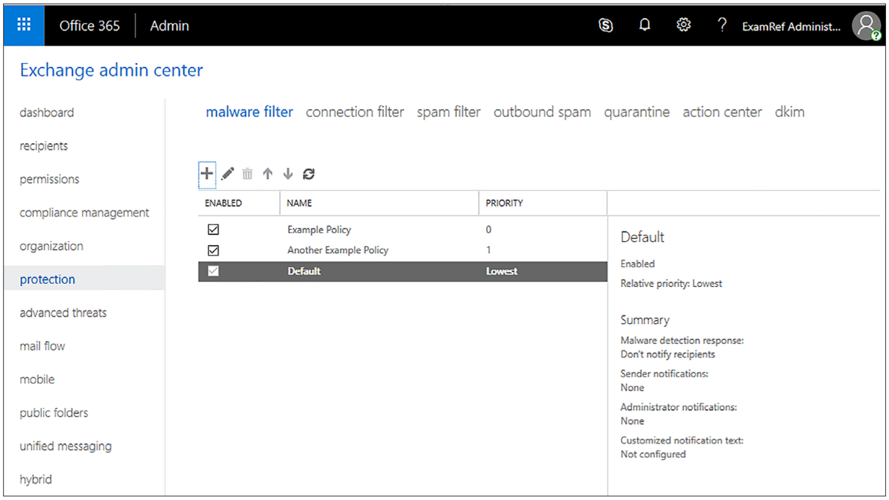
Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.
Do you want to notify recipients if their messages are quarantined?

● No
○ Yes and use the default notification text
○ Yes and use custom notification text

FIGURE 4-8 New anti-malware policy

When you have multiple policies, you can use the Malware Filter list to determine which apply and in which order they apply. The policy with the number closest to zero applies first. If the conditions of a message don't match the first policy, it moves to the next policy until it encounters the Default policy. If any malware filter policies are configured, as shown in Figure 4-9, Example Policy is applied first, and then Another Example Policy, and then finally the Default policy. You can use the arrows to change the priority assigned to each policy.



ENABLED	NAME	PRIORITY
☑	Example Policy	0
☑	Another Example Policy	1
☑	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

Malware detection response:
Don't notify recipients

Sender notifications:
None

Administrator notifications:
None

Customized notification text:
Not configured

FIGURE 4-9 Policy priorities

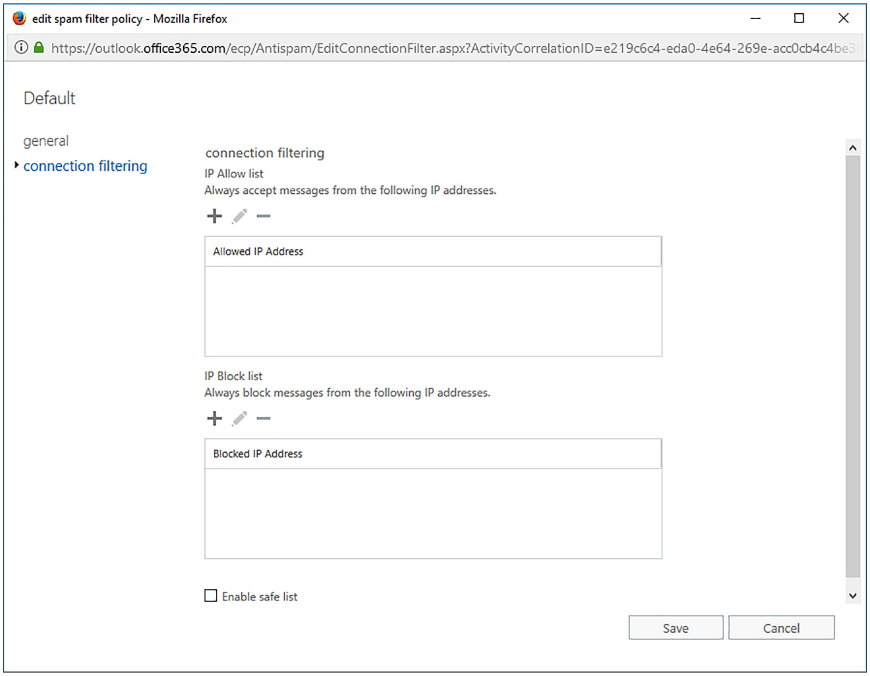
Windows PowerShell anti-malware policy cmdlets

There are a number of Windows PowerShell cmdlets that you can use to manage filter policies and malware filter rules. Filter rules determine the conditions under which a malware filter policy applies. For example, you might have one malware filter policy that applies to recipients in one recipient domain and another malware filter policy that applies to recipients in another recipient domain. The Windows PowerShell anti-malware policy cmdlets are as follows:

- **Get-MalwareFilterPolicy** This cmdlet allows you to view malware filter policy settings.
- **Set-MalwareFilterPolicy** This cmdlet allows you to modify malware filter policy settings.
- **New-MalwareFilterPolicy** Allows you to create a new custom malware filter policy. This includes configuring an action, either blocking a message, replacing attachments with the default alert, or with a custom alert, and configuring notification settings.
- **Remove-MalwareFilterPolicy** This cmdlet allows you to remove a custom filter policy.
- **New-MalwareFilterRule** Use this cmdlet to create a new filter rule that can be applied to a custom policy. For example, you could use this cmdlet to apply a specific malware filter policy named ContosoExamplePolicy when the email recipient is in the contoso.com domain.
- **Set-MalwareFilterRule** Use this cmdlet to edit an existing malware filter rule. For example, to change a rule so that it applies a specific policy to recipients in more than one email domain.
- **Enable-MalwareFilterRule** Use this cmdlet to turn on a malware filter rule.
- **Disable-MalwareFilterRule** Allows you to turn off a malware filter rule.

Connection filter policies

Connection filter policies let you always allow email from trusted senders and always block email from known spammers. Exchange Online only supports the default connection filter policy. You configure connection filters by configuring an IP Allow list and an IP block list, as shown in Figure 4-10.



edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=e219c6c4-eda0-4e64-269e-acc0cb4c4be3

Default

general

connection filtering

connection filtering

IP Allow list

Always accept messages from the following IP addresses.

Allowed IP Address

IP Block list

Always block messages from the following IP addresses.

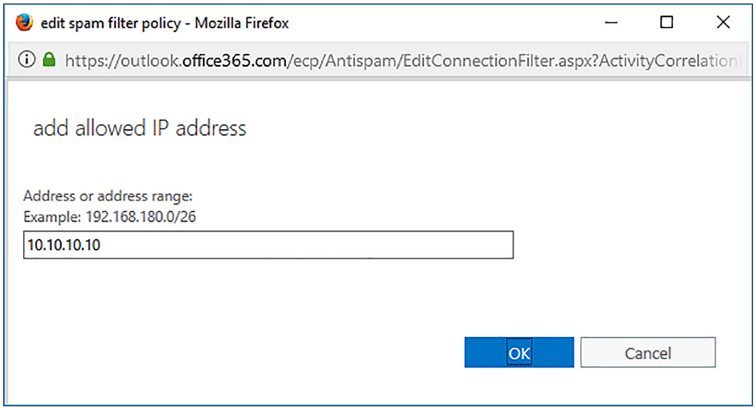
Blocked IP Address

□ Enable safe list

FIGURE 4-10 Connection Filtering

When configuring connection filters, you can also enable the Safe List check box. When you enable this check box, your connection filter allows messages from a list of third-party sources of trusted senders to which Microsoft subscribes.

When adding an IP address list, you can either specify the IP address directly, or use CIDR notation in the form xxx.xxx.xxx.xxx/yy, where yy is a number between 24 and 32. You can specify a maximum of 1,273 separate entries, where an entry is either a single IP address or a CIDR range. IPv6 addresses are supported for TLS encrypted messages. You enter allowed IP addresses on the Allowed IP Address WebPage Dialog, shown in Figure 4-11.


edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelation

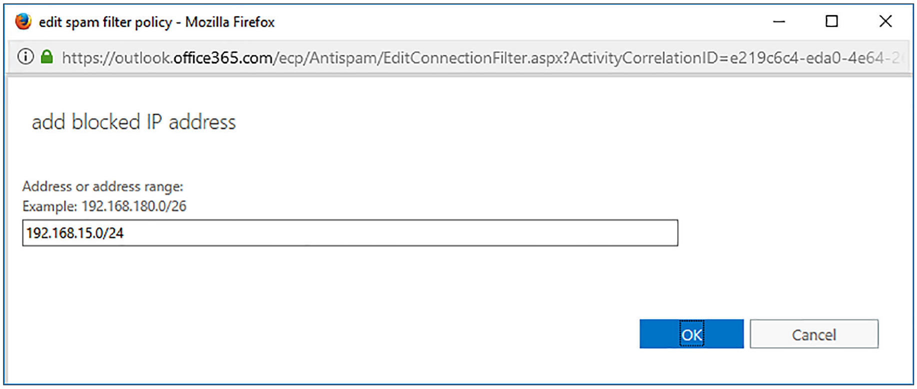
add allowed IP address

Address or address range:
Example: 192.168.180.0/26

10.10.10.10

FIGURE 4-11 Allowed IP address

You enter blocked IP address ranges on the Blocked IP Address webpage dialog box, as shown in Figure 4-12.


edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=e219c6c4-eda0-4e64-2

add blocked IP address

Address or address range:
Example: 192.168.180.0/26

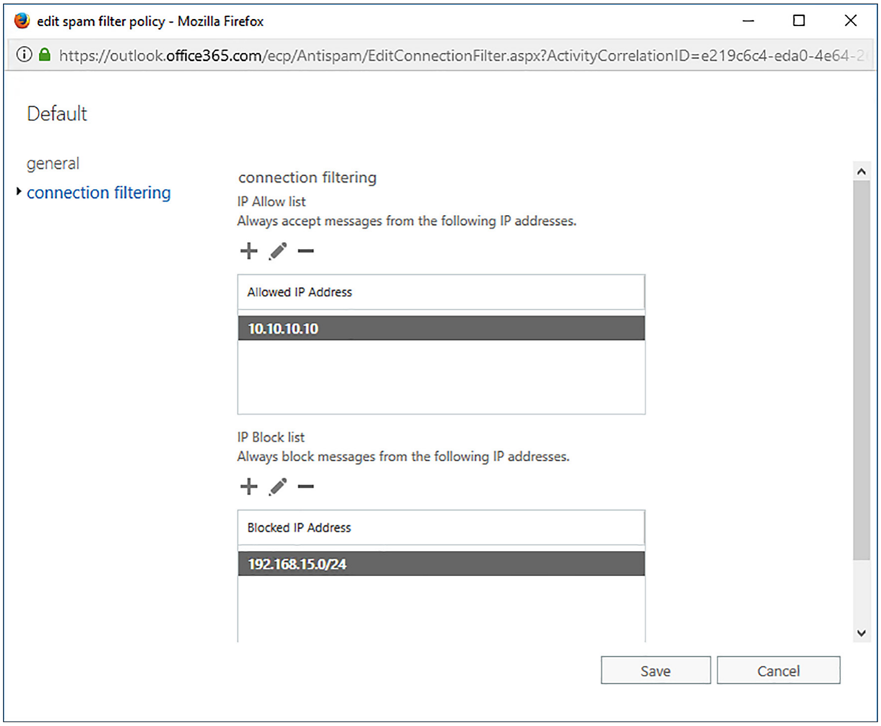
192.168.15.0/24

FIGURE 4-12 Add Blocked IP Address

If an IP address is added to both the allow list and the block list, email from that IP address will be allowed.

To edit the default connection filter policy, perform the following steps:

1. In the Office 365 Admin Center, click Exchange under Admin Centers.
2. In Exchange Admin Center, click Protection, and then click Connection Filter.
3. With the Default policy selected, click the Edit (Pencil) icon.
4. Click the Connection Filtering tab to access the IP Allow list, the IP Block list, and the Enable Safe List option, as shown in Figure 4-13.



edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=e219c6c4-eda0-4e64-2

Default

connection filtering

IP Allow list

Always accept messages from the following IP addresses.

Allowed IP Address
10.10.10.10

IP Block list

Always block messages from the following IP addresses.

Blocked IP Address
192.168.15.0/24

FIGURE 4-13 IP Allow and block lists

You can use the following Windows PowerShell cmdlets to managed the connection filter policy:

- **Get-HostedConnectionFilterPolicy** Use this cmdlet when you want to review the default policy settings.
- **Set-HostedConnectionFilterPolicy** Use this cmdlet to configure the connection filter policy settings. This cmdlet includes the `IPAllowLIst` and `IPBlockList` parameters.

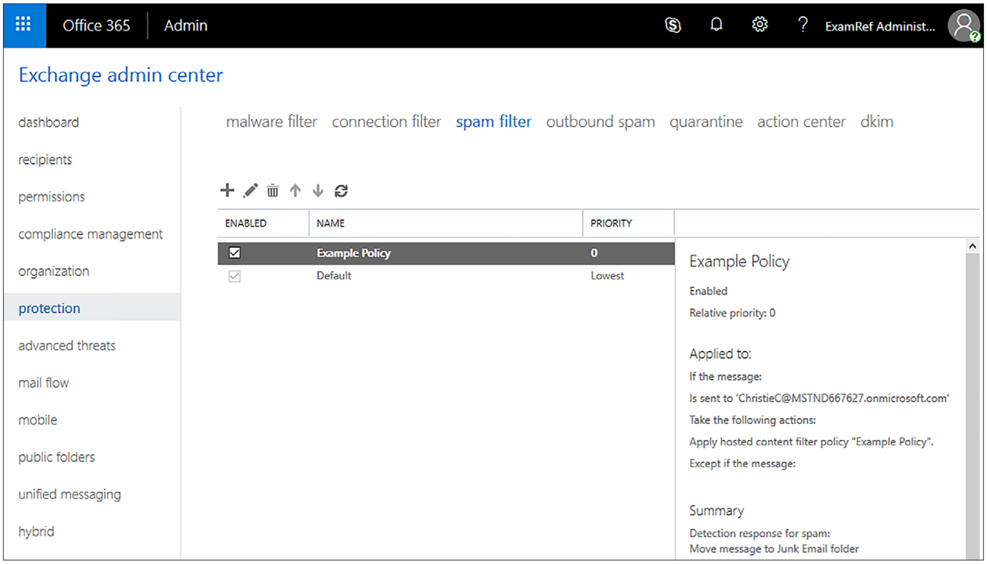
MORE INFO **CONNECTION FILTER POLICIES**

You can learn more about connection filter policies at: *https://technet.microsoft.com/en-us/library/jj200718(v=exchg.150).aspx*.

Spam filter policies

Spam filter policies allow you to configure how incoming messages are categorized, including which characteristics a message might have that means you want flagged as spam. The default policy applies to all users in the company. You can also configure custom policies that apply to specific users, groups, and domains within the organization.

You configure spam filter policies on the Spam Filter tab of the Protection section in Exchange Admin Center, as shown in Figure 4-14. You can have multiple policies as long as each policy has a different set of conditions. The highest priority policy that has conditions that match a message will apply. When there are multiple custom policies, you can adjust their priority using the arrow buttons in the Exchange Admin Center.



ENABLED	NAME	PRIORITY
☑	Example Policy	0
☑	Default	Lowest

Example Policy

Enabled

Relative priority: 0

Applied to:

If the message:

Is sent to 'ChristieC@MSTND667627.onmicrosoft.com'

Take the following actions:

Apply hosted content filter policy "Example Policy".

Except if the message:

Summary

Detection response for spam:
Move message to Junk Email folder

FIGURE 4-14 Policy priority

MORE INFO **SPAM FILTER POLICIES**

You can learn more about spam filter policies at: *https://technet.microsoft.com/en-us/library/jj200684(v=exchg.150).aspx.*

Spam and bulk actions

When configuring the default policy or creating a custom policy, you need to configure which actions to take for messages that are likely to be spam and messages that are almost certainly spam.

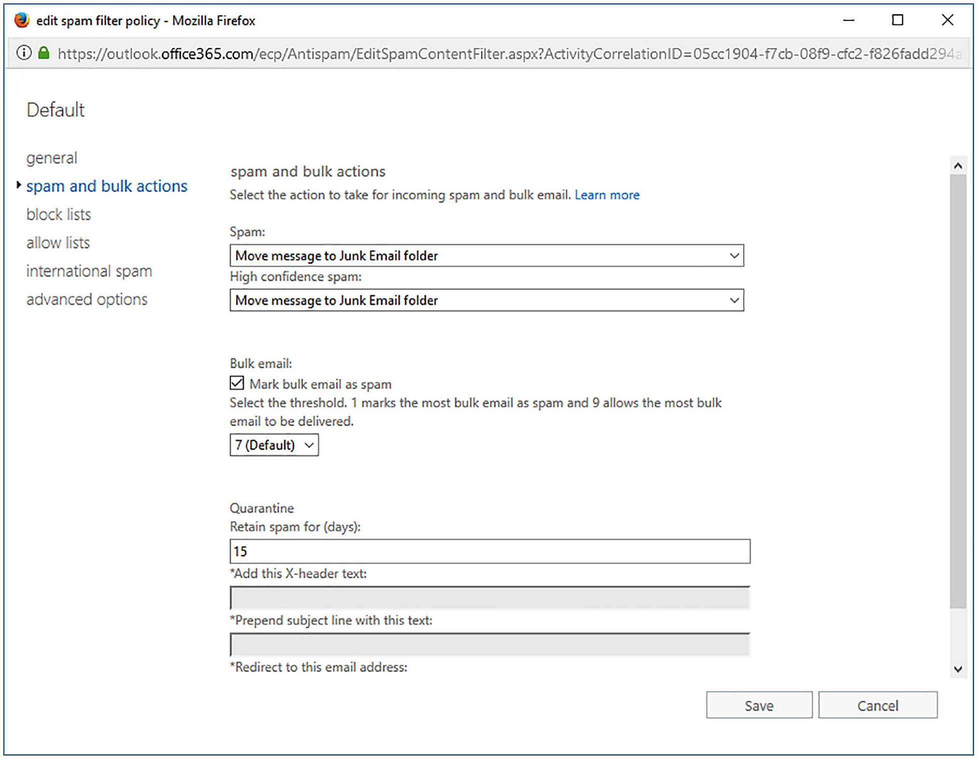
You can choose from the following options for messages that are likely to be spam and for messages that are almost certainly spam:

- **Move Message To Junk Email Folder** This is the default, with messages moved to each user's junk email folder.
- **Quarantine Message** When this setting is chosen, messages are moved to a quarantine folder for up to 15 days before being deleted. Being moved to quarantine allows someone to review the message so that they can determine whether or not it is actually

spam. For example, you might choose to quarantine messages that are likely to be spam and delete messages that are almost certainly spam.

- **Delete Message** When this setting is chosen, the message and any attachments are simply deleted.

You can also configure whether bulk email is marked as spam and the threshold that should be applied to bulk email. Setting the threshold as 1 will have almost all bulk email treated as spam and a setting of 9 will allow almost all bulk email to be delivered. A setting of 7 is the default. The Spam And Bulk Actions tab of a spam filter policy is shown in Figure 4-15.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9-cfc2-f826fadd294a
Default
general
spam and bulk actions
block lists
allow lists
international spam
advanced options
Save
Cancel

spam and bulk actions

Select the action to take for incoming spam and bulk email. Learn more

Spam: Move message to Junk Email folder

High confidence spam: Move message to Junk Email folder

Bulk email:

☑ Mark bulk email as spam

Select the threshold. 1 marks the most bulk email as spam and 9 allows the most bulk email to be delivered.

7 (Default)

Quarantine

Retain spam for (days): 15

*Add this X-header text:

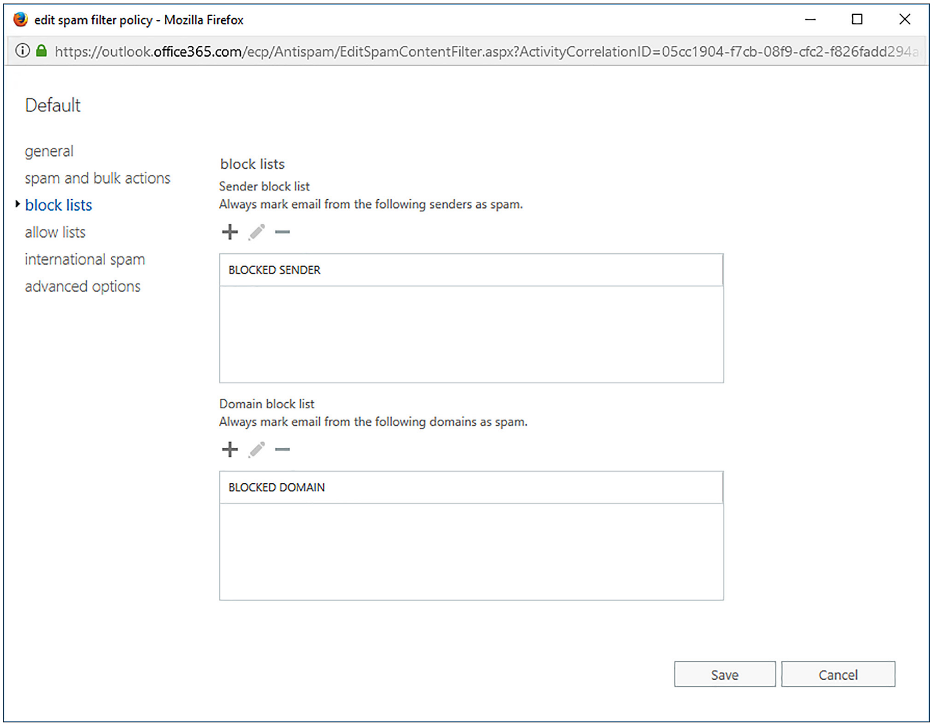
*Prepend subject line with this text:

*Redirect to this email address:

FIGURE 4-15 Spam And Bulk Actions

Spam filter block lists

The block lists setting of a spam filter policy, shown in Figure 4-16, allows you to block email messages from specific email addresses or specific email domains. When a message comes from a blocked sender or a blocked domain, it is subject to the high confidence spam action configured in the spam and bulk actions section of the policy.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9-cfc2-f826fadd294a
Default
general
spam and bulk actions
block lists
allow lists
international spam
advanced options
block lists
Save
Cancel

Sender block list

Always mark email from the following senders as spam.

BLOCKED SENDER

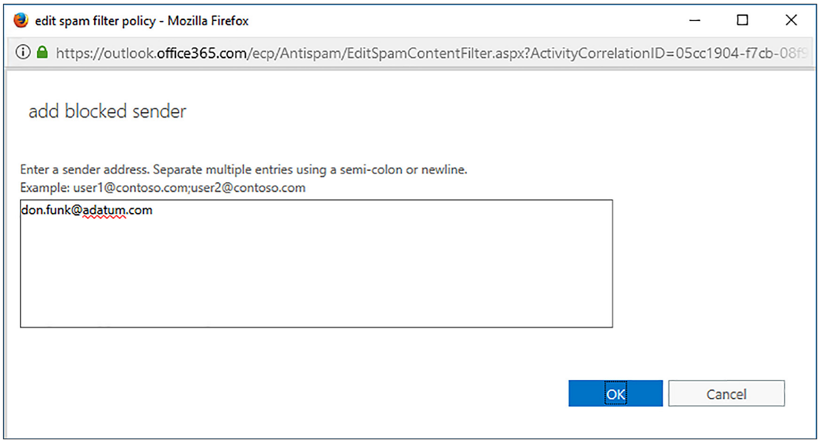
Domain block list

Always mark email from the following domains as spam.

BLOCKED DOMAIN

FIGURE 4-16 Block Lists

If you want to block all messages from a specific email address, you can add that email address to the blocked sender list. Figure 4-17 shows the email address don.funk@adatum.com being added to this list. The owner of the email address added to the list will not be notified that their email messages are being categorized as spam.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9
add blocked sender
OK
Cancel

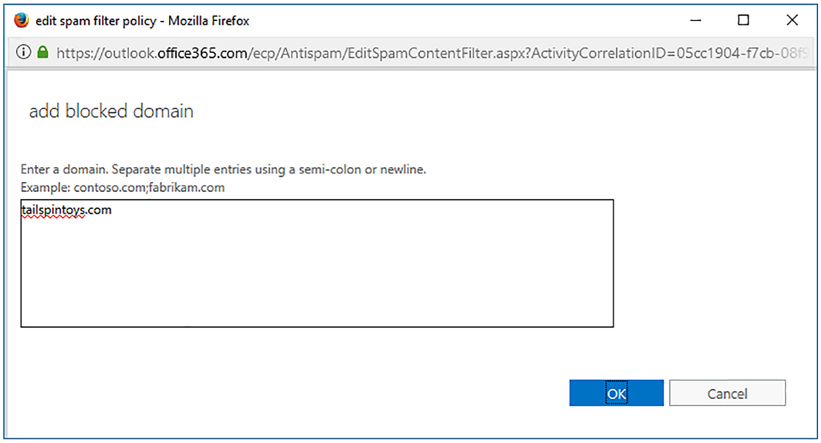
Enter a sender address. Separate multiple entries using a semi-colon or newline.

Example: user1@contoso.com;user2@contoso.com

don.funk@adatum.com

FIGURE 4-17 Block sender

You can add entire mail domains to a block list using the Add Blocked Domain dialog box shown in Figure 4-18. You should be as specific as possible when adding domains. If you add a top level domain, such as .com or .org to this list, all email messages that come from .com or .org addresses are marked as spam.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9
OK
Cancel

add blocked domain

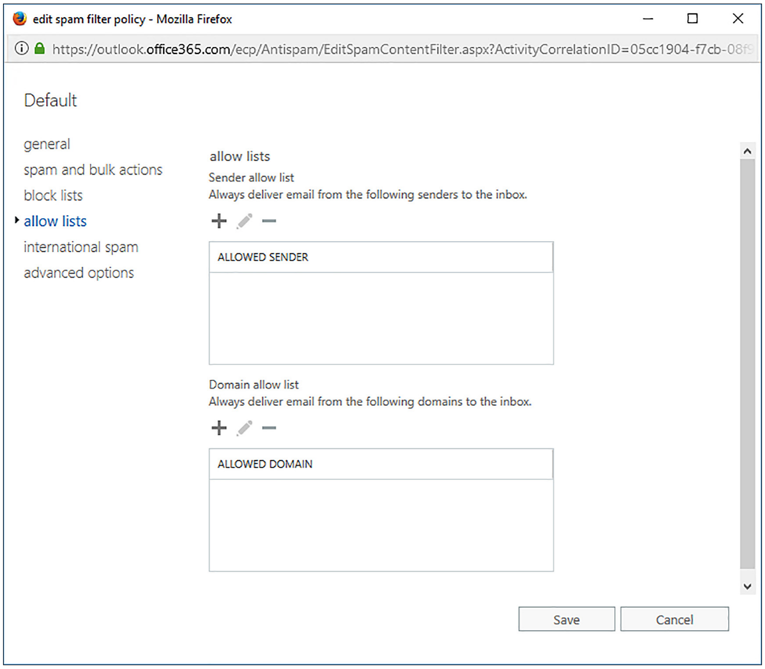
Enter a domain. Separate multiple entries using a semi-colon or newline.
Example: contoso.com;fabrikam.com

tailspintoys.com

FIGURE 4-18 Blocked Domain

Spam filter allow lists

Spam filter allow lists provide you with a way of ensuring that email messages from specific users or from specific domains will always be delivered to users in your organization. When configuring Allow Lists in a spam filter policy, you configure the Sender Allow List for specific email addresses and the Domain Allow List for specific email domains. The Allow Lists section of the spam filter policy is shown in Figure 4-19.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9
Default
general
spam and bulk actions
block lists
allow lists
international spam
advanced options
Save
Cancel

allow lists

Sender allow list

Always deliver email from the following senders to the inbox.

ALLOWED SENDER

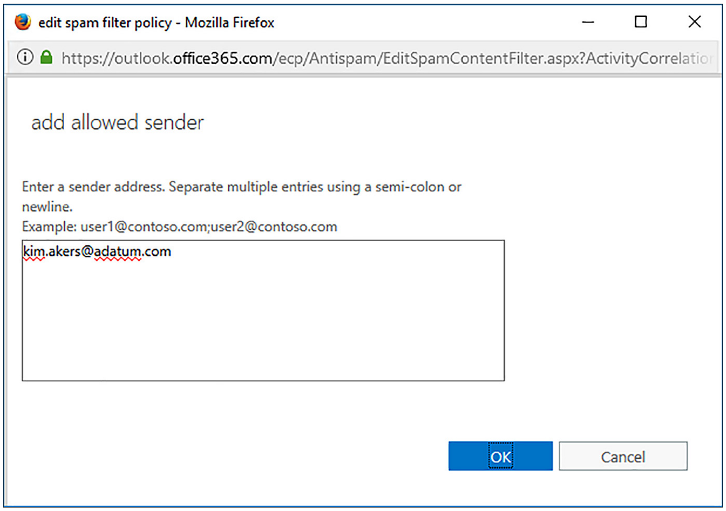
Domain allow list

Always deliver email from the following domains to the inbox.

ALLOWED DOMAIN

FIGURE 4-19 Allow Lists

You add users to the Allow List using the Add Allowed Sender dialog box, as shown in Figure 4-20. To separate email address entries, use a semicolon.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelatio
OK
Cancel

add allowed sender

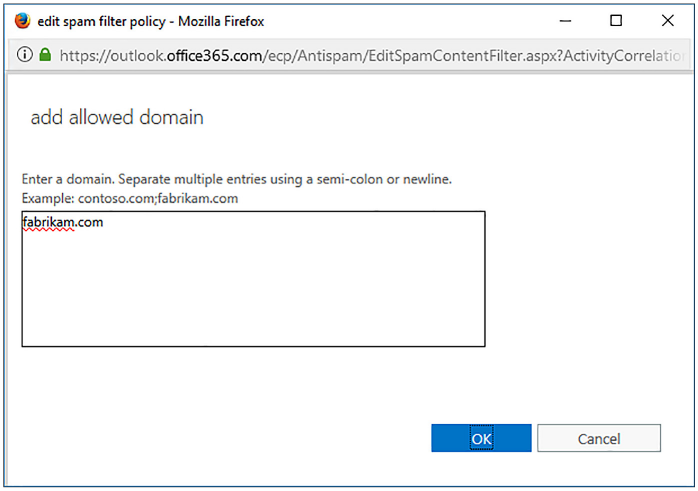
Enter a sender address. Separate multiple entries using a semi-colon or newline.

Example: user1@contoso.com;user2@contoso.com

kim.akers@adatum.com

FIGURE 4-20 Allowed Sender

You Add Allowed Domains on the Add Allowed Domain dialog box, shown in Figure 4-21. You should be as specific as possible and not add generic top-level domains such as .com or .org because this allows email from all .com and .org domains.



edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelatio

add allowed domain

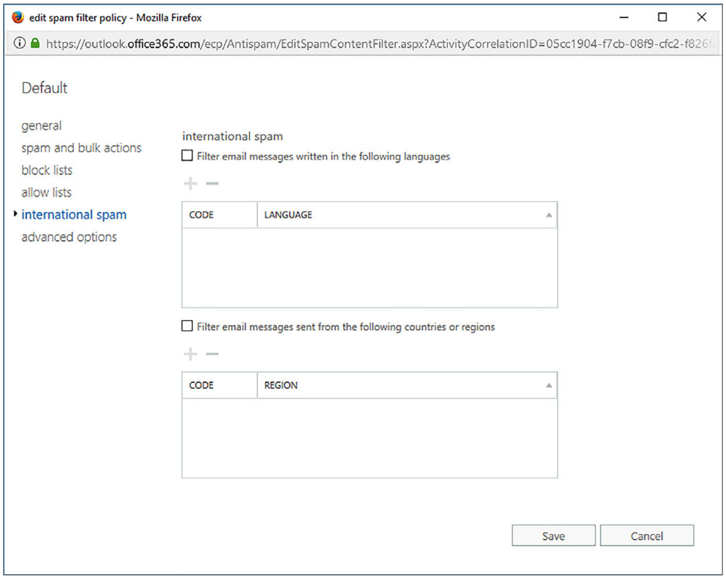
Enter a domain. Separate multiple entries using a semi-colon or newline.
Example: contoso.com;fabrikam.com

fabrikam.com

FIGURE 4-21 Allowed Domain

International spam

The International Spam settings, shown in Figure 4-22, allow you to filter messages based on the message language and the country or region from which the message is sent.



edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9-cfc2-f826f

Default

international spam

□ Filter email messages written in the following languages

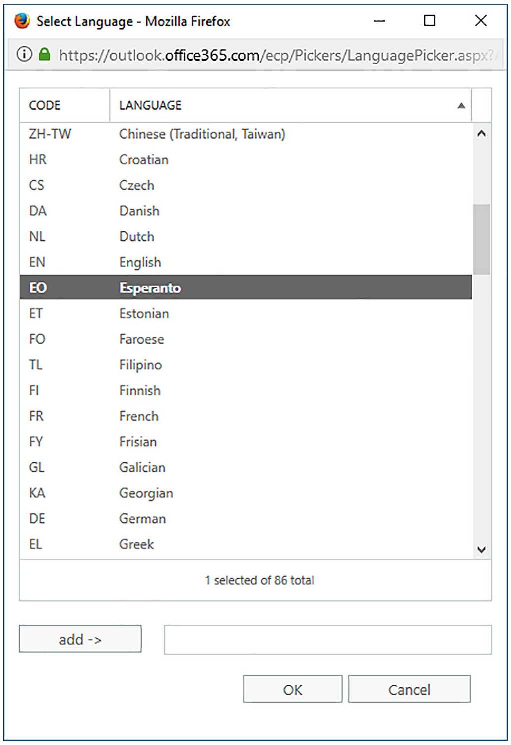
CODE	LANGUAGE

□ Filter email messages sent from the following countries or regions

CODE	REGION

FIGURE 4-22 International Spam

When blocking message content on the basis of language, you enable the Filter Email Messages Written In The Following Languages option, and then specify the languages you want to filter on the Select Language dialog box, as shown in Figure 4-23.


Select Language - Mozilla Firefox

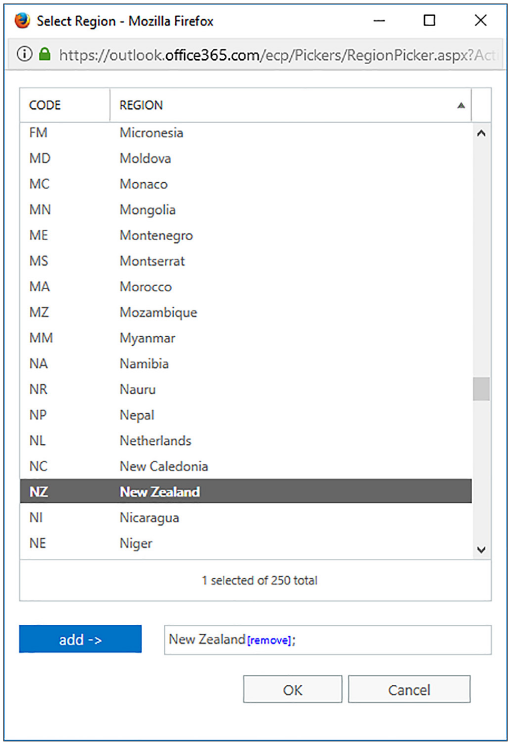
https://outlook.office365.com/ecp/Pickers/LanguagePicker.aspx?

CODE	LANGUAGE
ZH-TW	Chinese (Traditional, Taiwan)
HR	Croatian
CS	Czech
DA	Danish
NL	Dutch
EN	English
EO	Esperanto
ET	Estonian
FO	Faroese
TL	Filipino
FI	Finnish
FR	French
FY	Frisian
GL	Galician
KA	Georgian
DE	German
EL	Greek

1 selected of 86 total

FIGURE 4-23 Select language

To block messages from specific regions, enable the Filter Email Messages Sent From The Following Countries Or Regions option, and then specify the countries or regions that you want to filter out on the Select Region dialog box, as shown in Figure 4-24.



Select Region - Mozilla Firefox

https://outlook.office365.com/ecp/Pickers/RegionPicker.aspx?Act

CODE	REGION
FM	Micronesia
MD	Moldova
MC	Monaco
MN	Mongolia
ME	Montenegro
MS	Montserrat
MA	Morocco
MZ	Mozambique
MM	Myanmar
NA	Namibia
NR	Nauru
NP	Nepal
NL	Netherlands
NC	New Caledonia
NZ	**New Zealand**
NI	Nicaragua
NE	Niger

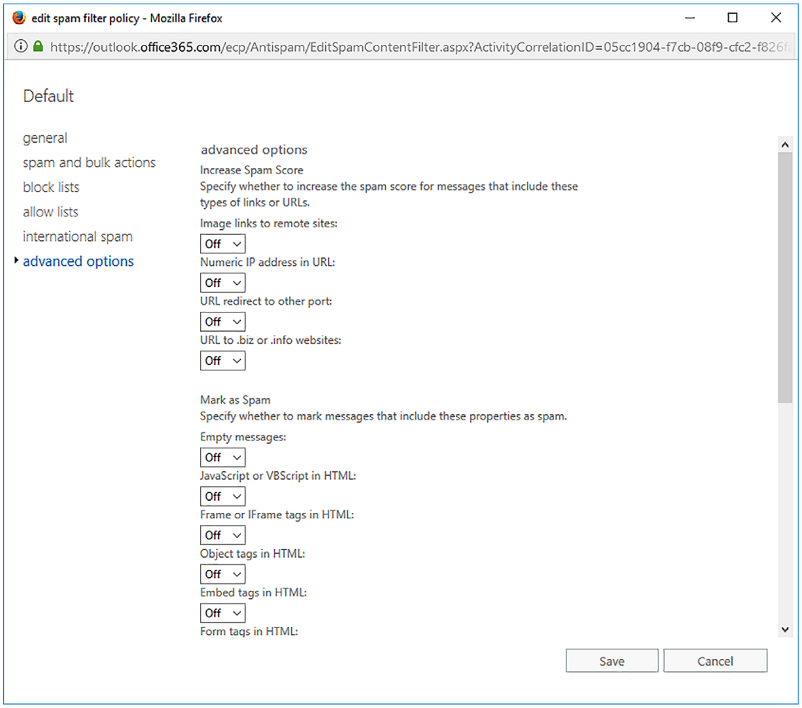
1 selected of 250 total

New Zealand [remove];

FIGURE 4-24 Select Region

Advanced policy options

Advanced policy options, shown in Figure 4-25, allow you to toggle specific options that either increase the spam score, making it more likely that Exchange Online will recognize the message as spam, or simply mark the message as spam directly.



edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=05cc1904-f7cb-08f9-cfc2-f826f
Default
general
spam and bulk actions
block lists
allow lists
international spam
advanced options
Save
Cancel

advanced options

Increase Spam Score

Specify whether to increase the spam score for messages that include these types of links or URLs.

Image links to remote sites: Off

Numeric IP address in URL: Off

URL redirect to other port: Off

URL to .biz or .info websites: Off

Mark as Spam

Specify whether to mark messages that include these properties as spam.

Empty messages: Off

JavaScript or VBScript in HTML: Off

Frame or IFrame tags in HTML: Off

Object tags in HTML: Off

Embed tags in HTML: Off

Form tags in HTML:

FIGURE 4-25 Advanced Options

You can configure the policy to increase the spam score if the message includes the following types of links or URLs:

- **Image Links To Remote Sites** Triggered if the message contains HTML content with an IMG tag linked to an image on a remote site.
- **Numeric IP Address In URL** Triggered if the message has an URL with a numeric IP address.
- **URL Redirect To Other Port** Triggered if the message contains a hyperlink that redirects to a port other than port 80, port 8080, or port 443.
- **URL To .Biz Or .Info Websites** Triggered if the message contains a URL that includes the .biz or .info suffix.

You can configure the policy to mark a message as spam under the following conditions:

- **Empty Messages** Triggered if the body and subject line are both empty and there is no attachment.
- **JavaScript Or VBScript In HTML** Triggered if either JavaScript or VBScript is present in the HTML included in the message.
- **Frame Or IFrame Tags In HTML** Triggered if the HTML code in the message includes the Frame or IFrame tags.

- **Object Tags In HTML** Triggered if the HTML code in the message contains the <Object> tag.
- **Embed Tags In HTML** Triggered if the HTML code in the message contains the <Embed> tag.
- **Form Tags In HTML** Triggered if the HTML code in the message contains the <Form> tag.
- **Web Bugs In HTML** Triggered if the message contains a web bug. Web bugs are small, usually one pixel by one pixel graphic images that are used to determine whether an email message has been read.
- **Apply Sensitive Word List** Triggered if a word on the sensitive word list is present in the message. These words are associated with messages that are likely to be offensive. Administrators cannot edit the sensitive word list.
- **SPF Record: Hard Fail** Triggered if the message fails a Sender Protection Framework (SPF) check. This means that the message was received from an IP address not listed in the SPF record. Used by organizations concerned about phishing messages.
- **Conditional Sender ID Filtering: Hard Fail** Triggered if the message fails a conditional sender ID check, which combines an SPF check with a Sender ID check to protect against messages where the sender header is forged.
- **NDR Backscatter** If you don't enable this setting, Non Delivery Reports (NDRs) go through spam filtering.

> ***MORE INFO*** **ADVANCED SPAM FILTERING OPTIONS**
>
> **You can learn more about advanced spam filtering options at *https://technet.microsoft.com/en-us/library/jj200750(v=exchg.150).aspx.***

Spam confidence levels

When a new message passes through the Exchange Online spam filtering algorithms, it is assigned a spam score. This spam score maps to a Spam Confidence Level (SCL) rating and is stamped in an X-Header for the message. Exchange Online performs actions on messages based on the SCL rating.

TABLE 4-1 SCL ratings

SCL rating	Meaning	Action
-1	Message coming from a sender, recipient, or IP address listed as trusted	Delivered to recipient
0,1	Message unlikely to be spam	Delivered to recipient
5,6	Message likely to be spam	Determined by filter policy setting for spam
7,8,9	Message very likely to be spam	Determined by filter policy setting for high confidence spam

You can have Exchange manually set an SCL rating for a message using a transport rule, but transport rules are not addressed by the 70-347 exam.

MORE INFO **SPAM CONFIDENCE LEVELS**

You can learn more about spam confidence levels at: *https://technet.microsoft.com/en-us/library/JJ200686(v=EXCHG.150).aspx*.

Applying spam filter policies

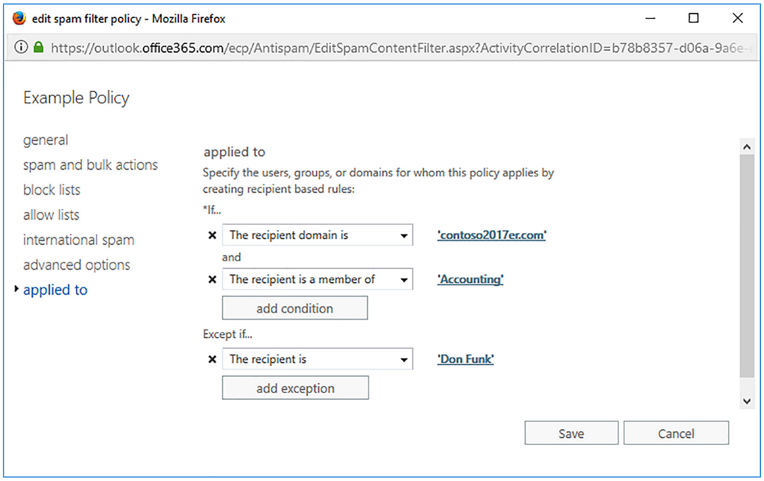
When creating a new custom spam filter policy, you need to configure the Applied To setting. This setting determines which recipients the policy applies. This setting takes the form of an If statement with a condition and exceptions. As is the case with anti-malware policies, the If conditions can include:

- The Recipient Is
- The Recipient Domain Is
- The Recipient Is A Member Of

The exceptions are the same and include:

- The Recipient Is
- The Recipient Domain Is
- The Recipient Is A Member Of

You can create as many conditions as you want, as long as those conditions are unique. For example, Figure 4-26 shows a set of condition that will apply if the recipient domain is contoso2017er.com, the recipient is a member of the Accounting group, and the recipient is not Don Funk.



edit spam filter policy - Mozilla Firefox

https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=b78b8357-d06a-9a6e-

Example Policy

applied to

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is 'contoso2017er.com'

and

The recipient is a member of 'Accounting'

Except if...

The recipient is 'Don Funk'

FIGURE 4-26 Applied To

Spam filter Windows PowerShell cmdlets

You can use the following PowerShell commands to configure spam filter policies:

- **Get-HostedContentFilterPolicy** This allows you to view existing spam filter settings.
- **Set-HostedContentFilterPolicy** Use this cmdlet to edit spam filter settings, including the recipients to which the spam filter policy applies.
- **New-HostedContentFilterPolicy** Use this cmdlet to create a new custom spam filter policy.
- **Remove-HostedContentFilterPolicy** This cmdlet allows you to remove a custom spam filter policy.

Outbound spam policy

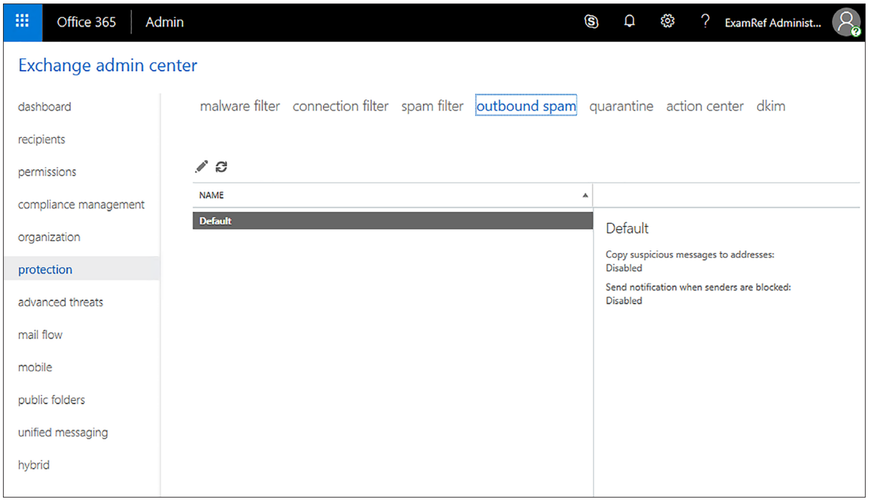
The Outbound Spam policy blocks users inside of the organization from sending spam to recipients outside of the organization. If an outbound message is suspected to be spam, it is sent through the higher risk delivery pool. Using the higher risk delivery pool reduces the likelihood that the IP address of the normal outbound delivery pool will be added to a block list by real-time block list providers.

By configuring the default Outbound Spam policy, you can specify whether:

- A copy of all suspicious messages is forwarded to one or more email addresses for review.
- A notification is sent to one or more email addresses when a sender is blocked for sending outbound spam.

You can configure the default outbound spam policy by performing the following steps:

1. In the Office 365 Admin Center, click Exchange under Admin Centers.
2. In Exchange Admin Center, click Protection, and then click Outbound Spam.
3. Ensure that the Default policy is selected, as shown in Figure 4-27, and then click the Edit (Pencil) icon.



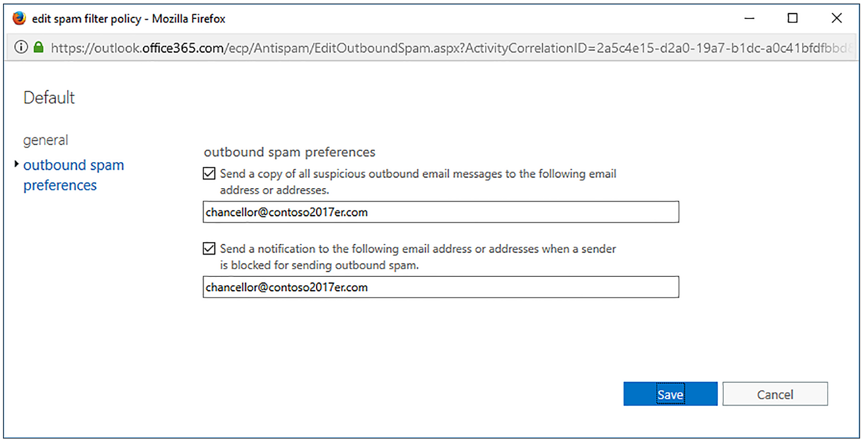
Default

Copy suspicious messages to addresses:
Disabled

Send notification when senders are blocked:
Disabled

FIGURE 4-27 Default Outbound Spam policy

4. On the Outbound Spam Preferences page, shown in Figure 4-28, configure whether a copy of all suspicious messages is forwarded to one or more email addresses for review, and whether a notification is sent to one or more email addresses when a sender is blocked for sending outbound spam.


edit spam filter policy - Mozilla Firefox
https://outlook.office365.com/ecp/Antispam/EditOutboundSpam.aspx?ActivityCorrelationID=2a5c4e15-d2a0-19a7-b1dc-a0c41bfdfbbd
Default
general
outbound spam preferences
Save
Cancel

outbound spam preferences

☑ Send a copy of all suspicious outbound email messages to the following email address or addresses.

chancellor@contoso2017er.com

☑ Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam.

chancellor@contoso2017er.com

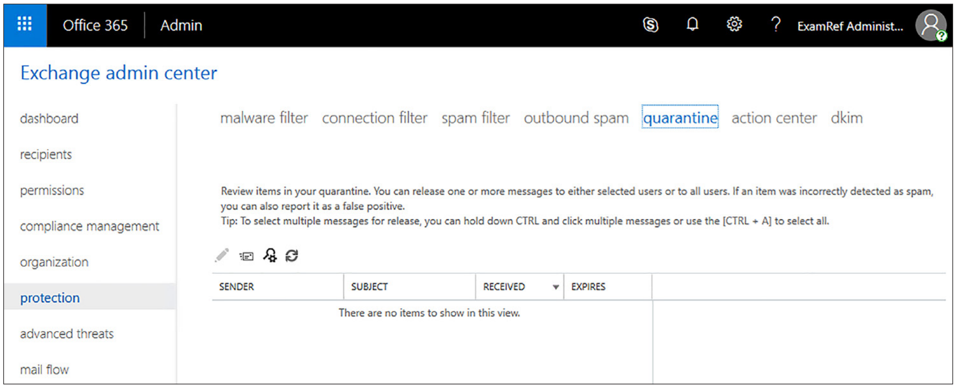
FIGURE 4-28 Outbound Spam Preferences

MORE INFO **OUTBOUND SPAM POLICY**

You can learn more about the outbound spam policy at: *https://technet.microsoft.com/en-us/library/jj200737(v=exchg.150).aspx*.

Quarantine

Content filtering can be configured to send messages to Quarantine rather than to a recipient's junk email folder, or to simply delete them. Messages sent to Quarantine can be viewed in the Quarantine section of the Exchange Admin Center, as shown in Figure 4-29. Messages in Quarantine remain there until released by an administrator or until they are automatically deleted when the Quarantine period expires. The maximum Quarantine period for messages recognized as spam is 15 days.



Review items in your quarantine. You can release one or more messages to either selected users or to all users. If an item was incorrectly detected as spam, you can also report it as a false positive.

Tip: To select multiple messages for release, you can hold down CTRL and click multiple messages or use the [CTRL + A] to select all.

SENDER	SUBJECT	RECEIVED	EXPIRES

There are no items to show in this view.

FIGURE 4-29 Quarantine

Administrators can use the Quarantine section of the Exchange Admin Center to search for quarantined messages and to release messages to their intended recipients. When releasing a message, an administrator can choose between the following options:

- **Release The Message Without Reporting It As A False Positive** When you select this option, you can choose to release the message to some or all of the message's original recipients.
- **Release The Message And Report It As A False Positive** If you choose this option, the message is released to all recipients. The message is also reported to the Microsoft Spam Analysis team, which might use the false positive result to adjust content filter rules across Exchange Online.

You can use the following Windows PowerShell cmdlets to manage quarantine:

- **Get-QuarantineMessage** Allows you to search for messages in quarantine. For example use the following command to find all messages from the adatum.com email domain:

```
Get-QuarantineMessage | ? {$_.Senderaddress -like "*@adatum.com"}
```

- **Release-QuarantineMessage** Allows you to release a message from quarantine. Use the `ReleaseToAll` parameter to allow the message.

MORE INFO **QUARANTINE**

You can learn more about quarantine at: *https://technet.microsoft.com/en-us/library/jj200776(v=exchg.150).aspx*.

Advanced Threat Protection

Advanced Threat Protection (ATP) provides Office 365 with the ability to protect your organization from attacks through email. ATP analyzes email messages and their attachments for malicious content. There are three primary methods through which ATP provides protection, safe links, safe attachments, and spoof intelligence. ATP is available for Office 365 Enterprise E5 subscriptions.

MORE INFO **ADVANCED THREAT PROTECTION**

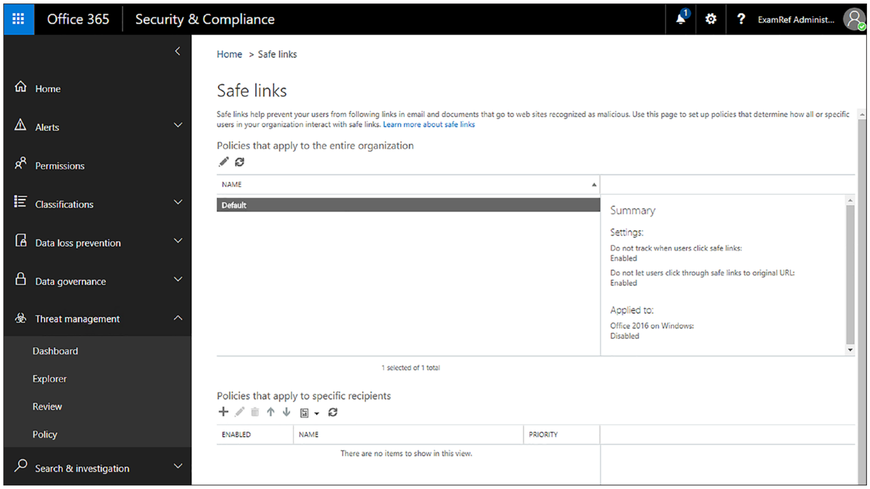
You can learn more about Advanced Threat Protection at *https://support.office.com/en-ie/article/Office-365-Advanced-Threat-Protection-overview-e100fe7c-f2a1-4b7d-9e08-622330b83653?ui=en-US&rs=en-IE&ad=IE*.

Safe links policies

Safe links policies allow you to protect your organization from URLs in messages or attached Office documents that might be used for phishing and other attacks. When you configure a safe link policy, URLs that Microsoft knows to be malicious are blocked as well as any custom URLs that you add to a safe link policy. To configure a safe links policy, the user creating the policy must be a member of the Hygiene Management or Organization Management role groups.

To configure a safe link policy that applies to the entire organization, perform the following steps:

1. In the Office 365 Admin Center, click Security And Compliance under Admin Centers.
2. In the Security & Compliance Center, under Thread Management, choose Policy. Click Safe Links.
3. In the Safe Links policies area, select the Default policy, shown in Figure 4-30, and click the Edit (pencil) icon.



Home > Safe links

Safe links

Safe links help prevent your users from following links in email and documents that go to web sites recognized as malicious. Use this page to set up policies that determine how all or specific users in your organization interact with safe links. Learn more about safe links

Policies that apply to the entire organization

NAME
Default

Summary

Settings:

Do not track when users click safe links:
Enabled

Do not let users click through safe links to original URL:
Enabled

Applied to:

Office 2016 on Windows:
Disabled

1 selected of 1 total

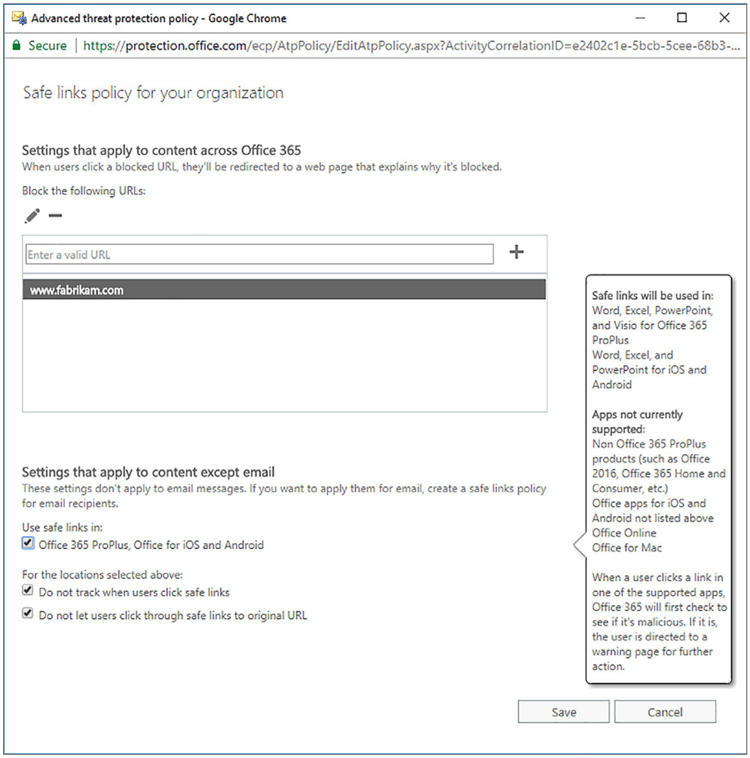
Policies that apply to specific recipients

ENABLED	NAME	PRIORITY

There are no items to show in this view.

FIGURE 4-30 Safe links

4. In the Safe Links Policy For Your Organization dialog box, shown in Figure 4-31, choose from the following options:


Advanced threat protection policy - Google Chrome
Secure
https://protection.office.com/ecp/AtpPolicy/EditAtpPolicy.aspx?ActivityCorrelationID=e2402c1e-5bcb-5cee-68b3-...
Save
Cancel

Safe links policy for your organization

Settings that apply to content across Office 365

When users click a blocked URL, they'll be redirected to a web page that explains why it's blocked.

Block the following URLs:

Enter a valid URL

www.fabrikam.com

Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

☑ Office 365 ProPlus, Office for iOS and Android

For the locations selected above:

☑ Do not track when users click safe links

☑ Do not let users click through safe links to original URL

Safe links will be used in:
Word, Excel, PowerPoint, and Visio for Office 365 ProPlus
Word, Excel, and PowerPoint for iOS and Android

Apps not currently supported:
Non Office 365 ProPlus products (such as Office 2016, Office 365 Home and Consumer, etc.)
Office apps for iOS and Android not listed above
Office Online
Office for Mac

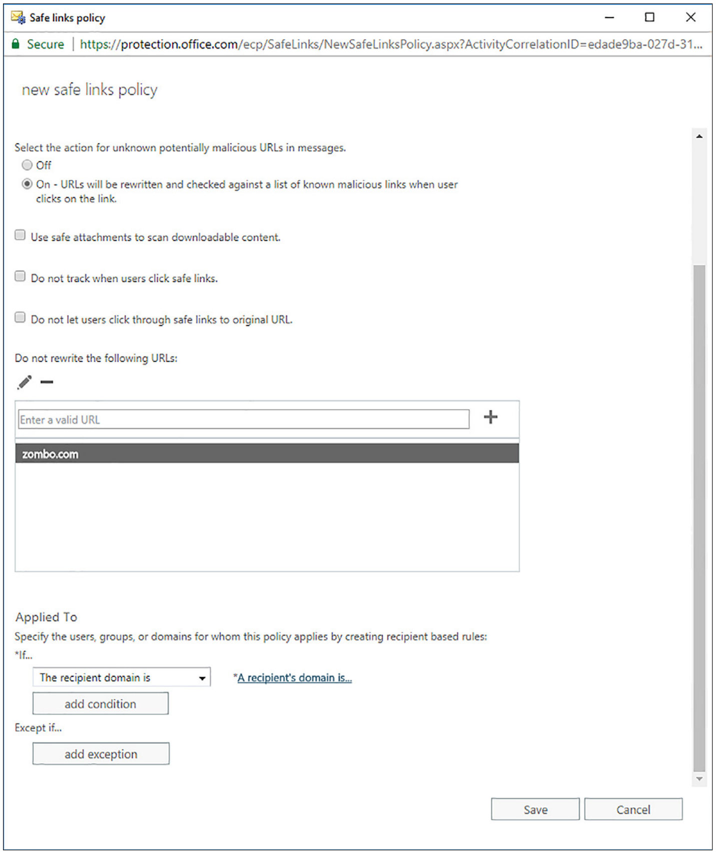
When a user clicks a link in one of the supported apps, Office 365 will first check to see if it's malicious. If it is, the user is directed to a warning page for further action.

FIGURE 4-31 Safe links policy

- **Block The Following URLS** Allows you to block a custom set of addresses in addition to URLs known to be malicious.
- **Office 365 ProPlus, Office For iOS And Android** ATP safe link policies apply to hyperlinks in documents open in Office 365 applications.
- **Do Not Track When Users Click Safe Links** Data about URLs that are encountered by ATP is not stored.
- **Don’t Let Users Click Through Safe Links To Original URLs** Blocks users form clicking past the ATP warning to the URL that has been blocked.

5. Click Save.

You can also configure safe link policies that apply to specific users rather than to the entire organization. To configure a safe link policy that applies to a specific set of recipients, in the Policies that apply to specific recipients section, create a new policy and specify the recipients. Recipient policies override the default policy that applies to all recipients. You can choose from the following options shown in Figure 4-32:


Safe links policy
Secure | https://protection.office.com/ecp/SafeLinks/NewSafeLinksPolicy.aspx?ActivityCorrelationID=edade9ba-027d-31...

new safe links policy

Select the action for unknown potentially malicious URLs in messages.

○ Off

● On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

□ Use safe attachments to scan downloadable content.

□ Do not track when users click safe links.

□ Do not let users click through safe links to original URL.

Do not rewrite the following URLs:

Enter a valid URL

zombo.com

Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*If...

The recipient domain is ▾ *A recipient's domain is...

Except if...

FIGURE 4-32 Safe links policy for specific recipients

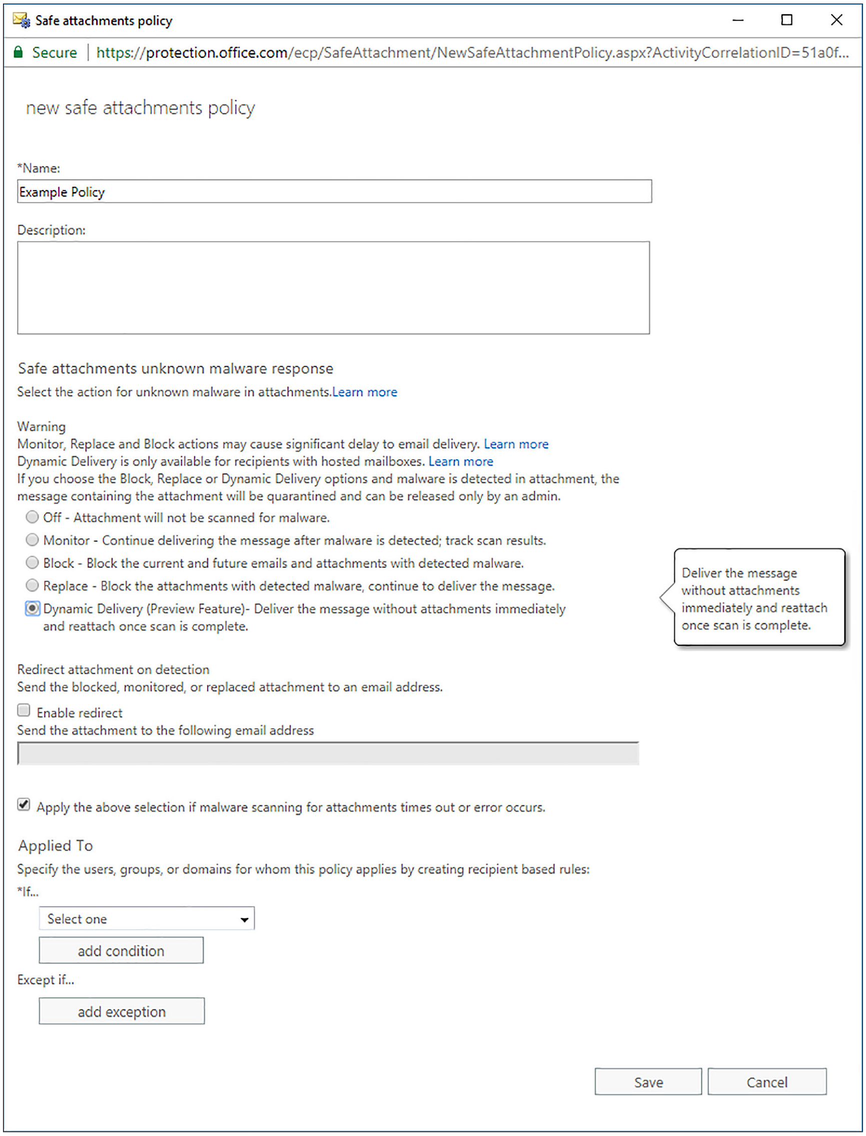
- **Off** Will not scan links in email messages. Use when you want to exempt a user from a safe links policy.
- **On** Rewrites URLs so that users are routed through ATP safe link protection. This service compares the URL with Microsoft's list of malicious URLs as well as the custom block list.
- **Use Safe Attachments To Scan Downloadable Content** Hyperlinks in attachments are scanned and compared against ATP safe links.
- **Do Not Track When User Clicks Safe Links** Click data for URLs is not stored.
- **Don't Let Users Click Through Safe Links To Original URLs** Blocks users form clicking past the ATP warning to the URL that has been blocked.
- **Do Not Rewrite The Following URLs** Leaves specific URLs as they presented in original message.
- **Applied To** Allows you to specify conditions under which the safe links policy applies.

MORE INFO **SAFE LINKS POLICIES**

You can learn more about safe links policies at *https://support.office.com/en-us/article/Set-up-Office-365-ATP-safe-links-policies-bdd5372d-775e-4442-9c1b-609627b94b5d*.

Safe attachments policies

Safe attachment policies allow Office 365 administrators to manage how attachments that may contain malware might be treated. Safe attachment policies are configured for specific recipients and take precedence over the default malware policies. Like safe link policies, safe attachments policies are only available with an Office 365 Enterprise E5 subscription. A safe attachment policy is shown in Figure 4-33.


Safe attachments policy
Secure | https://protection.office.com/ecp/SafeAttachment/NewSafeAttachmentPolicy.aspx?ActivityCorrelationID=51a0f...

new safe attachments policy

*Name:
Example Policy

Description:

Safe attachments unknown malware response
Select the action for unknown malware in attachments.Learn more

Warning
Monitor, Replace and Block actions may cause significant delay to email delivery. Learn more
Dynamic Delivery is only available for recipients with hosted mailboxes. Learn more
If you choose the Block, Replace or Dynamic Delivery options and malware is detected in attachment, the message containing the attachment will be quarantined and can be released only by an admin.

○ Off - Attachment will not be scanned for malware.
○ Monitor - Continue delivering the message after malware is detected; track scan results.
○ Block - Block the current and future emails and attachments with detected malware.
○ Replace - Block the attachments with detected malware, continue to deliver the message.
● Dynamic Delivery (Preview Feature)- Deliver the message without attachments immediately and reattach once scan is complete.

Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.
☐ Enable redirect
Send the attachment to the following email address

☑ Apply the above selection if malware scanning for attachments times out or error occurs.

Applied To
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:
*If...
Select one

Except if...

FIGURE 4-33 Safe attachments policy

The options in a safe attachment policy includes the following option:

- **Off** Do not scan attachments from internal senders for malware.
- **Monitor** Delivers messages that have attachments identified as containing malware. Monitors what happens next.

- **Block** Blocks messages identified as containing malware. Malware is sent to quarantine for review. Future messages and attachments containing the same identified malware are automatically blocked.
- **Replace** Removes attachments identified as containing malware. Message body is delivered.
- **Dynamic Delivery** Message body is delivered immediately, attachments are delivered after being scanned and deemed safe.
- **Enable Redirect** Forwards problematic attachments to a specific email address.

MORE INFO **SAFE ATTACHMENTS POLICIES**

You can learn more about safe attachments policies at: *https://support.office.com/en-ie/article/Set-up-ATP-safe-attachments-policies-in-Office-365-078eb946-819a-4e13-8673-fe-0c0ad3a775*.

EXAM TIP

Remember the Windows PowerShell cmdlets used to manage anti-malware policies and spam settings.

Skill 4.2: Recommend a mailbox migration strategy

This skill deals with migrating mailboxes from an on-premises messaging solution, which in most cases will be Microsoft Exchange, to Exchange Online. To master this skill, you'll need to understand the different migration options and the conditions why you would choose one migration method over another.

This skill covers the following topics:

- Remote move migration
- Staged migration
- Cutover migration
- IMAP migration
- Migration comparison

Remote move migration method

You use a remote move migration when you have an Exchange hybrid deployment. A hybrid deployment is where you have coexistence between an on-premises Exchange deployment and an Exchange Online deployment. You have to use a hybrid deployment and use the remote move migration method when you need to migrate more than 2,000 Exchange Server 2010, Exchange Server 2013, or Exchange Server 2016 mailboxes to Exchange Online.

With a hybrid deployment, you get the following advantages:

- User accounts are managed through your on-premises tools.
- Directory synchronization connects your on-premises Exchange organization with Exchange Online.
- Users are able to use single-sign on to access their mailbox whether the mailbox is hosted in the on-premises Exchange organization or Exchange Online.
- Email is routed securely between the on-premises Exchange deployment and Exchange Online.
- Free/busy calendar sharing between users with mailboxes hosted in the on-premises Exchange organization and mailboxes hosted in Exchange Online.

Prior to performing a remote move migration you need to ensure the following prerequisites are met:

- A hybrid deployment has already been configured between your on-premises Exchange organization and Exchange Online.
- You need to have been assigned the appropriate permissions. For mailbox moves in a hybrid deployment, this means that you need to have an account that is a member of the Organization Management, or the Recipient Management role groups.
- You need to have deployed the Mailbox Replication Proxy Service (MRSProxy) on all on-premises Exchange 2013 or Exchange 2016 Client Access servers.

Once these prerequisites have been met, you can move mailboxes from your on-premises Exchange deployment to Exchange Online by performing the following steps:

1. **Create migration endpoint** Migration endpoints host connection settings for an on-premises Exchange server running the MRS proxy service.
2. **Enable MRSProxy service** The MRSProxy service is hosted on on-premises Client Access servers. This service can be enabled using Exchange Administration Console by selecting the Client Access server, editing the properties of the EWS virtual directory, and ensuring that the MRS Proxy enabled check box is selected.
3. **Move mailboxes** You can move mailboxes using the Office 365 tab in EAC on the on-premises Exchange server by creating a new migration batch in Exchange Admin Console, or by using Windows PowerShell. When moving mailboxes, you move some, not all mailboxes, at a time in groups, which are termed batches.
4. **Remove completed migration batches** Once migration of a batch is complete, remove the migration batch using Exchange Administration Center, or Windows PowerShell.
5. **Re-enable offline access for Outlook Web App** If users have been migrated from on-premises Exchange Server to Office 365, it is necessary to reset the offline access setting in their browser.

MORE INFO **REMOTE MOVE MIGRATION**

You can learn more about remote move migrations at: *https://support.office.com/en-us/article/Ways-to-migrate-multiple-email-accounts-to-Office-365-0a4913fe-60fb-498f-9155-a86516418842?ui=en-US&rs=en-US&ad=US#remotemove.*

Staged migration method

In a staged migration, you migrate mailboxes from your on-premises Exchange organization to Office 365 in groups, termed batches. You would select a staged migration in the following circumstances:

- Your organization has more than 2,000 on-premises mailboxes hosted in Exchange 2007.
- Your organization intends to completely move its messaging infrastructure to Office 365.
- Your available migration period is in the timeframe of several weeks to several months.
- After migration completes, you still manage user accounts using on-premises management tools and have account synchronization performed with Azure Active Directory.
- The primary domain name used for your on-premises Exchange organization must be configured as a domain associated with the tenancy in Office 365.

Staged migration involves the following general steps:

1. You create a CSV file that includes a row for every user who has an on-premises mailbox that you want to migrate. This is not every user in the organization, just those who you will migrate in a particular batch.
2. Create a staged migration batch using Exchange Admin Center, or using Windows PowerShell.
3. Trigger the migration batch. Once the migration batch is triggered, Exchange Online performs the following steps:
   - Verify that directory synchronization is enabled and functioning. Directory synchronization migrates distribution groups, contacts, and mail enabled users.
   - Verifies that a mail-enabled user exists in Office 365 for every user listed in the batch CSV file.
   - Converts the Office 365 mail-enabled user to an Exchange Online mailbox for each user in the migration batch.
   - Configures mail forwarding for the on-premises mailbox.
4. Once these steps have been completed, Exchange Online sends you a status report informing you of which mailboxes have migrated successfully and which mailboxes have not migrated successfully. Successfully migrated users can start using Exchange Online mailboxes.

5. Once migration is successful, you convert the mailboxes of successfully migrated on-premises users to mail-enabled users in the on-premises Exchange deployment.
6. You configure a new batch of users to migrate and delete the current migration batch.
7. Once all users have been migrated, the administrator assigns licenses to Office 365 users, configures MX records to point to Exchange online, and creates an Autodiscover record that points to Office 365.
8. Decommission the on-premises Exchange deployment.

MORE INFO **STAGED MIGRATION METHOD**

You can learn more about staged migrations at *https://support.office.com/en-us/article/What-you-need-to-know-about-a-staged-email-migration-to-Office-365-7e2c82be-5f3d-4e36-bc6b-e5b4d411e207*.

Cutover migration method

In a cutover migration, all mailboxes in an on-premises Exchange deployment are migrated to Office 365 in a single migration batch. Cutover migrations migrate global mail contacts as well as distribution groups. Cutover migrations are suitable when:

- You intend all mailboxes to be hosted in Office 365 when the migration completes.
- You intend to manage user accounts using Office 365 tools.
- You want to perform the migration period in less than a week.
- Your organization has less than 2,000 mailboxes.
- Your on-premises messaging solution is Exchange Server 2007 or later. Exchange Server 2003 reached the end of extended support in April 2014 and Exchange Server 2007 on April 11, 2017.
- The primary domain name used for your on-premises Exchange organization must be configured as domain associated with the tenancy in Office 365.

You can perform a cutover migration using the Exchange Admin Center or by using Windows PowerShell.

The cutover migration method involves the following general steps:

1. An administrator creates empty mail-enabled security groups in Office 365.
2. An administrator connects Office 365 to the on-premises Exchange deployment. This is also termed creating a migration endpoint.
3. An administrator creates and starts a cutover migration batch using Exchange Admin Center or Windows PowerShell.

4. Once the migration batch is triggered, Exchange Online performs the following steps:
    - The address book of the on-premises Exchange deployment is queried to identify mailboxes, distribution groups, and contacts.
    - New Exchange Online mailboxes are provisioned.
    - Distribution groups and contacts are created within Exchange Online.
    - Mailbox data, including email messages, contacts, and calendar items, are migrated from each on-premises mailbox to the corresponding Exchange Online mailbox.
5. Exchange Online forwards the administrator a report providing statistics including the number of successful and failed migrations. The migration report includes automatically generated passwords for each new Exchange Online mailbox. Users are forced to change passwords the first time they sign in to Office 365.
6. Incremental synchronization occurs every 24 hours, updating Exchange Online with any new items created in the on-premises mailboxes.
7. Once migration issues have been resolved, the administrator changes the MX records to point to Exchange Online.
8. Once mail flow to Exchange Online has been successfully established, the administrator deletes the cutover migration batch. This terminates synchronization between the on-premises mailboxes and Office 365.
9. Administrator performs post migration tasks, including assigning Office 365 licenses, creating an Autodiscover DNS record, and decommissioning on-premises Exchange servers.

MORE INFO **CUTOVER MIGRATION**

You can learn more about cutover migrations at: *https://support.office.com/en-us/article/What-you-need-to-know-about-a-cutover-email-migration-to-Office-365-961978ef-f434-472d-a811-1801733869da*.

IMAP migration

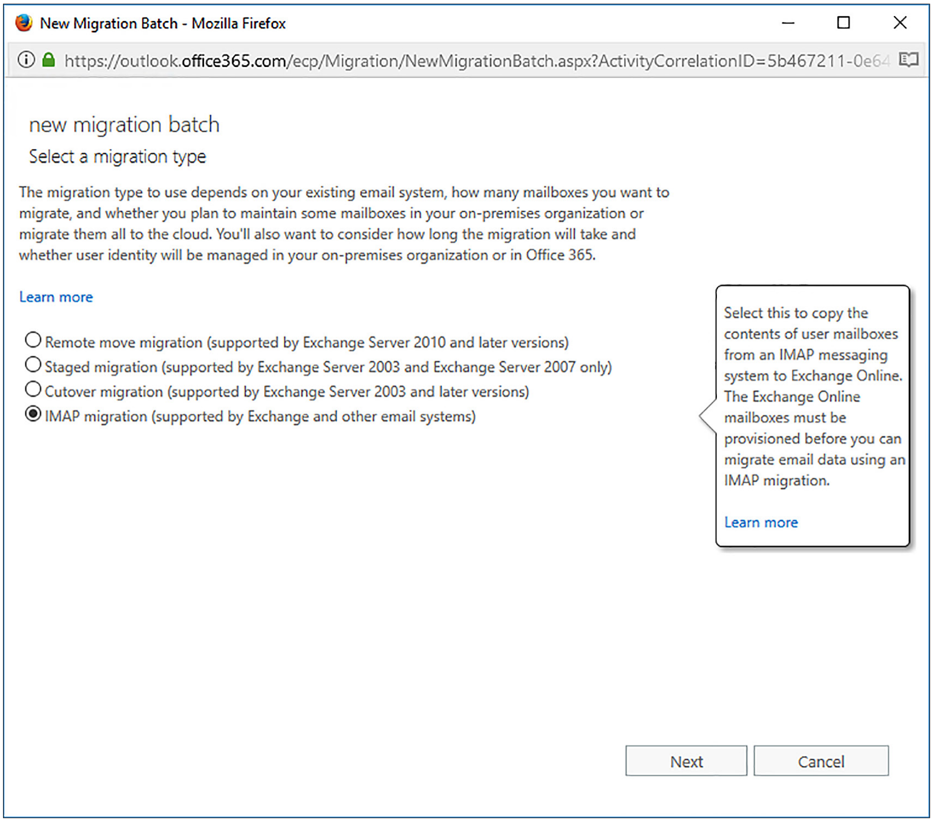
IMAP migrations use the IMAP protocol to move the contents of on-premises user mailboxes to Exchange Online. IMAP migrations are suitable where the on-premises mail server is not running Exchange Server, but is instead running an alternate mail server solution.

IMAP migration is supported for the following on-premises messaging solutions:

- Courier-IMAP
- Cyrus
- Dovecot
- UW-IMAP

IMAP migrations involve the following general steps:

1. A tenant administrator creates Office 365 user accounts and assigns them Exchange Online user licenses. This provisions the user accounts with Exchange Online mailboxes.
2. The tenant administrator creates a CSV file. This CSV file includes a row for each on-premises user who will be migrated to Exchange Online using IMAP. This CSV file needs to include the passwords used by each on-premises IMAP mailbox user. It is recommended that you reset user passwords for on-premises IMAP mailbox users to simplify this process.
3. The administrator creates and then triggers an IMAP migration batch. This can be done using the Migration dashboard, as shown in Figure 4-34, or through Windows PowerShell.


New Migration Batch - Mozilla Firefox

https://outlook.office365.com/ecp/Migration/NewMigrationBatch.aspx?ActivityCorrelationID=5b467211-0e64

new migration batch

Select a migration type

The migration type to use depends on your existing email system, how many mailboxes you want to migrate, and whether you plan to maintain some mailboxes in your on-premises organization or migrate them all to the cloud. You'll also want to consider how long the migration will take and whether user identity will be managed in your on-premises organization or in Office 365.

Learn more

○ Remote move migration (supported by Exchange Server 2010 and later versions)
○ Staged migration (supported by Exchange Server 2003 and Exchange Server 2007 only)
○ Cutover migration (supported by Exchange Server 2003 and later versions)
● IMAP migration (supported by Exchange and other email systems)

Select this to copy the contents of user mailboxes from an IMAP messaging system to Exchange Online. The Exchange Online mailboxes must be provisioned before you can migrate email data using an IMAP migration.

Learn more

FIGURE 4-34 IMAP Migration

4. Once the migration batch is initiated, the following occurs:
   - Exchange Online creates a migration request for each user in the CSV file.
   - Each migration request includes the credentials for the user in the on-premises IMAP messaging system.

- Messages from each user’s IMAP mailbox are copied to the corresponding Exchange Online mailbox until all data is migrated.

5. Exchange Online provides a status email to the administrator informing them of the status of the migration. This email contains statistics about the number of mailboxes successfully migrated, how many could not be migrated, and any error reports.
6. Exchange Online and the IMAP messaging system are synchronized every 24 hours to move any new messages from the on-premises environment to Exchange Online.
7. Once all migration issues have been resolved, the administrator updates MX records to point to Exchange Online. Once mail is flowing to Exchange Online, the administrator deletes the migration batches.

> ***MORE INFO*** **IMAP MIGRATIONS TO EXCHANGE ONLINE**
>
> **You can learn more about IMAP migrations to Exchange Online at: *https://support.office.com/en-us/article/Migrate-other-types-of-IMAP-mailboxes-to-Office-365-58890ccd-ce5e-4d94-be75-560a3b70a706***

Import service

Network upload allows you to import PST files into Office 365. This can be done either by directly uploading the files or by shipping hard drives to Microsoft and having them import data directly.

To import PST files, perform the following steps:

1. In the Data governance section of the Security & Compliance center, use the Import section to create a Shared Access Signature (SAS) key, also known as the SAS URL. This key provides the necessary permission and location to upload PST files to an Azure storage location.
2. Download and install the Azure AzCopy tool. Use AzCopy with the SAS URL to upload one or more PST files to Azure.
3. Once uploaded, review the list of PST files that have been successfully transferred to Office 365. You can do this with Azure Storage Explorer.
4. Create a mapping file that maps uploaded PST files to Office 365 mailboxes. This file must be in CSV format.
5. Create a PST import job from the Data governance section of the Security & Compliance center. You specify the mapping file when creating this job.
6. Run the job to import the data into the appropriate Office 365 mailboxes.

MORE INFO **IMPORT SERVICE**

You can learn more about the import service at: *https://support.office.com/en-us/article/Use-network-upload-to-import-your-organization-s-PST-files-to-Office-365-103f940c-0468-4e1a-b527-cc8ad13a5ea6*.

Migration comparison

Table 4-2 lists the difference between the different methods you can use to migrate from an on-premises messaging environment to Exchange Online.

TABLE 4-2 Migration type comparison

On-premises messaging environment	Number of mailboxes	Will user accounts be managed on-premises	Migration method
Exchange 2007 to Exchange 2016	Less than 2,000	No	Cutover migration
Exchange 2007	Less than 2,000	No	Staged migration
Exchange 2007	More than 2,000	Yes	Staged migration or remote move migration in hybrid deployment
Exchange 2010 or Exchange 2016	More than 2,000	Yes	Remote move migration in hybrid deployment
Non-Exchange on-premises messaging system	No maximum	Yes	IMAP migration

MORE INFO **COMPARE MIGRATION TYPES**

You can learn more about the differences between migration types at: *https://technet.microsoft.com/en-us/library/jj863291(v=exchg.150).aspx#comparetypes. Remember the conditions under which you would choose a specific migration type.*

Skill 4.3: Plan for Exchange Online

This skill deals with planning how to implement a variety of features in Exchange Online. This includes understanding what client prerequisites are required to ensure that users are able to access archive mailboxes, configuring in-place hold and litigation hold, allowing and blocking access to OWA, and allowing and blocking access to ActiveSync.

This skill covers the following topics:

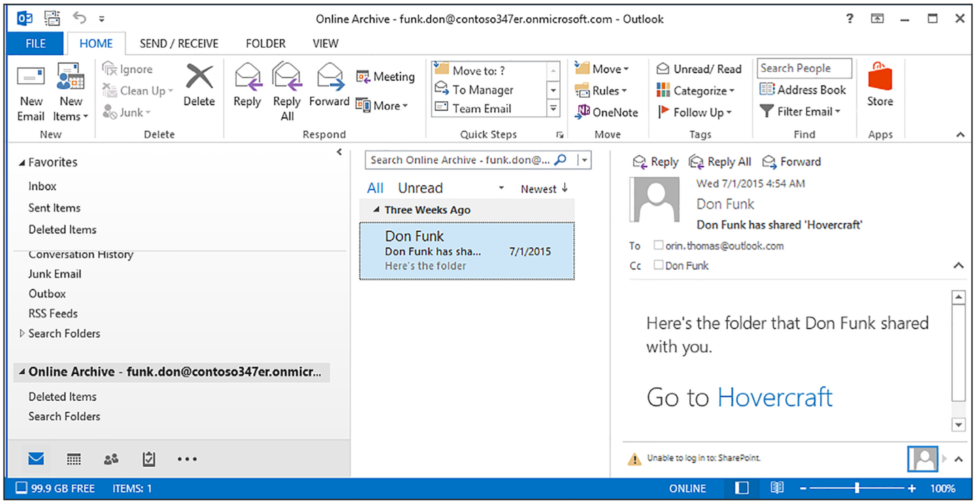
- Plan client requirements for archive
- Legal hold
- Configure OWA access
- Configure ActiveSync
- Mobile Device Management
- Data Loss Prevention

Plan client requirements for archive

In Chapter 3, “Configure Exchange Online and Skype for Business Online for end users,” you read about archive mailboxes. Users can access archive mailboxes on a computer running Outlook or Outlook Web App through a browser, but are unable to access the archive mailbox when using Outlook on a mobile device or accessing Outlook Web App through a browser on a mobile device. Archive mailboxes can be used with the following versions of Outlook:

- Outlook 2016
- Outlook 2013
- Outlook 2010
- Outlook 2007

The archive mailbox appears in Outlook as a folder, as shown in Figure 4-35.



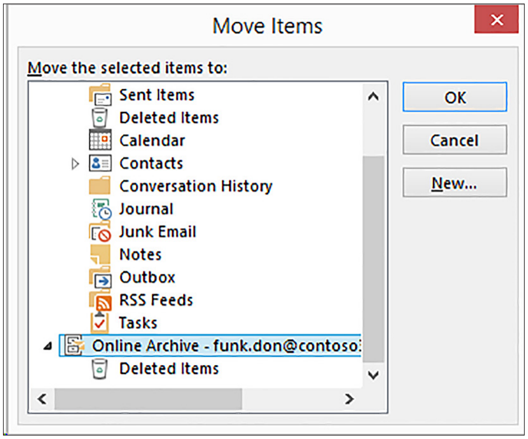
Here's the folder that Don Funk shared with you.

Go to Hovercraft

FIGURE 4-35 Move to archive mailbox

There are several methods that users can use to transfer items to the archive mailbox. These include:

- **Move messages manually** Users of clients that support archive mailboxes can manually move messages to the archive mailbox. This process is labor-intensive. Figure 4-36 shows moving an item to an archive mailbox.



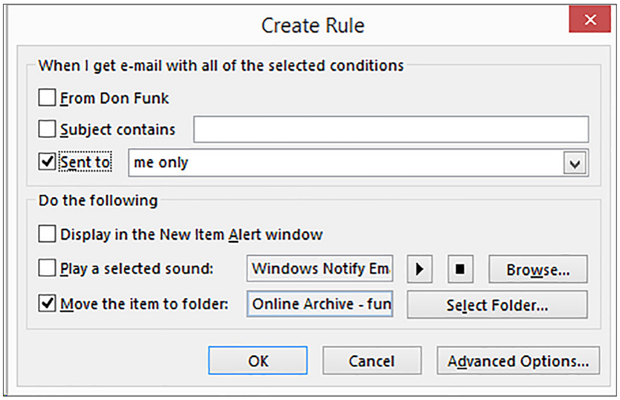
Move Items

Move the selected items to:

Sent Items
Deleted Items
Calendar
Contacts
Conversation History
Journal
Junk Email
Notes
Outbox
RSS Feeds
Tasks
Online Archive - funk.don@contoso:
Deleted Items

FIGURE 4-36 Move to archive mailbox

- **Use Inbox rules to move messages** Messages can be moved to the archive mailbox using inbox rules. This requires the user to configure the Inbox rule, as shown in Figure 4-37.



Create Rule

When I get e-mail with all of the selected conditions

☐ From Don Funk
☐ Subject contains
☑ Sent to: me only

Do the following

☐ Display in the New Item Alert window
☐ Play a selected sound: Windows Notify Em
☑ Move the item to folder: Online Archive - fun

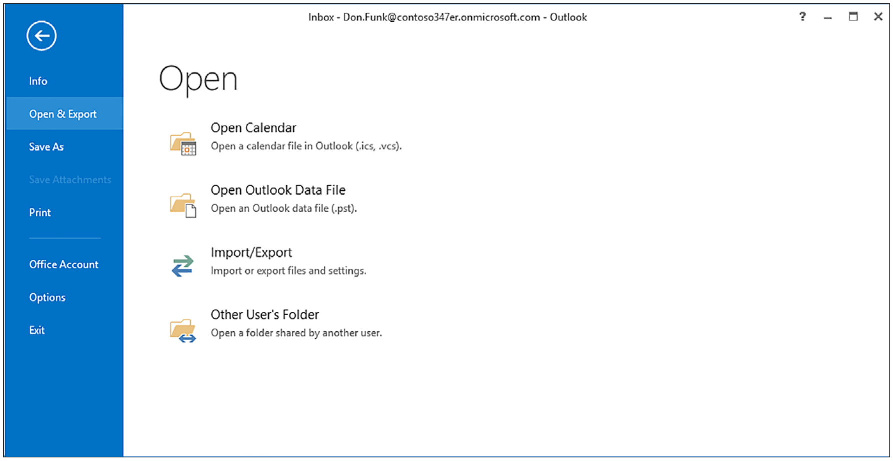
FIGURE 4-37 Create Rule

- **Have retention policies move messages** The default retention policy assigned to each Exchange Online mailbox automatically moves messages that are two years or older to the archive mailbox.
- **Importing messages from PST files** Users are able to manually import data from PST files on their local computers into the archive mailbox. Having the data stored centrally in Office 365, rather than on a specific computer, is also beneficial for users who

want to ensure that the message data in the .pst file is backed up and available on other computers.

Users can import PST files into their archive mailbox by performing the following steps:

1. In Outlook, select the Archive folder.
2. Click File, and then click Open & Export.
3. On the Open page, shown in Figure 4-38, click Import/Export.



Open

Open Calendar
Open a calendar file in Outlook (.ics, .vcs).

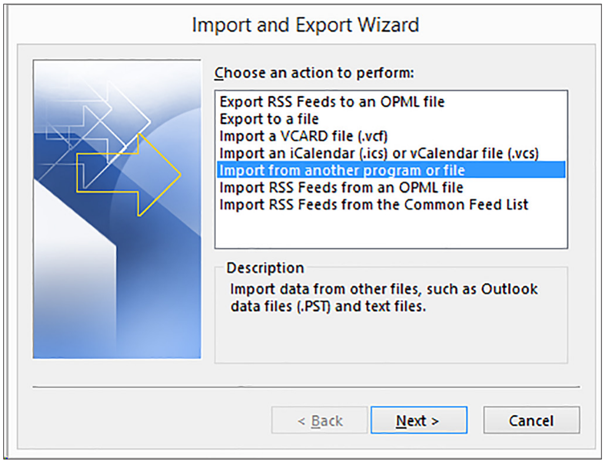
Open Outlook Data File
Open an Outlook data file (.pst).

Import/Export
Import or export files and settings.

Other User's Folder
Open a folder shared by another user.

FIGURE 4-38 Import/Export

4. On the Import And Export Wizard, click Import From Another Program Or File, as shown in Figure 4-39, and then click Next.



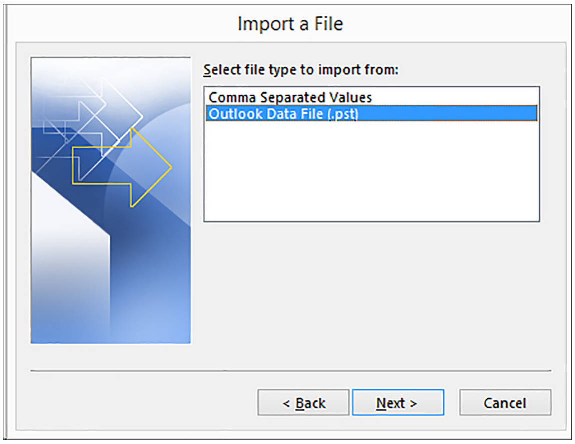
Choose an action to perform:

Export RSS Feeds to an OPML file
Export to a file
Import a VCARD file (.vcf)
Import an iCalendar (.ics) or vCalendar file (.vcs)
Import from another program or file
Import RSS Feeds from an OPML file
Import RSS Feeds from the Common Feed List

Description
Import data from other files, such as Outlook data files (.PST) and text files.

FIGURE 4-39 Import From Another Program Or File

5. On the Import A File page, select Outlook Data File (.pst), as shown in Figure 4-40, and click Next.

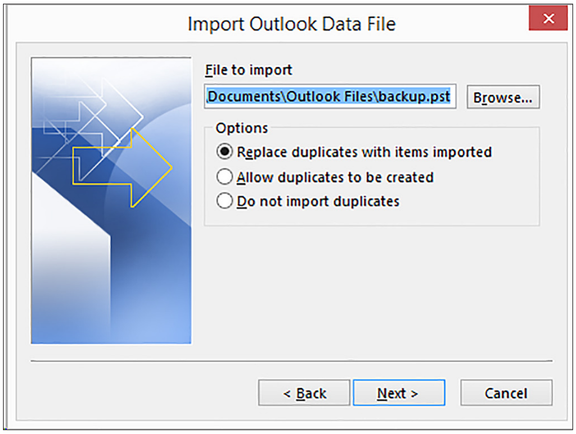


Select file type to import from:

Comma Separated Values
Outlook Data File (.pst)

FIGURE 4-40 Import Outlook Data File

6. Select the .pst file that you will import.
7. Under Options, select between the following methods of dealing with duplicates, as shown in Figure 4-41.
   - Replace Duplicates With Items Imported
   - Allow Duplicates To Be Created
   - Do Not Import Duplicates



File to import

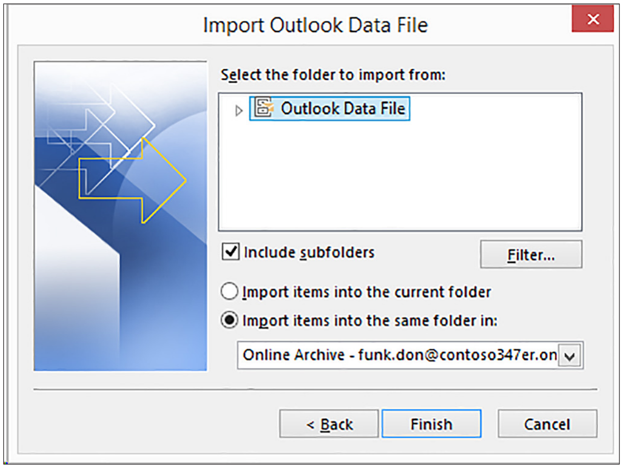
Documents\Outlook Files\backup.pst

Options

● Replace duplicates with items imported
○ Allow duplicates to be created
○ Do not import duplicates

FIGURE 4-41 Duplicate Options

8. Click Next. On the Import Outlook Data File page, ensure that the option to Import items into the same folder is set to Online Archive, as shown in Figure 4-42.



Select the folder to import from: Outlook Data File

☑ Include subfolders

○ Import items into the current folder

● Import items into the same folder in: Online Archive - funk.don@contoso347er.on

FIGURE 4-42 Import to archive

9. Click Finish.

MORE INFO **ARCHIVE MAILBOXES**

You can learn more about archive mailboxes at: ***https://technet.microsoft.com/en-us/library/dn922147(v=exchg.150).aspx***.

In-place hold and litigation hold

Litigation hold is a feature introduced in Exchange Server 2010 that allows preservation of data for eDiscovery. The feature is available in Exchange Server 2013, Exchange Server 2016, and Exchange Online. You apply litigation hold on a per-mailbox basis. For example, if you want to preserve the contents of all conversations between Don, Kim, and Dan, using the litigation hold functionality, you would need to place all three mailboxes on litigation hold.

In-place hold allows holds be applied on the basis of a query. For example, you could put an in-place hold on all conversations between Don, Kim, and Dan, but the hold would not apply to items outside the contents defined by the in-place hold query.

Enable litigation hold

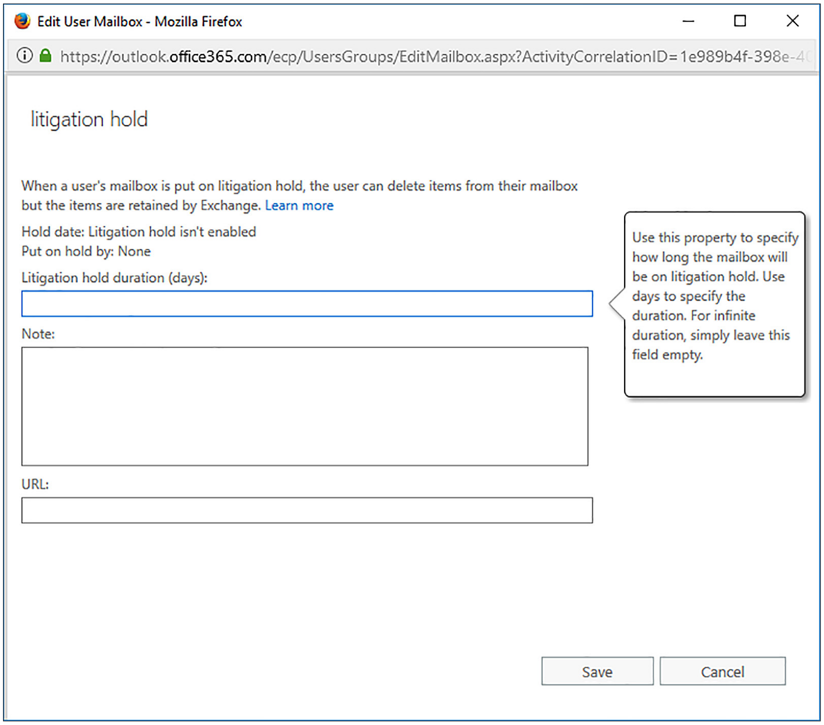
Litigation hold, also termed legal hold, is used when one or more users at an organization is subject to an internal investigation, legal discovery, or other procedure that requires the organization to preserve the stage of their Exchange Online mailbox. Litigation hold is necessary to avoid tampering with evidence. For example, if a person has sent abusive email messages from the email account associated with their Exchange Online mailbox, placing the mailbox on litigation hold ensures that any potential email messages containing abusive content will not be deleted by the person subject to the investigation.

When a mailbox is placed on litigation hold, the following occurs:

- Content in the archive mailbox is preserved.
- Original and modified versions of items are preserved.
- Deleted items are preserved for a specified period or until the hold is removed.
- Items in the recoverable items are preserved.

When a mailbox is placed on litigation hold, its storage requirements increase dramatically. Not only are deleted items stored, but so are the original versions of modified items, as well as the modified versions. To ensure that all items are kept and the mailbox remains functional, the quota applied to the recoverable items folder is increased from 30 GB to 100 GB. Even though the quota on the recoverable items folder is increased, Microsoft recommends that administrators monitor mailboxes placed on litigation hold to ensure that issues related to the exhaustion of applied quotas do not arise.

When you place a mailbox on litigation hold you can specify the duration of the hold. The person requesting the litigation hold should specify whether the litigation hold will be of a specific duration or indefinite. You should also ensure that documentation requesting the implementation of the hold is in order because a company's human resources or legal department usually requests litigation hold. To leave the mailbox on litigation hold indefinitely, leave the litigation hold duration field empty, as shown in Figure 4-43.


Edit User Mailbox - Mozilla Firefox
https://outlook.office365.com/ecp/UsersGroups/EditMailbox.aspx?ActivityCorrelationID=1e989b4f-398e-4
litigation hold

When a user's mailbox is put on litigation hold, the user can delete items from their mailbox but the items are retained by Exchange. Learn more

Hold date: Litigation hold isn't enabled
Put on hold by: None

Litigation hold duration (days):

Note:

URL:

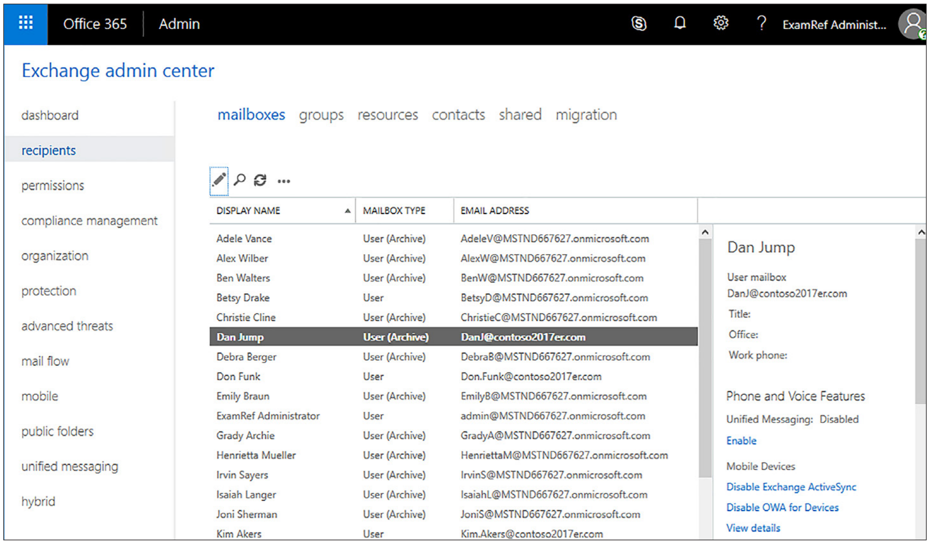
Use this property to specify how long the mailbox will be on litigation hold. Use days to specify the duration. For infinite duration, simply leave this field empty.

FIGURE 4-43 Litigation Hold

It is important to note that litigation hold can take up to 60 minutes to be enforced. You need to take this period into account in scenarios where you need to immediately preserve the contents of a mailbox and you suspect that the person subject to the litigation hold might attempt to scrub evidence. You should talk to your organization's human resources department about putting policies in place that provide enough time for a litigation hold to be enacted before the person subject to that hold is informed that this has occurred.

To put an Exchange Online mailbox on litigation hold, perform the following steps:

1. In the Recipients section of Exchange Admin Center, select the Mailboxes area, and then select the mailbox of the user for which you wish to configure a litigation hold. Figure 4-44 shows the Dan Jump mailbox selected.



DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Adele Vance	User (Archive)	AdeleV@MSTND667627.onmicrosoft.com
Alex Wilber	User (Archive)	AlexW@MSTND667627.onmicrosoft.com
Ben Walters	User (Archive)	BenW@MSTND667627.onmicrosoft.com
Betsy Drake	User	BetsyD@MSTND667627.onmicrosoft.com
Christie Cline	User (Archive)	ChristieC@MSTND667627.onmicrosoft.com
Dan Jump	User (Archive)	DanJ@contoso2017er.com
Debra Berger	User (Archive)	DebraB@MSTND667627.onmicrosoft.com
Don Funk	User	Don.Funk@contoso2017er.com
Emily Braun	User (Archive)	EmilyB@MSTND667627.onmicrosoft.com
ExamRef Administrator	User	admin@MSTND667627.onmicrosoft.com
Grady Archie	User (Archive)	GradyA@MSTND667627.onmicrosoft.com
Henrietta Mueller	User (Archive)	HenriettaM@MSTND667627.onmicrosoft.com
Irvin Sayers	User (Archive)	IrvinS@MSTND667627.onmicrosoft.com
Isaiah Langer	User (Archive)	IsaiahL@MSTND667627.onmicrosoft.com
Joni Sherman	User (Archive)	JoniS@MSTND667627.onmicrosoft.com
Kim Akers	User	Kim.Akers@contoso2017er.com

Dan Jump

User mailbox
DanJ@contoso2017er.com

Title:

Office:

Work phone:

Phone and Voice Features

Unified Messaging: Disabled

Enable

Mobile Devices

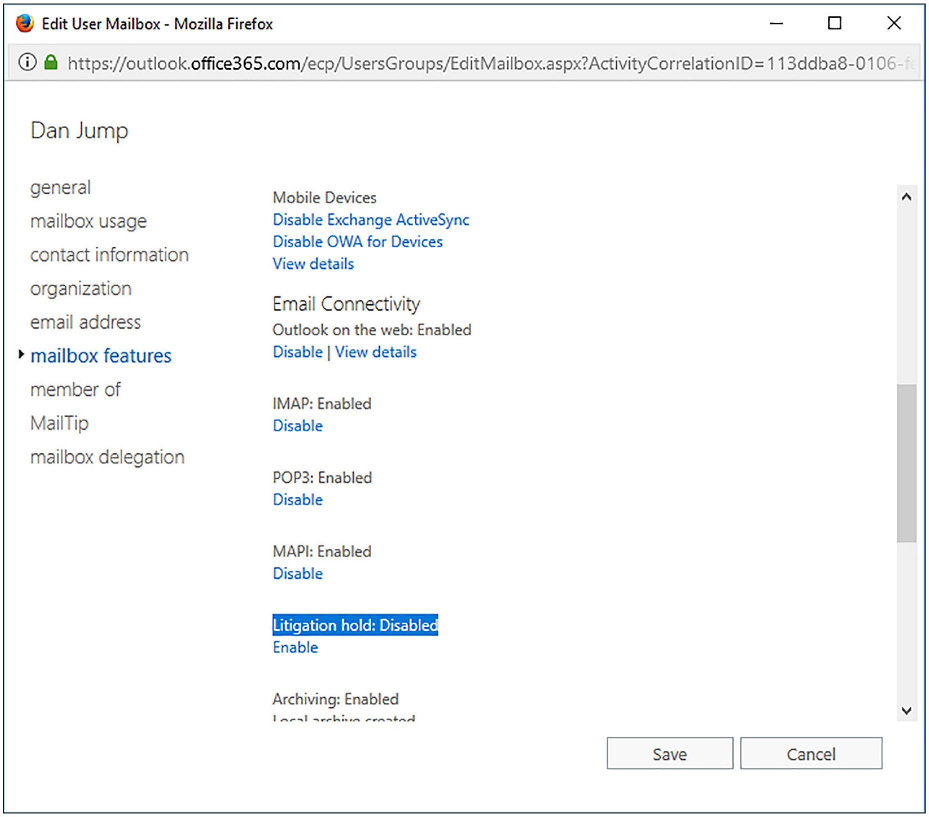
Disable Exchange ActiveSync

Disable OWA for Devices

View details

FIGURE 4-44 List of Mailboxes

2. Click the Edit (Pencil) icon to access the Mailbox Properties page.
3. On the Mailbox Properties page, click Mailbox Features.
4. Under Litigation Hold: Disabled, shown in Figure 4-45, click Enable.



Dan Jump

Mobile Devices

Email Connectivity

Outlook on the web: Enabled

IMAP: Enabled

POP3: Enabled

MAPI: Enabled

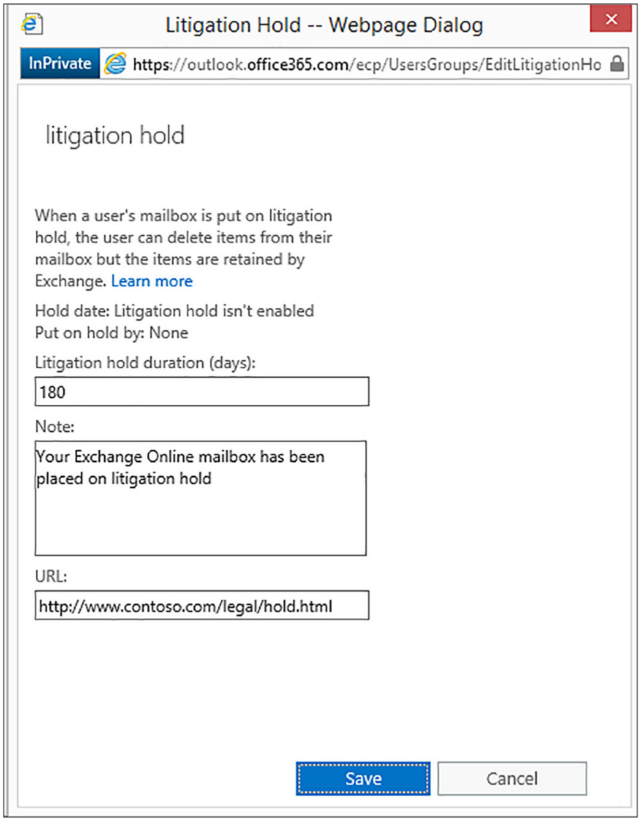
Litigation hold: Disabled

Archiving: Enabled

Local archive created

FIGURE 4-45 Enable Litigation Hold from Mailbox Features

5. On the Litigation Hold dialog box, shown in Figure 4-46, enter the litigation hold duration. If the litigation hold is to be indefinite, ensure that you do not enter a figure in this field. You can also provide a note about the litigation hold and a URL, which is used to inform the user that their mailbox has been placed on hold. You can also provide a URL to provide the user with more information. Click Save to enact the litigation hold.


Litigation Hold -- Webpage Dialog
InPrivate
https://outlook.office365.com/ecp/UsersGroups/EditLitigationHo

litigation hold

When a user's mailbox is put on litigation hold, the user can delete items from their mailbox but the items are retained by Exchange. Learn more

Hold date: Litigation hold isn't enabled
Put on hold by: None

Litigation hold duration (days):
180

Note:
Your Exchange Online mailbox has been placed on litigation hold

URL:
http://www.contoso.com/legal/hold.html

FIGURE 4-46 180-day Litigation Hold

6. Click Save on the User Mailbox properties page to enact the litigation hold.

If the Office 365 user account associated with a mailbox that is placed on litigation hold is deleted, the mailbox is converted into an inactive mailbox. Inactive mailboxes store the contents of the deleted user's mailbox and retain all mailbox items for the duration of the hold at the time when the hold was applied. For example, if a 90-day hold is placed on a mailbox, and the Office 365 user account is deleted five days later, the contents of the inactive mailbox will be preserved for another 85 days. Inactive mailboxes are unable to receive new email messages and are not displayed in address books or other lists.

Remove litigation hold

Removing a user from litigation hold means that all deleted items that have exceeded their retention period will be purged. The original versions of items that have since been modified will also be deleted once litigation hold is removed. Once litigation hold is removed, the quota on the recoverable items folder will also return to 30 GB from 100 GB.

To remove a user from litigation hold, perform the following steps:

1. In the Recipients section of Exchange Admin Center, select the mailboxes area, and then select the mailbox of the user for which you wish to remove the litigation hold.
2. Click the Edit (Pencil) icon.
3. In the Mailbox Features section of the mailbox properties dialog box click Disable under Litigation Hold: Enabled.
4. On the Warning dialog box, warning you that you are about to disable litigation hold, click Yes.
5. Click Save to apply the change to the user's mailbox.

Manage litigation hold with PowerShell

You use the Set-Mailbox Windows PowerShell cmdlet to place a mailbox on litigation hold. For example, to place the mailbox don.funk@contoso2017er.com on indefinite litigation hold, issue the following command:

```
Set-Mailbox don.funk@contoso2017er.com –LitigationHold $True
```

You can use the `LitigationHoldDuration` parameter to configure a duration for the litigation hold. For example, to place the kim.akers@contoso2017er.com mailbox on litigation hold for 180 days, issue the following command:

```
Set-Mailbox kim.akers@contoso2017er.com –LitigationHold $True –LitigationDuration 180
```

You can use a combination of the Get-Mailbox and the Set-Mailbox cmdlets to put all of the mailboxes in the organization on litigation hold. You might need to do this if your organization is subject to litigation and the contents of all user mailboxes must be preserved. For example, to place all user mailboxes in the organization on hold for a period of 90 days, issue the following Windows PowerShell cmdlet:

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} |
Set-Mailbox -LitigationHoldEnabled $true -LitigationHoldDuration 90
```

You can remove a mailbox from litigation hold using the Set-Mailbox Windows PowerShell cmdlet. For example, to remove the litigation hold on the mailbox don.funk@contoso2017er.com, issue the following command:

```
Set-Mailbox don.funk@contoso2017er.com –LitigationHoldEnabled $False
```

MORE INFO **LITIGATION HOLD**

You can learn more about litigation hold at: *https://technet.microsoft.com/en-us/library/dn790612.aspx*.

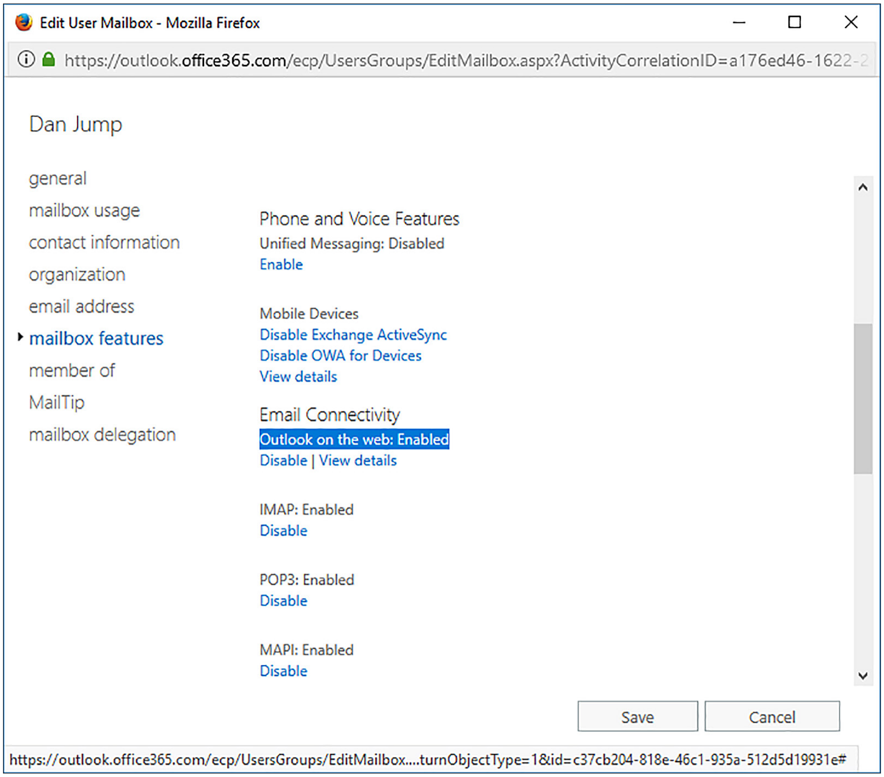
Configure OWA access

Outlook Web App (OWA), also termed Outlook On The Web, allows users to access their Office 365 Exchange Online mailbox through a web browser. While a large number of Office 365 users access their Exchange Online mailbox through the Outlook client software on their computer or mobile device, in some scenarios, such as when they are using a kiosk computer in an airport, they will want to access their mailbox through a web browser.

Allowing access to Office 365 Exchange Online mailboxes through OWA does provide users with convenience, but also exposes the organization to risk. Many users do not exercise due care when using computers in airports or Internet cafés. There are many instances where user credentials have been captured by malware installed on these computers provided for public use. These credentials can be used at a later point in time by attackers to access organizational data because they can gain access to OWA or even a user's Office 365 subscription. For this reason, many organizations disable OWA. Because smartphone users are able to access Office 365 Exchange Online mailboxes through the Outlook app, available in each vendor's App Store, fewer users require access to OWA when away from their trusted computers.

To disable OWA, perform the following steps:

1. In the Recipients area of the Exchange Admin Center, select the user for which you wish to disable ActiveSync.
2. Click the Edit (Pencil) icon.
3. In the Mailbox Features section, click Disable under Outlook On The Web: Enabled, as shown in Figure 4-47.



Edit User Mailbox - Mozilla Firefox

https://outlook.office365.com/ecp/UsersGroups/EditMailbox.aspx?ActivityCorrelationID=a176ed46-1622-2

Dan Jump

Phone and Voice Features

Unified Messaging: Disabled

Enable

Mobile Devices

Disable Exchange ActiveSync

Disable OWA for Devices

View details

Email Connectivity

Outlook on the web: Enabled

Disable | View details

IMAP: Enabled

Disable

POP3: Enabled

Disable

MAPI: Enabled

Disable

https://outlook.office365.com/ecp/UsersGroups/EditMailbox....turnObjectType=1&id=c37cb204-818e-46c1-935a-512d5d19931e#

FIGURE 4-47 Disable Outlook On The Web

4. On the Warning dialog box, click Yes.
5. Click Save to save the changes to the Office 365 Exchange Online mailbox.

You use the Set-CASMailbox Windows PowerShell cmdlet to enable and disable OWA on a per user basis. For example, to disable OWA for the dan.jump@contoso2017er.com account, issue the command:

```
Set-CasMailbox dan.jump@contoso2017er.com -OwaEnabled $False
```

You can use the Get-Mailbox cmdlet with the Set-CasMailbox cmdlet to disable OWA for all mailbox users. To do this, issue the following command:

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} |
Set-CasMailbox -OwaEnabled $False
```

To enable OWA for the dan.jump@contoso2017er.com account, issue the command:

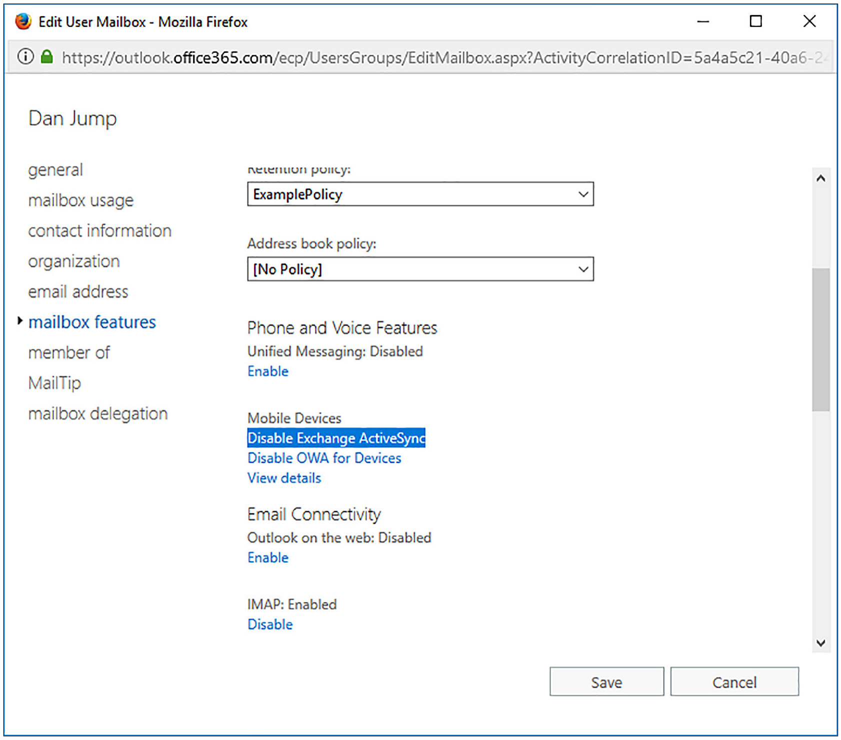
```
Set-CasMailbox dan.jump@contoso2017er.com -OwaEnabled $True
```

Configure ActiveSync

ActiveSync is a protocol, primarily used by mobile devices, that allows access to email, calendar, contacts, and tasks. ActiveSync is enabled by default on Office 365 Exchange Online mailboxes. In some scenarios, you might wish to disable ActiveSync.

To disable ActiveSync on a specific mailbox, perform the following steps:

1. In the Recipients area of the Exchange Admin Center, select the user for which you wish to disable ActiveSync, and click the Edit (Pencil) icon on the toolbar.
2. In the Mailbox Features section, shown in Figure 4-48, click Disable Exchange ActiveSync.



Edit User Mailbox - Mozilla Firefox

https://outlook.office365.com/ecp/UsersGroups/EditMailbox.aspx?ActivityCorrelationID=5a4a5c21-40a6-2

Dan Jump

Retention policy:
ExamplePolicy

Address book policy:
[No Policy]

Phone and Voice Features
Unified Messaging: Disabled
Enable

Mobile Devices
Disable Exchange ActiveSync
Disable OWA for Devices
View details

Email Connectivity
Outlook on the web: Disabled
Enable

IMAP: Enabled
Disable

FIGURE 4-48 Disable ActiveSync

3. On the Warning dialog box, click Yes.
4. Click Save to close the User Mailbox properties page.

You can use the Set-CASMailbox Windows PowerShell cmdlet to enable or disable ActiveSync. For example, to disable ActiveSync for the don.funk@contoso2017er.com mailbox, issue the command:

```
Set-CASMailbox -Identity don.funk@contoso2017er.com -ActiveSyncEnabled $False
```

You can use the Get-Mailbox cmdlet in conjunction with the Set-CasMailbox cmdlet to disable ActiveSync for all users in an organization. To do this, issue the command:

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} |
Set-CasMailbox –ActiveSyncEnabled
$False
```

To enable ActiveSync for the don.funk@contoso2017er.com mailbox, issue the command:

```
Set-CASMailbox –Identity don.funk@contoso2017er.com –ActiveSyncEnabled $False
```

MORE INFO **OFFICE 365 AND ACTIVESYNC**

You can learn more about managing ActiveSync for Office 365 at *https://support.office.com/en-us/article/Set-up-and-manage-mobile-access-for-your-users-01fff219-4492-40f2-82d3-fd2ffc0ad802*.

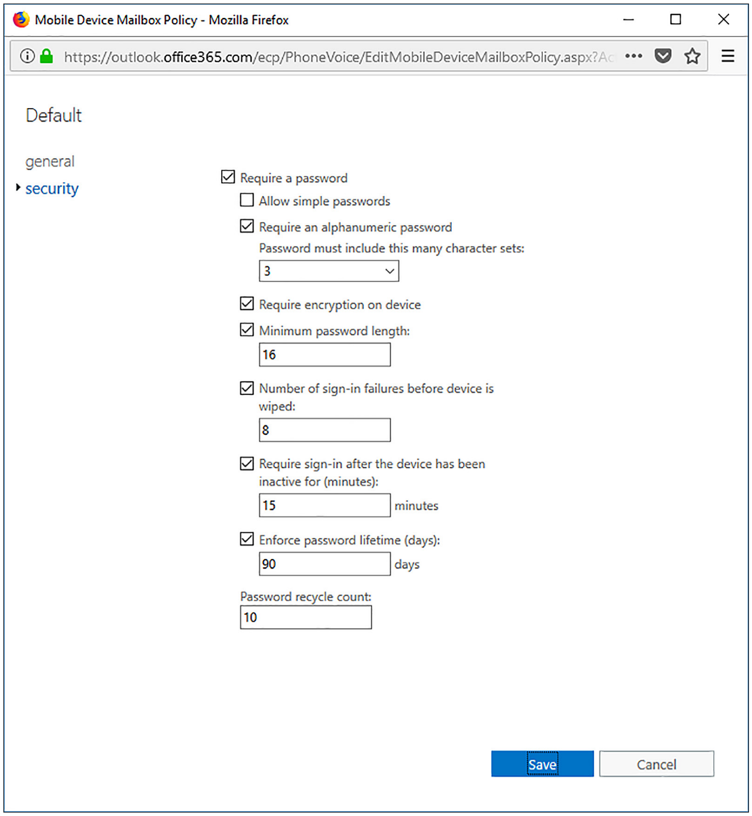
Mobile Device Management

Mobile Device Management (MDM) for Office 365 allows you to manage certain devices that interact with Office 365. You can control how Office 365 email and documents are accessed and Office 365 MDM allows you to remotely wipe devices to eradicate sensitive organizational information.

Office 365 MDM supports the following devices:

- iOS 7.1 and later
- Android 4 and later
- Windows 8.1 (limited)
- Windows 10 (requires that the device be joined to the Office 365 Azure AD instance)
- Windows 10 Mobile (requires that the device be joined to the Office 365 Azure AD instance)

You can use Office 365 MDM policies to configure the following policies shown in Figure 4-49:



Mobile Device Mailbox Policy - Mozilla Firefox

https://outlook.office365.com/ecp/PhoneVoice/EditMobileDeviceMailboxPolicy.aspx?Ac

Default

general

security

☑ Require a password

☐ Allow simple passwords

☑ Require an alphanumeric password

Password must include this many character sets:

3

☑ Require encryption on device

☑ Minimum password length:

16

☑ Number of sign-in failures before device is wiped:

8

☑ Require sign-in after the device has been inactive for (minutes):

15 minutes

☑ Enforce password lifetime (days):

90 days

Password recycle count:

10

FIGURE 4-49 Mobile Device Mailbox Policy

- Require a password
- Allow simple password
- Require an alphanumeric password (specify number of character sets required)
- Require encryption on device
- Minimum password length
- Number of sign-in failures before device is wiped
- Require sign-in after the device has been inactive for (minutes)
- Enforce password lifetime (days)
- Password recycle count

MORE INFO **OFFICE 365 AND MOBILE DEVICE MANAGEMENT**

You can learn more about managing mobile devices using Office 365 at *https://support.office.com/en-us/article/Capabilities-of-built-in-Mobile-Device-Management-for-Office-365-a1da44e5-7475-4992-be91-9ccec25905b0*.

Data Loss Prevention

Data Loss Prevention (DLP) policies allow you to accomplish the following goals:

- **Identify information that is sensitive across a variety of locations including Exchange Online, SharePoint Online, or OneDrive for Business** Sensitive information can include credit card numbers, passport numbers, or any readily identifiable combination of characters.
- **Prevent accidental sharing of information** Block access to documents that contain sensitive information from being accessed by unauthorized people, including those outside the organization. Block email messages that include sensitive information from being sent.
- **Monitor and protect sensitive information in desktop versions of Excel 2016, PowerPoint 2016, and Word 2016** Identify sensitive information as it is generated and apply DLP policies.
- **View DLP reports showing content that matches your organization's DLP policies** Allows you to determine how well your organization is complying with specific DLP policies. Also allows you to view false positive reports.

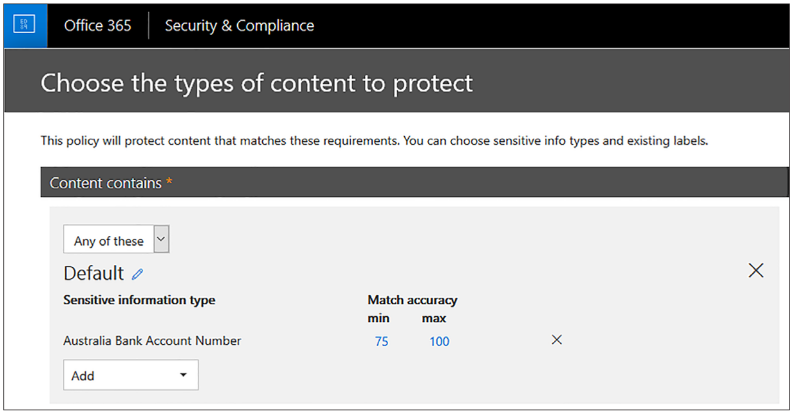
DLP policies can be configured to protect some or all SharePoint sites or OneDrive accounts. At present it isn't possible to select specific mailboxes, so if you choose to apply DLP policies to Exchange Online, it will apply to Exchange Online in its entirety.

DLP policies

DLP policies contain one or more rules. A rule includes conditions, actions, user notifications, user overrides, and incident reports.

Conditions determine the type of information being searched for and whether to take an action. Conditions can include:

- A type of sensitive information, as shown in Figure 4-50. This can include common types of sensitive information, such as credit card numbers, national ID numbers, and passport numbers. Detection goes beyond looking for a specific string of numbers, but also includes contextual content examination and regular expressions.
- A specific label is applied to the content. A label may be applied manually or through another mechanism such as a transport rule.
- Content is shared with people outside the organization. A determination is made as to the identity of the person trying to access the information.



Office 365 | Security & Compliance

Choose the types of content to protect

This policy will protect content that matches these requirements. You can choose sensitive info types and existing labels.

Content contains *

Any of these

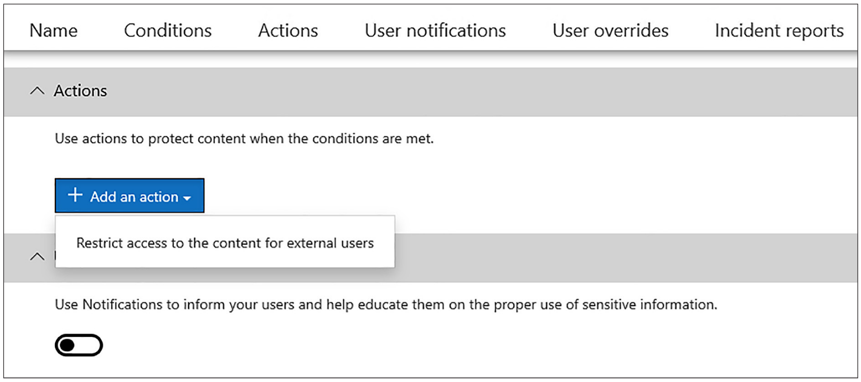
Default

Sensitive information type	Match accuracy min	 max
Australia Bank Account Number	75	100

Add

FIGURE 4-50 DLP conditions

Actions determine what occurs automatically when specific sensitive information is detected. Figure 4-51 shows access to the content being restricted. Depending on the action options selected, this would block access to the document to everyone except the primary site collection administrator, document owner, and the person who last modified the document or would just apply to blocking people from outside the organization. This action would also block a message that contained the sensitive information, either in the message body, or as an attachment, from being sent.



Name | Conditions | Actions | User notifications | User overrides | Incident reports

Actions

Use actions to protect content when the conditions are met.

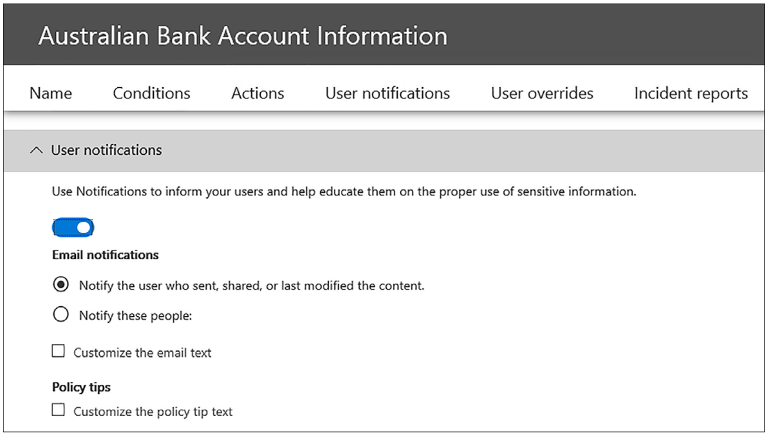
+ Add an action

Restrict access to the content for external users

Use Notifications to inform your users and help educate them on the proper use of sensitive information.

FIGURE 4-51 DLP actions

User notifications, shown in Figure 4-52, determine what happens when a rule is triggered. You can choose to have no notification occur, to send a notification to the user who sent, shared, or modified the content, or to send a notification to a specific person, such as a compliance officer. You can customize the notification. If the rule applies to content generated in Word, Excel, PowerPoint, Outlook, OWA, SharePoint Online or OneDrive for Business, a policy tip text may be configured that will inform the person interacting with the content that the content includes sensitive information.



Australian Bank Account Information

User notifications

Use Notifications to inform your users and help educate them on the proper use of sensitive information.

Email notifications

● Notify the user who sent, shared, or last modified the content.

○ Notify these people:

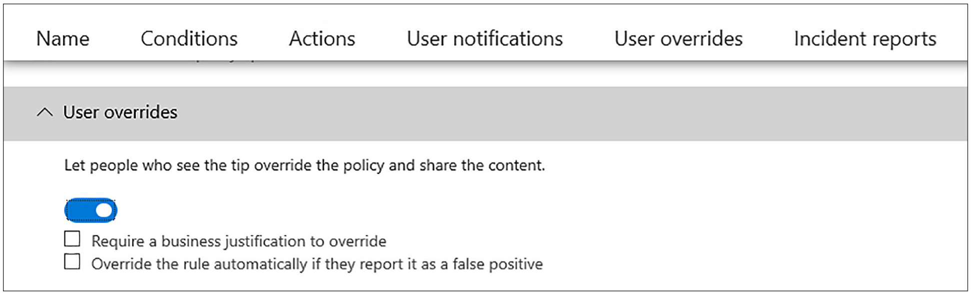
□ Customize the email text

Policy tips

□ Customize the policy tip text

FIGURE 4-52 DLP notification

You can also configure the rule to allow users to override the restriction. You can allow them to provide a business justification to override the rule, or to submit a false positive report as a method of overriding the restriction. User override options are shown in Figure 4-53.



User overrides

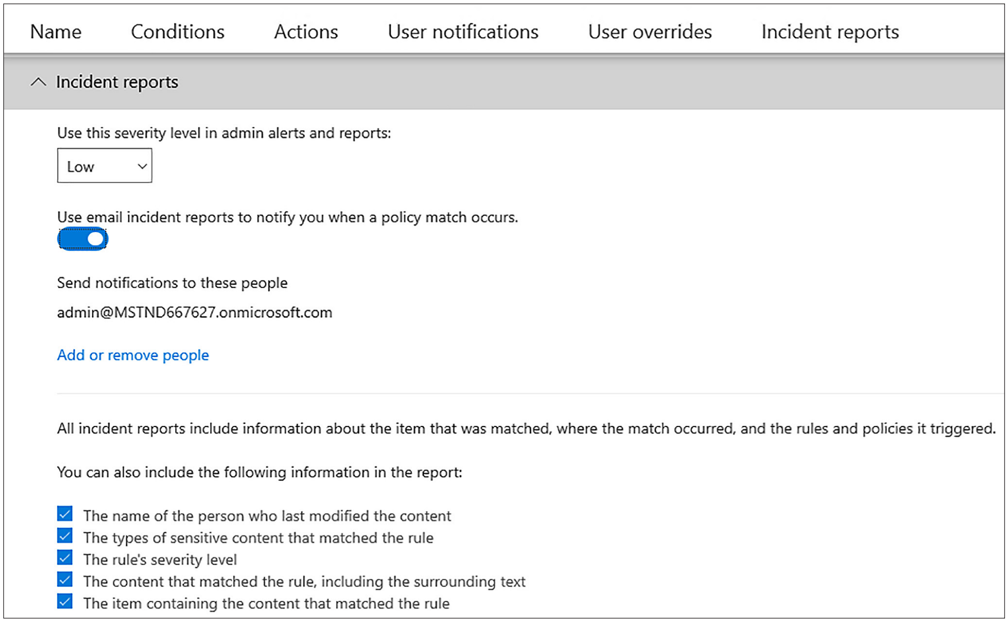
Let people who see the tip override the policy and share the content.

□ Require a business justification to override

□ Override the rule automatically if they report it as a false positive

FIGURE 4-53 User override

Incident reports allow you to have a report generated and to be sent when the rule is triggered. For email message, the report includes the original message that triggered the rule. You can configure the following items for the report, as shown in Figure 4-54.



Use this severity level in admin alerts and reports:

Low

Use email incident reports to notify you when a policy match occurs.

Send notifications to these people

admin@MSTND667627.onmicrosoft.com

All incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered.

You can also include the following information in the report:

☑ The name of the person who last modified the content
☑ The types of sensitive content that matched the rule
☑ The rule's severity level
☑ The content that matched the rule, including the surrounding text
☑ The item containing the content that matched the rule

FIGURE 4-54 User override

- The Name Of The Person Who Last Modified The Content
- The Types Of Sensitive Content That Matched The Rule
- The Rule's Severity Level
- The Content That Matched The Rule, Including The Surrounding Text
- The Item Containing The Content That Matched The Rule

Rules are assigned a priority based on the order in which the rule is created. You can't change the priority of a rule, other than by deleting and re-creating the rule. If content matches multiple rules, the rules are processed in priority order, and the most restrictive action is applied.

MORE INFO **DATA LOSS PREVENTION**

You can learn more about managing Data Loss Prevention Office 365 at *https://support.office.com/en-us/article/Overview-of-data-loss-prevention-policies-1966b2a7-d1e2-4d92-ab61-42efbb137f5e*.

EXAM TIP

Remember the Windows PowerShell cmdlets used to configure and manage litigation hold.

Skill 4.4: Manage Skype for Business global external communications settings

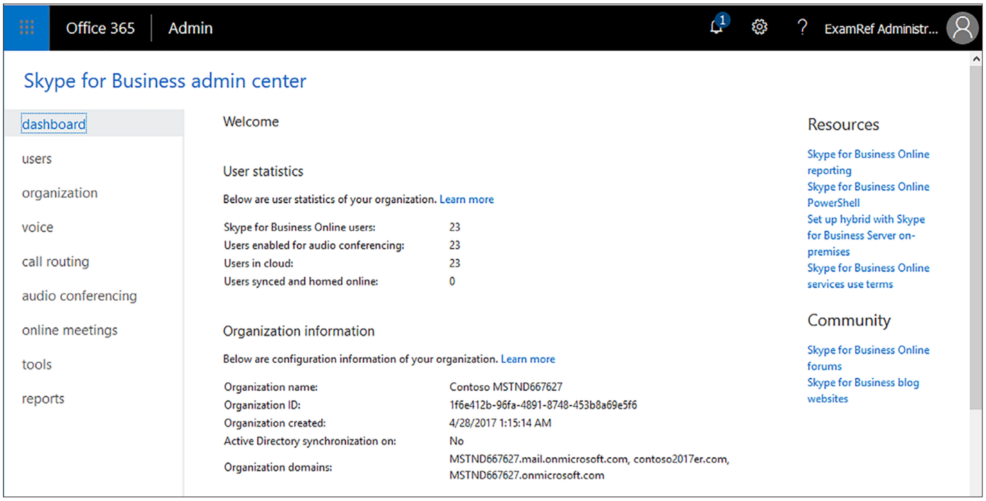
This skill deals with managing tenancy level settings for Skype for Business. These settings allow you to manage, at the tenancy level, which external users Skype for Business clients are able to communicate with, including whether communication is allowed with the consumer version of Skype.

This skill covers the following topics:

- Manage external communication and domains
- Manage Skype consumer connectivity
- Customize meeting invitations
- Disable push notifications
- Cloud PBX
- PSTN Conferencing
- Skype Meeting Broadcast

Manage external communication and domains

In the previous chapter, you read about how to manage external communication for Skype for Business Online users using the browser and the Skype for Business Admin Center, as shown in Figure 4-55.


Office 365
Admin
1
ExamRef Administr...
Skype for Business admin center
dashboard
users
organization
voice
call routing
audio conferencing
online meetings
tools
reports
Resources
Skype for Business Online reporting
Skype for Business Online PowerShell
Set up hybrid with Skype for Business Server on-premises
Skype for Business Online services use terms
Community
Skype for Business Online forums
Skype for Business blog websites

Welcome

User statistics

Below are user statistics of your organization. Learn more

Skype for Business Online users:	23
Users enabled for audio conferencing:	23
Users in cloud:	23
Users synced and homed online:	0

Organization information

Below are configuration information of your organization. Learn more

Organization name:	Contoso MSTND667627
Organization ID:	1f6e412b-96fa-4891-8748-453b8a69e5f6
Organization created:	4/28/2017 1:15:14 AM
Active Directory synchronization on:	No
Organization domains:	MSTND667627.mail.onmicrosoft.com, contoso2017er.com, MSTND667627.onmicrosoft.com

FIGURE 4-55 Skype for Business admin center

You can also use a set of Skype for Business Online specific Windows PowerShell cmdlets to manage external communication settings. These cmdlets are as follows:

- **New-CsEdgeAllowAllKnownDomains** This cmdlet allows Skype for Business Online users to communicate with any domain, except those on the block list.
- **New-CsEdgeAllowList** Use this cmdlet to configure the domains with which Skype for Business Online users can communicate. This cmdlet must be used in conjunction with the New-CsEdgeDomainPattern and Set-CsTenantFederationConfiguration cmdlets.
- **New-CsEdgeDomainPattern** You use this cmdlet to modify the list of allowed or blocked domains because string values cannot be passed directly to the cmdlets used to manage the list.
- **Get-CsTenantFederationConfiguration** You can use this cmdlet to view information about the allowed domains and the blocked domains.

Managed allowed domain list

The following Windows PowerShell code allows users to only communicate with users in the tailspintoys.com and wingtiptoys.com domains.

```
$x = New-CsEdgeDomainPattern -Domain "tailspintoys.com"
$y = New-CsEdgeDomainPattern -Domain "wingtiptoys.com"
$newAllowList = New-CsEdgeAllowList -AllowedDomain $x,$y
Set-CsTenantFederationConfiguration -AllowedDomains $newAllowList
```

To remove a domain from the allowed list, you need to use a set of commands. First you need to place the current list of allowed domains in a variable:

```
$x = (Get-CsTenantFederationConfiguration).AllowedDomains
```

You then need to determine the number of the domain that you want to remove. You do this by issuing the variable as a command and then counting the number of lines until the domain that you want to remove, with the first line as zero. For example, if you had the following list output when you issued the variable as a command:

```
adatum.com
contoso.com
fabrikam.com
```

The domain contoso.com would be number 1, and adatum.com would be 0. Once you've determined which domain you want to remove, you issue the command $x.AllowedDomain.RemoveAt(Y), where Y is the number of the domain you want to remove. So if you wanted to remove fabrikam.com from the list, you would issue the command:

```
$x.AllowedDomain.RemoveAt(2)
```

You can repeat the process to remove other domains from the list. Once you've pruned all of the domains that you want to remove, you can then assign the list using the following command:

```
Set-CsTenantFederationConfiguration -AllowedDomains $x
```

The following command removes all domains from the current allow list:

```
$newAllowList = New-CsEdgeAllowList -AllowedDomain $Null
Set-CsTenantFederationConfiguration -Tenant -AllowedDomains $newAllowList
```

You can use the Get-CsTenantFederationConfiguration cmdlet to view the list of allowed domains by issuing the following command:

```
Get-CsTenantFederationConfiguration | Select-Object -ExpandProperty AllowedDomains
 | Select-Object AllowedDomain
```

Manage blocked domain list

To add a domain to the blocked list, use the `BlockedDomains` parameter. For example, to add margiestravel.com to the list of blocked domains, issue the following command:

```
$x = New-CsEdgeDomainPattern ''margiestravel.com''
Set-CsTenantFederationConfiguration –BlockedDomains @{Add=$x}
```

You can use the Get-CsTenantFederationConfiguration cmdlet to view the list of blocked domains by issuing the following command:

```
Get-CsTenantFederationConfiguration | Select-Object -ExpandProperty BlockedDomains
```

To remove the domain margiestravel.com from the domain blocked list, perform the following steps:

```
$x = New-CsEdgeDomainPattern ''margiestravel.com''
Set-CsTenantFederationConfiguration –BlockedDomains @{Remove=$x}
```

You can remove all domains from the blocked domain list by issuing the following command:

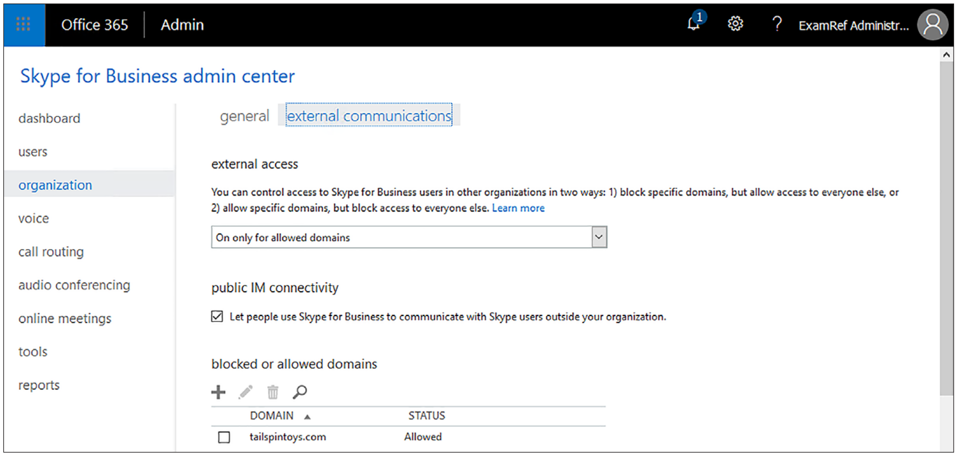
```
Set-CsTenantFederationConfiguration -BlockedDomains $Null
```

MORE INFO **MANAGE EXTERNAL COMMUNICATION**

You can learn more about managing external communication using Windows PowerShell for Skye for Business Online at: *https://technet.microsoft.com/en-us/library/dn362813(v=ocs.15).aspx*.

Manage Skype consumer connectivity

As you read about in the last chapter, you can use the Turn On Communication With Skype Users And Users Of Other Public IM Service Providers option, found in the External Communications area of the Skype for Business Admin Center, as shown in Figure 4-56, to allow or block Skype for Business users from communicating with Skype users.



Skype for Business admin center

external access

You can control access to Skype for Business users in other organizations in two ways: 1) block specific domains, but allow access to everyone else, or 2) allow specific domains, but block access to everyone else. Learn more

On only for allowed domains

public IM connectivity

☑ Let people use Skype for Business to communicate with Skype users outside your organization.

blocked or allowed domains

	DOMAIN ▲	STATUS
□	tailspintoys.com	Allowed

FIGURE 4-56 Allow Skype communication

You can use the Set-CsTenantFederationConfiguration cmdlet to also disable and enable public IM connectivity. The following command enables public IM connectivity:

```
Set-CsTenantFederationConfiguration –AllowPublicUsers $True
```

Once you've enabled public IM connectivity, you can allow or block specific providers. You do this with the Set-CsTenantPublicProvider cmdlet. When using this cmdlet, you must specify the tenant identifier. You can determine the tenant ID using the following command:

```
Get-CsTenant | Select-Object TenantID
```

Once you have the tenant ID, you can enable connectivity to Skype using the following command:

```
Set-CsTenantPublicProvider -Tenant "TenantID" -Provider "Skype"
```

The following command disables public IM connectivity:

```
Set-CsTenantFederationConfiguration –AllowPublicUsers $False
```

MORE INFO **PUBLIC IM PROVIDER CONNECTIVITY**

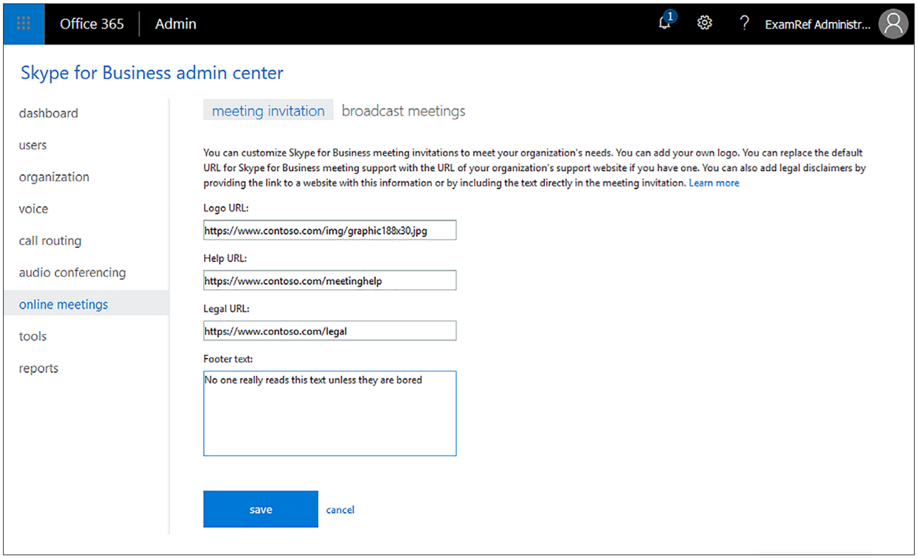
You can learn more about allowing access to public IM providers at: *https://technet.microsoft.com/en-us/library/dn362809(v=ocs.15).aspx*.

Customize meeting invitations

You can customize meeting invitations, including a logo, help URL, legal URL, and meeting footer text. The logo can be up to 188 pixels by 30 pixels in size and can be in .jpg or .gif format. By default, meeting invitations are not customized.

To configure custom meeting invitations, perform the following steps:

1. Select the Meeting Invitation section in the Skype for Business Admin Center.
2. Provide information in the following areas, as shown in Figure 4-57:
   - **Logo URL** The URL of a JPG or GIF file no larger than 188 pixels by 30 pixels.
   - **Help URL** The URL of documentation providing assistance to meeting attendees.
   - **Legal URL** The URL of any legal information necessary for meeting attendees to be aware of.
   - **Footer text** Text that is included in the footer of any meeting invitation.



You can customize Skype for Business meeting invitations to meet your organization's needs. You can add your own logo. You can replace the default URL for Skype for Business meeting support with the URL of your organization's support website if you have one. You can also add legal disclaimers by providing the link to a website with this information or by including the text directly in the meeting invitation. Learn more

Logo URL: https://www.contoso.com/img/graphic188x30.jpg

Help URL: https://www.contoso.com/meetinghelp

Legal URL: https://www.contoso.com/legal

Footer text: No one really reads this text unless they are bored

FIGURE 4-57 Custom meeting invitation

MORE INFO **CUSTOMIZE MEETING INVITATIONS**

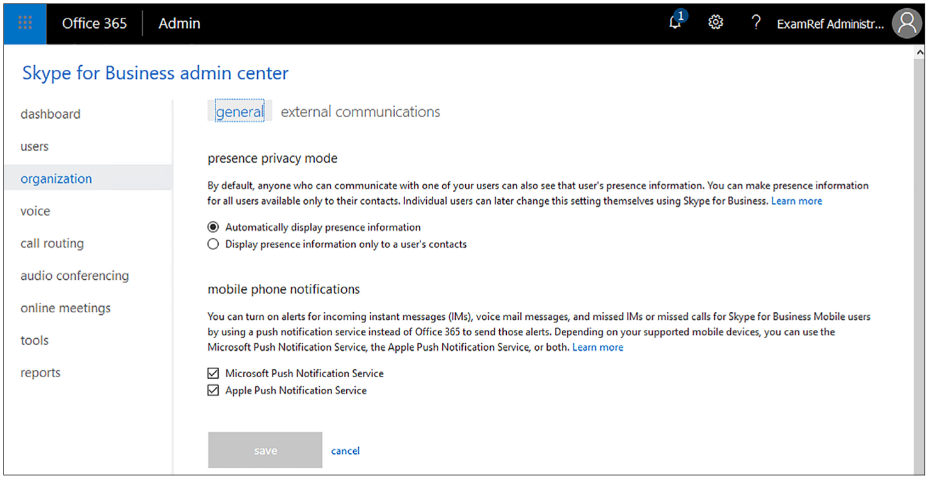
You can learn more about customizing Skype for Business Online meeting notifications at: *https://support.office.com/en-us/article/Customize-meeting-invitations-9af52080-dd56-4b66-b056-41ed1a7aaae3*.

Disable push notifications

Push notification allows alerts about incoming and missed instant messages to be displayed whenever the user is not actively using Skype for Business on their phone or tablet. Push notifications are enabled by default in Skype for Business. Users are able to disable them through the options in the Skype for Business client on their own device. If you want to disable push notifications, users will receive alerts about incoming and missed instant messages the next time they use the Skype for Business client on their mobile device.

To disable push notifications, perform the following steps:

1. Select the Organization section in the Skype for Business Admin Center.
2. Ensure the General section is selected.
3. Under Mobile Phone Notifications, shown in Figure 4-58, and remove the check next to each of the notification types that you would like to remove.



presence privacy mode

By default, anyone who can communicate with one of your users can also see that user's presence information. You can make presence information for all users available only to their contacts. Individual users can later change this setting themselves using Skype for Business. Learn more

● Automatically display presence information
○ Display presence information only to a user's contacts

mobile phone notifications

You can turn on alerts for incoming instant messages (IMs), voice mail messages, and missed IMs or missed calls for Skype for Business Mobile users by using a push notification service instead of Office 365 to send those alerts. Depending on your supported mobile devices, you can use the Microsoft Push Notification Service, the Apple Push Notification Service, or both. Learn more

☑ Microsoft Push Notification Service
☑ Apple Push Notification Service

FIGURE 4-58 Push notifications

4. Click Save to apply the changes.

You use the Set-CsPushNotificationConfiguration cmdlet to enable or disable the Push Notification Service. To disable the Apple and Microsoft Push Notification Services, issue the following command:

```
Set-CsPushNotificationConfiguration -EnableApplePushNotificationService $False
-EnableMicrosoftPushNotificationService $False
```

You can disable the push notification for one service while keeping the push notification for the other service running. For example, to disable the Microsoft Push Notification Service, but enable the Apple Push Notification Service, issue the following command:

```
Set-CsPushNotificationConfiguration -EnableApplePushNotificationService $True
-EnableMicrosoftPushNotificationService $False
```

MORE INFO **PUSH NOTIFICATIONS**

You can learn more about configuring push notifications at: *https://support.office.com/en-us/article/Turn-off-mobile-phone-notifications-2de47013-4f09-493c-abc5-372f56ad69e3*.

Cloud PBX

Cloud PBX, also known as Phone System in Office 365, allows organizations to replace their existing PBX deployment with Office 365. Phone System for Office 365 performs the following basic call tasks:

- Placing calls to the PSTN network
- Receiving calls from the PSTN network
- Transferring calls
- Muting and unmuting calls

Users are able to place and receive calls using their mobile devices, a headset with a laptop or desktop PC, or IP phones that support Skype for Business. You can connect Phone System in Office 365 to the PSTN network in one of the following ways:

- Purchasing a calling plan add-on for Office 365. In this scenario Microsoft is the provider of both core calling and PSTN services. Microsoft is also able to provide or port your user's existing phone numbers.
- Using on-premises PSTN connectivity, where on-premises software connects to an existing telephony interface. Cloud Connector is a set of packaged virtual machines that provide on-premises PSTN connectivity with Phone System for Office 365. This solution is appropriate for organizations that want to allow Skype for Business Online users to use existing PSTN connections with call control managed by Office 365 in the cloud.

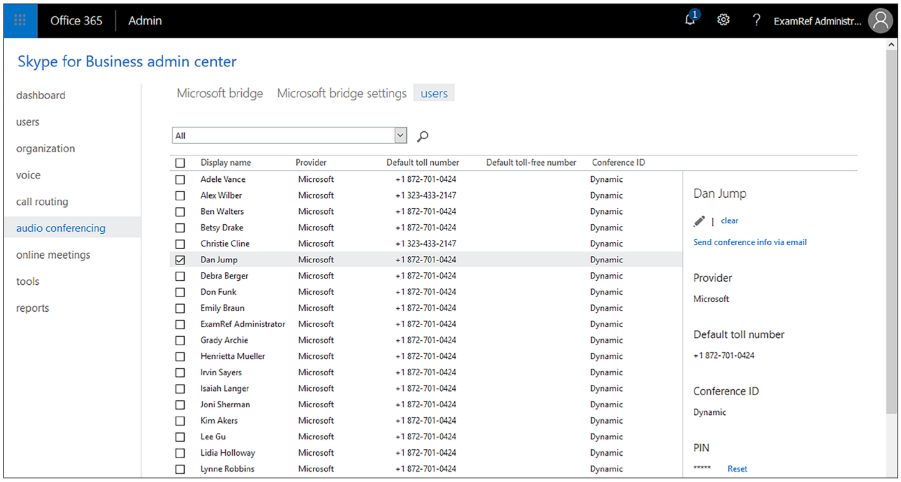
> ***MORE INFO*** **CLOUD PBX**
>
> **You can learn more about Cloud PBX at: *https://technet.microsoft.com/en-us/library/mt612869.aspx*.**

PSTN Conferencing

Office 365 PSTN Conferencing is an Office 365 E5 feature that provides the ability for meeting attendees to connect to the audio portion of a Skype for Business meeting using a dial-in phone number as an additional option to using the Skype for Business client.

To enable PSTN conferencing, perform the following steps:

1. In the Office 365 Admin Center, navigate to Skype for Business under Admin Centers.
2. In the Skype for Business Admin Center click Audio Conferencing.
3. On the Users tab, shown in Figure 4-59, select the user you wish to assign a dial-in conferencing number to, and click the edit (pencil) icon.



☐	Display name	Provider	Default toll number	Default toll-free number	Conference ID
☐	Adele Vance	Microsoft	+1 872-701-0424		Dynamic
☐	Alex Wilber	Microsoft	+1 323-433-2147		Dynamic
☐	Ben Walters	Microsoft	+1 872-701-0424		Dynamic
☐	Betsy Drake	Microsoft	+1 872-701-0424		Dynamic
☐	Christie Cline	Microsoft	+1 323-433-2147		Dynamic
☑	Dan Jump	Microsoft	+1 872-701-0424		Dynamic
☐	Debra Berger	Microsoft	+1 872-701-0424		Dynamic
☐	Don Funk	Microsoft	+1 872-701-0424		Dynamic
☐	Emily Braun	Microsoft	+1 872-701-0424		Dynamic
☐	ExamRef Administrator	Microsoft	+1 872-701-0424		Dynamic
☐	Grady Archie	Microsoft	+1 872-701-0424		Dynamic
☐	Henrietta Mueller	Microsoft	+1 872-701-0424		Dynamic
☐	Irvin Sayers	Microsoft	+1 872-701-0424		Dynamic
☐	Isaiah Langer	Microsoft	+1 872-701-0424		Dynamic
☐	Joni Sherman	Microsoft	+1 872-701-0424		Dynamic
☐	Kim Akers	Microsoft	+1 872-701-0424		Dynamic
☐	Lee Gu	Microsoft	+1 872-701-0424		Dynamic
☐	Lidia Holloway	Microsoft	+1 872-701-0424		Dynamic
☐	Lynne Robbins	Microsoft	+1 872-701-0424		Dynamic

Dan Jump

| clear

Send conference info via email

Provider

Microsoft

Default toll number

+1 872-701-0424

Conference ID

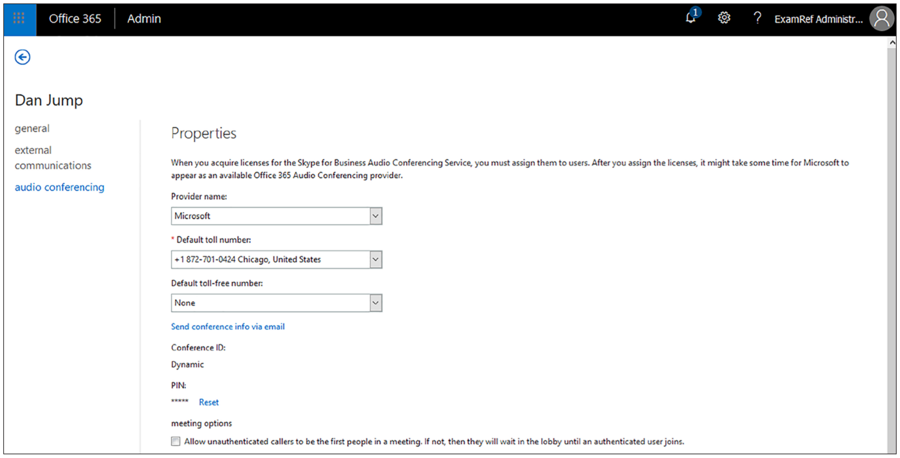
Dynamic

PIN

***** Reset

FIGURE 4-59 Audio conferencing users

4. On the Properties page, shown in Figure 4-60, select a default number. This will be the default number used for all meeting invites sent by this user.



Dan Jump

Properties

When you acquire licenses for the Skype for Business Audio Conferencing Service, you must assign them to users. After you assign the licenses, it might take some time for Microsoft to appear as an available Office 365 Audio Conferencing provider.

Provider name:

Microsoft

* Default toll number:

+1 872-701-0424 Chicago, United States

Default toll-free number:

None

Send conference info via email

Conference ID:

Dynamic

PIN:

***** Reset

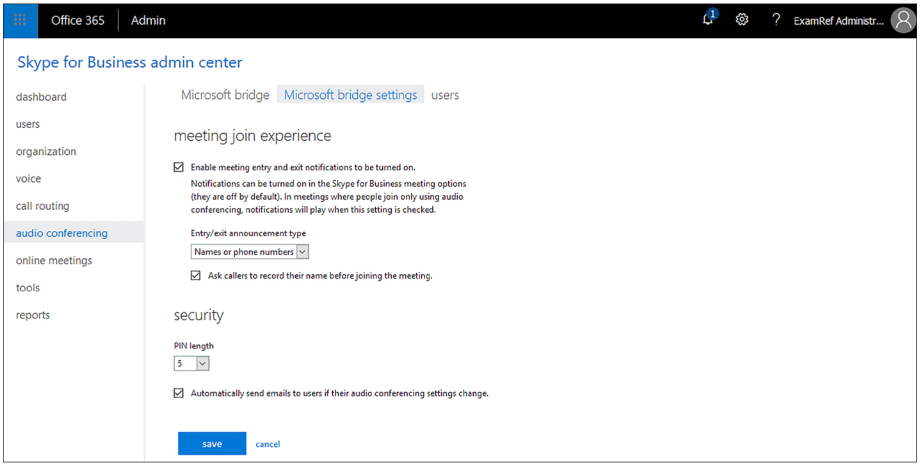
meeting options

☐ Allow unauthenticated callers to be the first people in a meeting. If not, then they will wait in the lobby until an authenticated user joins.

FIGURE 4-60 User toll number properties

5. Once you click Save, the user is sent an email message informing them that they have been configured for Skype for Business Dial-In conferencing, the telephone number to access conference, their personal conference ID, and their organizer PIN.

6. On the Microsoft bridge settings page, shown in Figure 4-61, you can configure the following options.



meeting join experience

☑ Enable meeting entry and exit notifications to be turned on.

Notifications can be turned on in the Skype for Business meeting options (they are off by default). In meetings where people join only using audio conferencing, notifications will play when this setting is checked.

Entry/exit announcement type: Names or phone numbers

☑ Ask callers to record their name before joining the meeting.

security

PIN length: 5

☑ Automatically send emails to users if their audio conferencing settings change.

FIGURE 4-61 Microsoft bridge settings

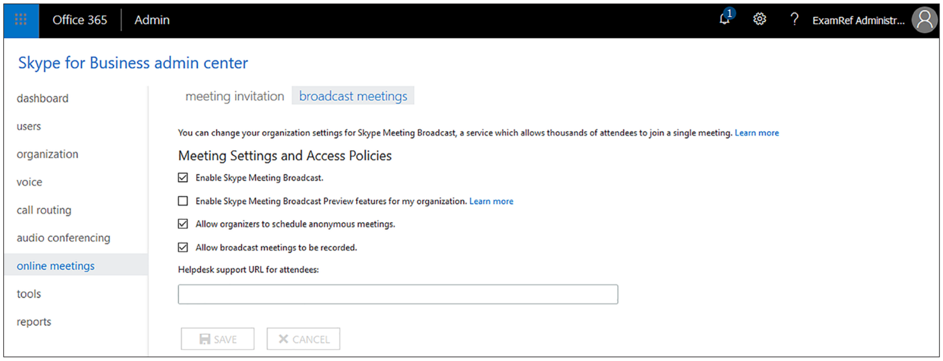
- Entry and exit notification settings. Allows you to determine whether or not entry and exit notifications are made and the nature of those notifications.
- Whether callers are asked to record their name prior to entering the meeting.
- Length of the PIN.
- Sending an email when changes are made to a user's dial-in conference settings.

> ***MORE INFO*** **PSTN CONFERENCING**
>
> You can learn more about PSTN conferencing at: *https://blogs.technet.microsoft.com/skype-hybridguy/2016/01/30/cloud-pbx-modern-voice-pstn-calling-in-office365-2/.*

Skype Meeting Broadcast

Skype Meeting Broadcast allows you to schedule, produce, and broadcast meetings online for audiences of up to 10,000 attendees. To enable Skype meeting broadcast, perform the following steps:

1. In the Office 365 Admin Center, navigate to Skype for Business under Admin Centers.
2. In the Skype for Business admin center, navigate to Broadcast meetings under Online meetings, and then select Enable Skype Meeting Broadcast, as shown in Figure 4-62.



You can change your organization settings for Skype Meeting Broadcast, a service which allows thousands of attendees to join a single meeting. Learn more

Meeting Settings and Access Policies

☑ Enable Skype Meeting Broadcast.

□ Enable Skype Meeting Broadcast Preview features for my organization. Learn more

☑ Allow organizers to schedule anonymous meetings.

☑ Allow broadcast meetings to be recorded.

Helpdesk support URL for attendees:

FIGURE 4-62 Broadcast meetings

You can enable broadcast meetings using the following PowerShell command:

```
Set-CsBroadcastMeetingConfiguration –EnableBroadcastMeeting $True
```

MORE INFO **SKYPE MEETING BROADCAST**

You can learn more about Skype Meeting Broadcast at: *https://support.office.com/en-us/article/What-is-a-Skype-Meeting-Broadcast-c472c76b-21f1-4e4b-ab58-329a6c33757d.*

EXAM TIP

Remember the different Windows PowerShell cmdlets you would use to manage allowed and blocked domains.

Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answers to this thought experiment in the next section.

You are in the process of planning the alteration of the default spam filter used for your organization's Office 365 tenancy. Currently, messages that have an SCL of 7 are being placed in a user's junk email folders. Many of these messages are turning out to be legitimate, so for the next six months you want to have them moved to quarantine instead, where they can be examined by members of your team to check if they are being classified appropriately.

Recently, for reasons that aren't entirely clear, several email accounts at your organization are being sent email from addresses in New Zealand. The contents of these emails are entirely in the Esperanto language. A variety of different IP addresses are used to send the emails, so filtering based on IP addresses hasn't been entirely successful. You have been asked to ensure that all messages of this nature are classified as spam.

You are also in the process of planning an IMAP migration from a third-party on-premises messaging system that hosts 200 mailboxes to Office 365. You are reviewing the migration process.

You are looking at replacing the current practice of using litigation hold at Tailspin Toys when users are subject to discovery requests with instead switching to in-place hold. Management is especially interested in using the query functionality of in-place hold to locate items subject to discovery requests that are stored across multiple mailboxes. Management is also interested in what changes occur in terms of archive mailbox functionality when in-place hold is applied.

You are in the process of configuring Skype for Business Online using Windows PowerShell. You are interested in configuring public IM connectivity, disabling the Apple push notification service, and removing all of the currently blocked domains from the blocked domain list. To do this, you need to research the appropriate Windows PowerShell commands to accomplish these tasks.

With all of this in mind, answer the following questions:

1. What steps do you need to take to modify the default spam filter policy to ensure that messages with an SCL of 7 are placed in quarantine?
2. What steps do you need to take to modify the default spam filter policy to ensure that all messages in the Esperanto language that originate from New Zealand are marked as spam?
3. Which Windows PowerShell cmdlet and parameter should be used to release a message to all recipients if that message is currently in quarantine?
4. What is the first step in an IMAP migration?
5. What step should an administrator take after all IMAP mailboxes that will be migrated are successfully synchronized to corresponding Office 365 mailboxes and are successfully performing periodic synchronization every 24 hours?
6. When should the tenant administrator delete the IMAP migration batches?
7. Which Exchange Administrator role must a user be a member of to configure a query-based in-place hold?
8. When an in-place hold is applied on a mailbox, what is the new quota value assigned to the archive mailbox?
9. Which Windows PowerShell command, including parameters and values, would you use to disable public IM connectivity?
10. Which Windows PowerShell command, including parameters and values, would you use to disable the Apple Push Notification Service?
11. Which Windows PowerShell command, including parameters and values, would you use to remove all domains from the blocked domains list?

Thought experiment answers

This section contains the solutions to the thought experiment.

1. Edit the default spam filter policy and alter the Spam action to Quarantine message.
2. Edit the international spam settings of the default spam filter policy and specify the Esperanto language and the New Zealand country or region.
3. Use the Release-QuarantineMessage cmdlet with the `ReleaseToAll` parameter to release a message currently in quarantine to all recipients.
4. The first step in an IMAP migration is to create user accounts in Office 365 that correspond to the on-premises IMAP accounts that must be migrated.
5. Once synchronization is successful and periodic synchronization is proceeding without problem, the administrator should update MX records to point to Exchange Online.
6. The tenant administrator should delete the IMAP migration batches after mail flow is occurring successfully to Exchange Online and not the on-premises IMAP messaging system.
7. A user must be a member of the Discovery Management Exchange Administrator role to be able to configure a query-based in-place hold.
8. When an in-place hold or litigation hold is applied on a mailbox, the archive mailbox quota is increased from 30 GB to 100 GB.
9. You would use the Set-CsTenantFederationConfiguration –AllowPublicUsers $False command to disable public IM connectivity.
10. You would use the Set-CsPushNotificationConfiguration –EnableApplePushNotificationService $False command to disable the Apple Push Notification Service.
11. You use the Set-CsTenantFederationConfiguration -BlockedDomains $Null command to remove all domains from the blocked domains list.

Chapter summary

- The malware detection response settings are Delete Entire Message, Delete All Attachments And Use Default Alert Text, and Delete All Attachments And Use Custom Alert Text.
- You can configure the following notification options when malware is detected: Notify Internal Senders, Notify External Senders, Notify Administrators About Undelivered Messages From Internal Senders, and Notify Administrators About Undelivered Messages From External Senders.
- You can create different anti-malware policies and then apply them to different groups of mail users.

- When creating a new custom anti-malware policy, you need to configure the Applied To setting. This setting takes the form of an If statement with a condition and exceptions.
- Spam filter blocks lists and allows lists, allowing you to filter on the basis of email address and sender domain.
- Spam filter international settings allow you to filter based on language and country, or region of origin.
- Outbound spam policy allows you to configure how spam originating from within your organization is managed.
- Use the cmdlets with the MalwareFilterPolicy noun to view, modify, create, and remove malware filter policies.
- Use the cmdlets with the MalwareFilterRule noun to view, modify, create, and disable malware filter rules.
- Use the cmdlets with the HostedConnectionFilterPolicy noun to manage connection filter policies.
- Use the cmdlets with the HostedContentFilterPolicy noun to view and edit spam filter settings.
- Use the Get and Release-QuarantineMessage cmdlets to search for and release messages from quarantine.
- Cutover migration is suitable if your on-premises environment has Exchange Server 2007 or later, less than 200 mailboxes, and you will perform cloud-based account management.
- Staged migration is suitable if you have an on-premises deployment of Exchange 2007 deployment with any number of user accounts. Staged migration can be used with on-premises or cloud-based user account management.
- Remove move migrations are appropriate if you have more than 2,000 user accounts, have Exchange 2007 or later, and intend to manage migrated users using cloud tools.
- IMAP migration is appropriate if you have non-Exchange on-premises messaging solutions.
- Use the New-CsEdgeAllowAllKnownDomains cmdlet to allow Skype for Business Online users to communicate with any domain, except those on the blocked list.
- Use the New-CsEdgeAllowList cmdlet to configure the domains with which Skype for Business Online users can communicate. This cmdlet must be used in conjunction with the New-CsEdgeDomainPattern and Set-CsTenantFederationConfiguration cmdlets.
- Use the New-CsEdgeDomainPattern to modify the list of allowed or blocked domains.
- Use the Get-CsTenantFederationConfiguration to view information about the allowed domains and the blocked domains.
- You can use the Set-CsTenantFederationConfiguration cmdlet to also disable and enable public IM connectivity.

- You can customize meeting invitations, including a logo, help URL, legal URL, and meeting footer text.
- Skype for Business push notification allow alerts about incoming and missed instant messages to be displayed whenever the user is not actively using Skype for Business on their phone or tablet.
- You can disable push notifications for the Microsoft and Apple Push Notification Service through the Skype for Business Admin Center, or by using the Set-CsPushNotification-Configuration.
- Archived mailboxes can be accessed by clients running Outlook 2007 and later, as well as people running Outlook Web App on computers.
- Archive mailboxes cannot be accessed from mobile versions of Outlook and cannot be accessed from Outlook Web App when used from a mobile device web browser.
- Litigation hold is applied to an entire mailbox and preserves the contents of that mailbox until the duration of the litigation hold expires, including modified and deleted items.
- It can take up to 60 minutes for a litigation hold to be enforced by Exchange Online after an administrator enables the hold.
- You can enable litigation hold on a mailbox using the Set-Mailbox Windows PowerShell cmdlet.
- When litigation hold or in-place hold are enabled, the quota on the archive mailbox is increased to 100 GB from 30 GB.
- In-place hold differs from litigation hold in that only the items that meet the query condition will be protected, rather than all items in the mailbox.
- Only users who have been assigned membership of the Discovery Management role group can configure query-based in-place holds.
- In-Place hold is managed from Windows PowerShell using cmdlets with the Mailbox-Search noun and the `InPlaceHold` parameter.
- You can disable and enable Outlook Web App (OWA), also termed Outlook on the Web, through Exchange Admin Center, or by using the Set-CasMailbox cmdlet with the `OwaEnabled` parameter.
- You can disable and enable ActiveSync through the Exchange Admin Center or by using the Set-CasMailbox cmdlet with the `ActiveSyncEnabled` parameter.

Index

S

This page intentionally left blank

About the author

ORIN THOMAS is an MVP, a Microsoft Regional Director, an MCT, and has a string of Microsoft MCSE and MCITP certifications. He has written more than 3 dozen books for Microsoft Press on topics including Windows Server, Windows Client, Azure, Office 365, System Center, Exchange Server, Security, and SQL Server. He is an author at PluralSight and is completing a Doctorate of Information Technology at Charles Sturt University. You can follow him on Twitter at *http://twitter.com/orinthomas*.