Secure configuration guide for Exchange Online
Edit:

© National Cryptologic Centre, 2019

NIPO: 083-19-262-1

Date of Edition: december 2019

Plain Concepts has participated in the creation and modification of this document and its annexes.
Sidertia Solutions S.L. has participated in the revision of this guide.

LIMITATION OF RESPONSABILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

Without written authorization from the National Cryptologic Centre, it is strictly forbidden, incurring penalties set by law, to partially or totally reproduce this document by any means or procedure, including photocopying and computer processing, or distribute copies of it by means of rental or public lending.
The current national and international scenario is dominated by developments in Information and Communication Technologies (ICT) and by risks emerging from their use. The Administration is fully aware of this scenario and it is necessary for this body to develop, acquire, conserve and secure use of ICTs to guarantee that its services run effectively for the citizen's and the country's best interests.

Working from the Centre's knowledge and experience on threats and vulnerabilities in terms of emerging risks, Law 11/2002, dated 6th May, regulating the National Intelligence Centre, entrusts the National Intelligence Centre the functions related to information technology security, according to the Article 4.e), and to the protection of classified information, according to the Article 4.f). It also gives, through the Article 9.2.f), its Secretary of State-Director the responsibility of managing the National Cryptologic Centre.

One of the most outstanding functions that it assigns to it, in Royal Decree 421/2004, dated 12th March, regulating the National Cryptologic Centre is to draw up and disseminate standards, instructions, guides and recommendations to guarantee security for the Administration's information and communication technologies.

Royal Decree 3/2010, dated 8th January, develops the National Security Framework (hereinafter called ENS) in the field of Electronic Administration which is also referred in the second section of Article 156 of Law 40/2015, dated 1st October, of the Public Sector Legal System. The National Security Framework establishes the security policy, in matters of use of electronic means, which ensures the protection of information.

Indeed, Royal Decree 3/2010, dated 8th January, updated by Royal Decree 951/2015, dated 23rd October, sets the basic principles and minimum requirements as well as any protection measures to be introduced in Administration systems. In article 29, it authorises the CCN to develop CIS guidelines to ease the fulfilment of these minimum requirements.

The CCN-STIC documents series was drawn up to comply with this function and the ENS, aware of the importance of establishing a frame of reference on this matter that can be used as support so that Administration staff can carry out their difficult and occasionally thankless task of providing security for ICT systems within their responsibility.

July 2019

Félix Sanz Roldan
Secretary of State
Director of the National Cryptologic Centre
INDEX

1. EXCHANGE ONLINE ........................................................................................................................................... 6
   1.1 DESCRIPTION OF THE USE OF THIS GUIDE .......................................................................................... 6
   1.2 SERVICE DEFINITION .............................................................................................................................. 6
   1.3 PREREQUISITES FOR DEPLOYMENT USING POWERSHELL .................................................................... 6

2. ONLINE EXCHANGE DEPLOYMENT .................................................................................................................... 8
   2.1 ADMINISTRATOR - INITIAL CONFIGURATION ....................................................................................... 8
   2.2 END USER - FIRST STEPS .......................................................................................................................... 9

3. ONLINE EXCHANGE CONFIGURATION ............................................................................................................ 17
   3.1 OPERATIONAL FRAMEWORK .................................................................................................................... 17
      3.1.1 ACCESS CONTROL .............................................................................................................................. 17
         3.1.1.1 IDENTIFICATION .......................................................................................................................... 17
         3.1.1.2 ENTRY REQUIREMENTS ................................................................................................................ 17
         3.1.1.3 SEGREGATION OF FUNCTIONS AND TASKS .............................................................................. 18
         3.1.1.4 ACCESS RIGHTS MANAGEMENT PROCESS .............................................................................. 21
         3.1.1.5 AUTHENTICATION MECHANISMS .............................................................................................. 24
         3.1.1.6 LOCAL ACCESS ............................................................................................................................ 24
         3.1.1.7 REMOTE ACCESS .......................................................................................................................... 26
      3.1.2 EXPLOITATION ........................................................................................................................................ 26
         3.1.2.1 PROTECTION AGAINST MALWARE ............................................................................................ 26
         3.1.2.2 ACTIVITY RECORD ....................................................................................................................... 27
         3.1.2.3 INCIDENT MANAGEMENT ............................................................................................................ 31
         3.1.2.4 PROTECTION OF ACTIVITY RECORDS ..................................................................................... 31
   3.2 PROTECTION MEASURES .............................................................................................................................. 31
      3.2.1 PROTECTION OF COMMUNICATIONS ............................................................................................... 31
      3.2.2 SYSTEM MONITORING ....................................................................................................................... 31
      3.2.3 PROTECTION OF INFORMATION ....................................................................................................... 33
         3.2.3.1 RATING OF INFORMATION ........................................................................................................... 33
         3.2.3.2 ENCRYPTION ................................................................................................................................. 35
         3.2.3.3 BACKUP COPIES ............................................................................................................................ 36

National Cryptologic Centre
3.2.3.4 MAIL FLOW RULES ................................................................................................. 38
3.2.4 PROTECTION OF SERVICES .................................................................................. 39
3.2.4.1 EMAIL PROTECTION ......................................................................................... 39
3.2.4.2 PROTECTION AGAINST DENIAL OF SERVICE ................................................. 68

4. OTHER SECURITY CONCERNS ................................................................................. 69

4.1 TYPES OF MAILBOXES ............................................................................................ 69
4.2 DEVICE ACCESS AND QUARANTINE RULES ....................................................... 74
4.3 MAILBOX POLICIES FOR MOBILE DEVICES ....................................................... 75
4.4 SHARED USE POLICY .............................................................................................. 76

5. GLOSSARY AND ABBREVIATIONS ..................................................................... 78
1. EXCHANGE ONLINE

1.1 Description of the use of this guide

The purpose of this guide is to indicate the steps to follow for the configuration of the Exchange Online service, complying with the necessary requirements of the National Security Framework in its HIGH category.

This guide should be used in conjunction with [CCN-STIC-885A - Secure Configuration Guide for Office 365], which describes generalities of Office 365 and features common to all services, as well as a glossary of security terms and abbreviations used in these guides.

The following sources have been consulted for the preparation of this guide:

- Official Microsoft documentation.
- CCN-STIC-823 Cloud Services.
- ENS Royal Decree BOE-A-2010-1330.

1.2 Service definition

Exchange Online (EXO) is the email platform included with Office 365, a set of cloud-based applications and services hosted on Microsoft own servers and available from devices with Internet connection. It should also be noted that Office 365 runs on Microsoft Azure.

The main features of Exchange Online are:

- It provides the user with access to email, calendar, contacts and tasks from desktops, mobile devices and via web.
- Possibility of connection with Outlook client.
- Protection against spam and malware with Exchange Online protection.
- Fully integrated with Azure Active Directory.
- EXO servers are hosted in Microsoft Data Centers.

The Exchange Online subservices involved in this guide are:

- Microsoft Exchange Online Archiving. Provides archiving, compliance and eDiscover functionality.
- Protecting Microsoft Exchange Online. Email filtering service that helps to protect against spam and malware and allows to set policies to safeguard information.

1.3 Prerequisites for deployment using PowerShell

Office 365 PowerShell allows to manage and configure Exchange Online from the command line, with one user having management rights. See the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].
See prerequisites on the Microsoft page:
https://docs.microsoft.com/es-es/powershell/exchange/exchange-online/connect-to-exchange-online-powershell?view=exchange-ps

To manage Exchange Online settings from the command line on a local computer, a remote PowerShell session in Exchange Online has to be created.

1. Write down the credentials of Office 365.

```powershell
$UserCredential = Get-Credential
```

2. Provide the necessary connection settings.

```powershell
```

3. Import the Exchange Online cmdlets into the local Windows PowerShell session so they can be used.

```powershell
Import-PSSession $Session -DisableNameChecking
```

At the end do not forget to disconnect the remote session.

```powershell
Remove-PSSession $Session
```

To use Multi-Factor Authentication (MFA) to connect to Exchange Online PowerShell, you need to download and use the Exchange Online Remote PowerShell Module. To install the module from the Exchange Administration Center (EAC)

1. Connect to the Exchange Management Center using Internet Explorer or Edge.
2. In the [Hybrid] menu, click on the "Configuration" button to download the module.
2. ONLINE EXCHANGE DEPLOYMENT

*Exchange Online* does not require prior installation in the clients' *on-premise* environment, as it is an *online* service accessible from the Internet and hosted in the organization's Office 365 *tenant*. It uses the "Public Cloud" infrastructure referred to in the [823-Cloud Computing] guide.

*Exchange Online*, as well as the Office 365 set, is included in the *SaaS* (Software as a Service) category. The CSP (Microsoft) is responsible for offering the software as a service to the client.

2.1 Administrator - initial configuration

The *administrator* user can access the *Exchange Online administration portal* through the Office 365 administration portal (portal.office365.com).

These are the features listed in the left navigation panel.
<table>
<thead>
<tr>
<th>Area</th>
<th>What you can be done here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panel</td>
<td>An introduction to the administration center.</td>
</tr>
<tr>
<td>Recipients</td>
<td>View and manage mailboxes, groups, resource mailboxes, contacts, shared mailboxes, and mailbox migrations</td>
</tr>
<tr>
<td>Permits</td>
<td>Manage Administrator Roles, User Roles, and Policies of Outlook in the Web (formerly known as Outlook Web App)</td>
</tr>
<tr>
<td>Compliance Management</td>
<td>Manage local electronic document suspension and display, audits, data loss prevention (DLP), retention policies, retention labels, and journaling rules</td>
</tr>
<tr>
<td>Organization</td>
<td>Manage organizational and application sharing for Outlook</td>
</tr>
<tr>
<td>Protection</td>
<td>Manage your organization's malware filters, connection filters, content filters, outgoing spam, and quarantine.</td>
</tr>
<tr>
<td>Mail flow</td>
<td>Manage rules, message tracking, accepted domains, remote domains and connectors.</td>
</tr>
<tr>
<td>Mobile</td>
<td>Manage the mobile devices that allow to connect the organization. Mobile device access and mobile device mailbox policies can be managed.</td>
</tr>
<tr>
<td>Unified Messaging</td>
<td>Manage Unified Messaging (UM) dial-up plans and Unified Messaging IP gateways</td>
</tr>
</tbody>
</table>

### 2.2 End user - first steps

The end user can access the Office 365 portal through the url: portal.office365.com or www.office.com. After entering your credentials, a panel is displayed with all the applications you have access to.

Click on the Outlook icon to access the email client.
Environment configuration

1. From the **Configuration** menu in the upper right panel, click link: "View all Outlook settings."
2. Set options for the different categories.

- If a message containing online images is received, the images may not be secure and may pose a risk to personal data. *Outlook.com* helps to **protect data by loading external images with an image proxy**. It is recommended to have the following **check** activated, menu [General]\Privacy and data]:

- It is recommended to define an "**email signature**" and to include it automatically in the emails that are drafted. Menu [Mail]\Draft and respond.
- Apply rules to incoming mail. It is possible to move, mark, categorize or forward an incoming mail depending on the content. Menu [Mail\Rules].

In the example, when you receive an email that includes in the subject the word: keyword, it will be moved to the CCN-TEST folder.

- Spam. [Mail/Spam] menu.

You can specify individual senders or spam domains that will be automatically moved to the corresponding folder.

A list of secure senders can also be established:
And set a series of filters based on the options chosen:

- **Synchronize mail. Menu** [Mail\Synchronize email].

- **Message management.** The [Mail\Message management] menu.

Interesting options such as *Empty the Deleted Items folder* when closing the Outlook session, *mark read messages and read confirmations* are managed.
Retention Policies. Menu [Mail]\Retention policies].

These retention policies allow to set how long the message is kept in the mailbox. From this menu option you can choose the policies that will appear in the policies value drop-down list for each message.

From the message tray, by selecting one of them, the desired policy can be applied.
• **S/MIME.** [Mail/MIME] menu.

You can use S/MIME in Outlook Web App to enhance the security of your messages. Only recipients who have the correct key will be able to open a digitally encrypted message. A digital signature assures recipients that the message has not been altered.

S/MIME is a feature that must be enabled by the Administrator in advance to be available. Use the Get-SmimeConfig and set-SmimeConfig cmdlets to view and manage this feature in Exchange Online PowerShell. More information:

- **Groups.** Menu [Mail\Groups].

You can select the sending of an email copy every time you send an email to a group you are member of.

- **Events and invitations.** Menu [Calendar\Events and notifications].

- **Email events.** Menu [Calendar\Email Events]. Outlook automatically retrieves important events from supported senders from user e-mail and adds the items to your calendar. It is activated by default.
• **Shared calendars.** Menu \([\text{Calendar}\backslash\text{Shared calendars}]\). It allows to specify with whom the calendar is shared and what permissions you will have on it.

3. **ONLINE EXCHANGE CONFIGURATION**

The following will address the configuration of the *Exchange Online* service focusing on compliance with the National Security Framework requirements that apply exclusively to this service.

3.1 **Operational Framework**

3.1.1 **Access Control**

3.1.1.1 **Identification**

*Exchange Online* Identity Management is common to all Office 365 applications and is described in the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide.

3.1.1.2 **Entry requirements**

In the *Exchange Management Center*, you can view and manage mailboxes, groups, resource boxes, contacts, shared mailboxes, and mailbox migrations. For example, you can set permissions to access a shared mailbox, specifying the delegated users who are able to log in to the shared mailbox and whether they are allowed to "send as" on behalf of the shared mailbox. For more information, see [4.1 Types of Mailboxes].
3.1.1.3 Segregation of functions and tasks

Office 365 Exchange Online includes a wide variety of predefined permissions, based on the Role-Based Access Control (RBAC) permission model, which makes it easy to grant permissions to administrators and users.

- **Management Roles** - These roles contain permissions that can be assigned to administrators or specialist users using role groups that manage a part of the Exchange Online organization, such as recipients or compliance management.
- **End-user roles**: These roles, which are assigned through role assignment policies, allow users to manage aspects of their own mailbox and the distribution groups they own. End-user roles start with *Myprefix*.

**Role groups and role assignment policies**

Administration roles grant permissions to perform tasks in Exchange Online, but a simple method is needed to assign the roles to administrators and users. Exchange Online offers the following features to help you make your assignments:

- **Role groups**: role groups allow to grant permissions to administrators and specialist users.
- **Role assignment policies**: Role assignment policies allow to grant permissions to end users to change the settings of their own mailbox or distribution groups that they own.

More information about role groups and role assignment policies is shown in the following sections.

**Role groups**

To make it easier to assign multiple roles to an administrator, Exchange Online includes role groups. Role groups usually cover wider management areas, such as recipient management. They are only used with administration roles, i.e. they cannot be used with end-user roles. Members of role groups can be users of Exchange Online and other role groups.

The following figure shows the relationship between users, role groups and roles.
Exchange Online includes several integrated role groups, each of which gives permissions to manage specific areas of Exchange Online. Some role groups may overlap with other groups. The table below explains the use of each of the role groups.

<table>
<thead>
<tr>
<th>Role group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Management</td>
<td>Administrators or users who are members of <em>Discovery Management</em> can search mailboxes in the Exchange Online organization to find data that meets certain criteria and can configure legal retention of mailboxes.</td>
</tr>
<tr>
<td>Help Desk</td>
<td>By default, it lets members view and modify <em>Outlook Web App</em> options on the Web (formerly known as <em>Outlook Web App</em>) for any user in your organization. Among other things, the user’s display name, address or phone number can be changed. They don't include options that aren't available in <em>Outlook Web App</em> options, such as modifying the size of a mailbox or configuring the mailbox database where a mailbox is located.</td>
</tr>
<tr>
<td>Help Desk Administrators</td>
<td>Is member of the <em>View-Only Organization Management</em> role group and inherits permissions from this group. This role group cannot be managed in Exchange Online. You can add members to this role group by adding users to the Office 365 <em>Password administrator</em> role.</td>
</tr>
<tr>
<td>Organization Management</td>
<td>Administrators who are members of the group have administrative access to the entire Exchange Online organization and can perform virtually any task on any</td>
</tr>
<tr>
<td>Role Group</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exchange Online object</td>
<td>Exchange Online object, with some exceptions such as the Discovery Management role. Important: this is a very powerful role and must be granted with great caution.</td>
</tr>
<tr>
<td>Recipient Management</td>
<td>They have administrative access to create or modify Exchange Online recipients within the Exchange Online organization.</td>
</tr>
<tr>
<td>Records Management</td>
<td>They can configure compliance features such as retention policy labels, message classifications, and mail flow rules (also known as transport rules).</td>
</tr>
<tr>
<td>View-Only Organization Management</td>
<td>They can view the properties of all objects in your Exchange Online organization.</td>
</tr>
<tr>
<td>Compliance Management</td>
<td>They are responsible for compliance, to correctly configure and manage compliance settings in Exchange.</td>
</tr>
</tbody>
</table>

These role groups are displayed in the Exchange Administration Center, [permissions] menu.

1. Access the Exchange Administration Center as described in section [2.1.]
2. In the menu on the left, select the [permissions] option in the "Administrator Roles" tab.

From here you can **create new role groups**:

1. Press the "+" icon to create a new role.
2. Complete the form.

- Name the group.
- Description.
- Group roles.
- Group members.

Modifying role groups is also allowed:

A form like the one described above will appear where all values can be modified.

**Online Exchange permissions in Office 365**

When you create a user in Office 365, you can assign various management roles, some of which grant the user management permissions in Exchange Online. Consult guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

**3.1.1.4 Access rights management process**

**Role assignment guidelines**

Exchange Online provides *role assignment policies* that allow you to control the settings that users can configure in their own mailboxes and in the distribution groups they have. These options include display name, contact information, voice mail settings, and distribution group membership.
The Exchange Online organization may have several role assignment policies that provide different levels of permissions for various types of users in the organization. One of the organization's role assignment policies is marked as default.

These role assignment policies are displayed in the Exchange Administration Center, [Permissions] menu.

1. Access the Exchange Administration Center as described in section [2.1.]

2. In the menu on the left, select the [permissions] option in the "User Roles" tab.

By default, the policy "Default Role Assignment Policy" is defined, with the following characteristics:

**Default Role Assignment Policy**
This policy grants end users the permission to set their options in Outlook on the web and perform other self-administration tasks.

**Contact information**
- **MyContactInformation**
  This role allows users to modify their contact information, such as address and phone numbers.

**Profile Information**
- **MyProfileInformation**
  This role allows users to change their name.

**Distribution groups**
- **MyDistributionGroups**
  This role allows individual users to create, modify, and view distribution groups, and modify, view, add, and remove members to distribution groups they own.

**Distribution group memberships**
- **MyDistributionGroupMembership**
  This role allows users to view and modify their membership of distribution groups in an organization, as long as those groups allow the manipulation of group membership.

**Other Roles**
- **My Custom Apps**
  This role will allow users to view and modify their custom applications.
- **My Marketplace Apps**
  This role will allow users to view and modify their market applications.
- **My ReadWriteMailbox Apps**
  This role allows users to install applications with ReadWriteMailbox permissions.
- **MyBaseOptions**
  This role allows users to view and modify the basic configuration of their own mailbox and associated settings.
- **MyMailSubscriptions**
  This role allows users to view and modify their e-mail subscription settings, such as protocol default values and message formatting.
- **MyRetentionPolicies**
  This role allows individual users to view their retention tags, and view and modify their retention tag settings and default values.
- **MyTeamMailboxes**
This role allows individual users to create mailboxes on the site and connect SharePoint sites to them.

- MyTextMessaging

This role allows individual users to create, view, and modify their text messaging settings.

- MyVoiceMail

This role allows individual users to view and modify their voice mail settings.

New role assignment policies can be created from this panel:

1. Press the "+" icon to create a new role assignment policy.

2. Complete the form.

Or modify role assignment policies:
A form like the one described above will appear where all the values can be modified.

### 3.1.1.5 Authentication mechanisms

Information on password policies, MFA authentication and other authentication issues is shown in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

Simply note that modern authentication is **enabled by default in Exchange Online**, Skype Business Online and SharePoint Online.

**Modern authentication in Exchange Online**

Modern authentication in Exchange Online enables authentication features such as multi-factor authentication (MFA) using smart cards, certificate authentication (CBA), and third-party SAML identity providers. Modern authentication is based on the Active Directory Authentication Library (ADAL) and OAuth 2.0.

If modern authentication is disabled in Exchange Online, Windows-based Outlook clients that support modern authentication will use basic authentication to connect to Exchange Online mailboxes.

**Note:** Basic authentication is not recommended unless another authentication model is technically not supported. Basic authentication continuously transmits the combination of user and password, while modern authentication is based on an access token.

### 3.1.1.6 Local access

It is understood as **local access** to the access from the corporate network or authorized locations.

It requires the establishment of a "multi-factor authentication" (MFA) and an appropriate credential management policy, which are described in section [3.1.1.5 Authentication mechanisms]. A record of successful and unsuccessful system access attempts is also required, as described in section [3.1.2.2 Activity Record]. Additionally, access to Office 365 can be controlled through conditional access policies or rules in ADFS, as described in the guide [CCN-STIC-884A - Secure Configuration Guide for Azure].

Access to Exchange Online can be controlled through conditional access policies by network location in **Azure AD Management Center**.
1. Access the *Microsoft Administration Center 365*, menu [Azure Active Directory]. The *Azure Active Directory Administration Center* will open.

2. From the *Azure Active Directory Administration Center*, option [Business Applications\All the applications\Office 365 Exchange Online].
3. Access the [Conditional access] menu.

![Conditional access menu](image)

**Note:** Access to unmanaged devices can also be limited. Security measures can be relaxed when the computer is on one of the corporate subnetworks.

### 3.1.1.7 Remote Access

Remote access is understood as access from the Internet (any IP). It is recommended to reinforce security when accessed from the Internet (*only managed computers, MFA, device compliance, etc.*).

Everything can be managed from the Azure AD portal, as mentioned in previous sections.

It should be noted at this point that Office 365 is a *cloud* solution accessible by the end user through the Internet. Data encryption will be applied as described in section [3.2.3.2 Encryption].

### 3.1.2 Exploitation

*Exchange Online will always be up to date.* That is, the service is permanently maintained by Microsoft, taking care of updates and patches, as well as establishing the mechanisms for detection and protection against threats.

#### 3.1.2.1 Protection against malware

Office 365 includes a variety of threat protection features. Threat protection features are included in all Office 365 subscriptions; however, some subscriptions include more advanced features. The table below lists the protection features along with the minimum subscription requirements.
Exchange Online Protection (EOP) is a cloud-based e-mail filtering service that helps to protect your organization from spam and malware. Exchange Online Protection is included in Exchange Online and in any Office 365 plan that encompasses Exchange Online.

In addition, if an organization has Office 365 Advanced Threat Protection (Office 365 ATP), you it will have a real-time detection browser, accessible from the Office 365 Security and Compliance Center.

**Note:** O365 has unified all solutions at: https://protection.office.com/threatpolicy

See the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365] and section [3.2.4.1 Email Protection] of this guide.

<table>
<thead>
<tr>
<th>Type of protection</th>
<th>Subscription Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware protection</td>
<td>Exchange Online Protection EOP</td>
</tr>
<tr>
<td>Protection from malicious URLs and files in email and Office documents</td>
<td>Office 365 Advanced Threat Protection ATP</td>
</tr>
<tr>
<td>Anti-phishing protection</td>
<td>EOP</td>
</tr>
<tr>
<td>Advanced anti-phishing protection</td>
<td>Office 365 ATP</td>
</tr>
<tr>
<td>Spam protection</td>
<td>EOP</td>
</tr>
<tr>
<td>Zero-hour automatic purge (for email)</td>
<td>EOP</td>
</tr>
<tr>
<td>Audit log (used for reporting purposes)</td>
<td>Exchange Online</td>
</tr>
</tbody>
</table>

**ZAP (Zero-hour auto purge)**

Zero-hour automatic purge (ZAP) is an email protection feature that detects messages with *phish*, *spam* or malware. Allows to remove malicious content even after the message has been delivered to its recipient.

ZAP is available with the default Exchange Online protection that is included with any Office 365 subscription that contains Exchange Online mailboxes.

ZAP is enabled by default, but the following conditions must be met:

- *Spam* action is set to move the message to the spam folder.
- Users have kept their default *spam* settings and have not deactivated spam protection.

### 3.1.2.2 Activity Record

To configure the *Exchange* service activity record, it will be necessary to make use of the Audit functionality available through the *Office 365 Security and Compliance Center*. More information in this section of the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

From January 2019, Microsoft activates the mailbox *audit* log by **default** for all Office 365 organizations. This means that certain actions performed by mailbox owners, delegates and
administrators are automatically recorded and the corresponding mailbox audit logs are available when you search for them in the mailbox audit log. The actions that can be audited are:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>An item is copied to another folder.</td>
</tr>
<tr>
<td>Create</td>
<td>An item is created in the Calendar, Contacts, Notes, or Tasks folder in your mailbox. For example, a new meeting request is created. Please note that the creation of folders or messages is not audited.</td>
</tr>
<tr>
<td>FolderBind</td>
<td>Access to a mailbox folder is obtained</td>
</tr>
<tr>
<td>HardDelete</td>
<td>An item is deleted from the permanently recoverable Items folder.</td>
</tr>
<tr>
<td>MailboxLogin</td>
<td>The user is logged in to his mailbox.</td>
</tr>
<tr>
<td>MessageBind</td>
<td>An item is opened or accessed from the reading panel.</td>
</tr>
<tr>
<td>Move</td>
<td>An item is moved to another folder.</td>
</tr>
<tr>
<td>MoveToDeletedItems</td>
<td>An item is moved to the Deleted Items folder.</td>
</tr>
<tr>
<td>SendAs</td>
<td>A message is sent with the Send As permissions.</td>
</tr>
<tr>
<td>SendOnBehalf</td>
<td>A message is sent with the Send on behalf of permissions.</td>
</tr>
<tr>
<td>SoftDelete</td>
<td>An item is deleted from the Deleted Items folder.</td>
</tr>
<tr>
<td>Update</td>
<td>The properties of an item are updated.</td>
</tr>
</tbody>
</table>

**Check that mailbox auditing is enabled**

```powershell
# Get-OrganizationConfig | Format-List AuditDisabled
```

The `false` value indicates that mailbox auditing is enabled by default for the organization.

**Enable shared mailbox auditing**

In case it is deactivated, follow the next steps:

1. Initiate a remote PowerShell session as described in section [1.3 Prerequisites for Deployment via PowerShell].
2. Activate the mailbox audit.

```powershell
# Set-Mailbox "Shared Mailbox CCN1" -AuditEnabled $true
```

Audited actions for delegates on a shared mailbox are displayed with the following command:
Regarding the audit log for Exchange mailboxes, some specific examples of interesting searches are highlighted below:

**Searches related to shared mailboxes**

Example: "Detect if a delegated user has sent a mail on behalf of a shared mailbox”.

1. From the *Office Security and Compliance Center 365* menu [Search/Audit Log Search].
2. In activities select "A message has been sent with permission to Send as".
3. Select date ranges and click on the "Press" button.

4. Clicking on the activity field of any of the logs appears:

![Details of activity](image)

This displays, for example, information about the *delegated user* who sent the message, the *shared mailbox* (shown in the sender field) and the *date of issue*. 
Other types of searches

Other actions to be audited of mailboxes are shown in the following list:

**Journaling**

*Journaling* can help an organization to respond to legal, regulatory, and organizational compliance requirements by recording the incoming and outgoing email communications.

This objective is achieved by creating "journal rules", which contain the following key aspects:

- **Journal Rule Scope**: defines the messages that the journaling agent will log.
- **Journal Recipient**: Specifies the SMTP address of the recipient that you want to log in the journal.
- **Journal Entry Box**: Specifies one or more boxes used to collect journaling reports.

It is accessed from the *Exchange Administration Center*, menu [compliance management\journal rules].

---

When you "create a new journal rule" a form appears with the following information:
3.1.2.3 Incident Management


3.1.2.4 Protection of activity records

When a user or administrator performs an audited activity, an audit log is generated and stored in the organization's Office 365 audit log. See the corresponding section in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

3.2 Protection measures

3.2.1 Protection of communications

In terms of communications protection, it should be noted that the cryptographic protocols for TLS connections, which are automatically integrated into Office 365, are used. This is when:

- Users work with files stored in OneDrive For Business or SharePoint Online.
- Users share files in online meetings and instant messaging conversations.

In fact, all Office 365 communications are encrypted: Mail Clients (POP, IMAP, SMTP-TLS), Outlook Clients (MAPI-HTTPS), Browsers (Web HTTPS), Mobile Devices (ActiveSync HTTPS), Teams and Skype (SIP-TLS). No additional configuration is required, but it is important to note that as of June 2020, TLS 1.0 and 1.1 support will be removed. This has direct implications for customers.


3.2.2 System monitoring

Please refer to the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365] to see the different service monitoring mechanisms.

It should be noted that at the configuration level of alert policies, there are many activities related to Exchange. Some default alert policies are available if the organization has a corresponding add-on subscription in addition to an E1 or E3 subscription.

Here are some default alert policies related to this service:

<table>
<thead>
<tr>
<th>Default Alert Policy</th>
<th>Description</th>
<th>Office 365 Enterprise Subscription</th>
</tr>
</thead>
<tbody>
<tr>
<td>A click on a potentially malicious URL has been detected</td>
<td>Generates an alert when a user is protected by Office 365’s secure ATP links. This event is triggered when Office 365 ATP identifies changes in the URL or when users override Office 365 ATP secure link pages.</td>
<td>E5 or Office 365 ATP P2 add-on subscription</td>
</tr>
<tr>
<td>Feature Description</td>
<td>Description</td>
<td>Exchange Management Privilege Elevation</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td><strong>Creating a Forwarding/Redirect Rule</strong></td>
<td>Generates an alert when someone in the organization creates an inbox rule to forward or redirect messages to another e-mail account.</td>
<td>E1, E3 or E5</td>
</tr>
<tr>
<td><strong>Exchange Management Privilege Elevation</strong></td>
<td>Generates an alert when a user is assigned management permissions in the Exchange Online organization.</td>
<td>E1, E3 or E5</td>
</tr>
<tr>
<td><strong>Emails containing malware removed after delivery</strong></td>
<td>When malware messages are delivered to mailboxes in your organization, Office 365 removes infected messages from Exchange Online mailboxes.</td>
<td>E5 or Office 365 ATP P2 add-on subscription</td>
</tr>
<tr>
<td><strong>Emails containing phishing URLs removed after delivery</strong></td>
<td>Generates an alert when phishing messages are delivered to the organization’s mailboxes. If this event occurs, Office 365 removes the infected messages from the Exchange mailboxes online.</td>
<td>E5 or Office 365 ATP P2 add-on subscription</td>
</tr>
<tr>
<td><strong>Malware campaign detected after delivery</strong></td>
<td>Generates an alert when an unusually large number of messages containing malware are delivered to the organization’s mailboxes if this event occurs, Office 365 removes infected messages from Exchange Online mailboxes.</td>
<td>E5 or Office 365 ATP P2 add-on subscription</td>
</tr>
<tr>
<td><strong>Malware campaign detected and blocked</strong></td>
<td>Generates an alert when someone tries to send an unusually high number of e-mail messages containing some type of malware to users in the organization. If this event occurs, infected messages are blocked by Office 365 and are not delivered to mailboxes.</td>
<td>E5 or Office 365 ATP P2 add-on subscription</td>
</tr>
<tr>
<td><strong>Suspicious e-mailing patterns</strong></td>
<td>Generates an alert when someone in the organization has sent a suspicious email. This is an early warning that may indicate that the account is in danger, but not serious enough to restrict the user.</td>
<td>E1, E3 or E5</td>
</tr>
<tr>
<td><strong>Restricted tenant for sending email</strong></td>
<td>Generates an alert when most of the organization’s email traffic is detected as suspicious and Microsoft has restricted the email from being sent to the organization.</td>
<td>E1, E3 or E5</td>
</tr>
<tr>
<td><strong>Restricted user for the sending of email</strong></td>
<td>Generates an alert when a person in the organization has been restricted from sending mail. Typically, this occurs when an account is compromised, and the user appears on the restricted users page of the security &amp; compliance center.</td>
<td>E1, E3 or E5</td>
</tr>
</tbody>
</table>
3.2.3 Protection of information

3.2.3.1 Rating of information

Office 365 has several mechanisms for qualifying information, as explained in section [3.2.3.1 Qualifying Information] of the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide. Below are described several from the point of view of Exchange Online.

Retention labels

Retention labels are used to apply retention settings to individual folders and items, such as e-mails and voice mail. These settings specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age. When the message reaches the retention age, it is deleted or moved to the user's Local File mailbox.

**Note:** More information on creating retention labels is available in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

1. To apply a retention policy on an item, click on the "More actions" icon.
2. Then, click on the item [Assign policies] and select the corresponding retention label within "labels".

It is possible to select several elements in the folder and apply the "mass" policy:
O365 Sensitivity labels

Users need to collaborate with other users, both inside and outside the organization. This means that content no longer stays behind a firewall: it moves around, passing through devices, applications and services. And when it moves, it's required to be in a safe and secure manner that complies with the organization’s compliance policies. With sensitivity labels, it is possible to classify and help to protect sensitive content, without impeding users' productivity and ability to collaborate.

Note: More information on creating sensitivity labels is available in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

To apply a "Sensitivity label" simply access the [sensitivity] menu of the element and apply the corresponding label:

DLPs (Data Loss Prevention)

With these Data Loss Prevention policies, you can identify, monitor and protect sensitive information throughout Office 365. For example, you can set up policies to ensure that information in emails and documents is not shared with inappropriate contacts.
Note: More information on creating DLPs is available in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

3.2.3.2 Encryption

Encryption is the process by which information is encoded so that only an authorized recipient can decode and consume the information. Office 365 uses encryption in two ways: on the service and as a client control. On the service, encryption is used by default in Office 365. It is not necessary to configure anything. For example, Office 365 uses transport layer security (TLS) to encrypt the connection, or session, between two servers.

Previously, to send an encrypted message to someone outside your organization, you had to install the Office Message Encryption plug-in to encrypt your e-mail messages. The steps involved in encrypting a mail message were very different from the steps involved in restrictingIRM permissions.

With the latest updates to Office 365, users are provided with the same message security experience inside and outside the organization. In short, the sender does not have to worry about choosing the right encryption method for each recipient.

Recipients will see improvements as well. Regardless of the recipient's email provider or email application, you can read the encrypted message. If the recipients use Outlook, the experience is transparent. If you don't use Outlook, you'll receive a time-limited web view link that allows you to read the message. Without any software to install. Simply open the web view link to view the encrypted message.

**Send an encrypted message with Outlook**

On the message editing screen, press the "More actions" menu and then select the "Encrypt" option.

![Encrypted Message Screen]

From that moment the message will remain encrypted and the recipients will not be able to remove it.
Reading the email from another provider

The recipient will receive a message in their inbox with a link to open the message.

Even if such mail is forwarded to another email address, the encryption mechanism will require the authorized user to log in.

3.2.3.3 Backup copies

Office 365 has a very basic and time limited backup service.

It offers protection in case of hardware or software errors. To do this, Office 365 automatically creates a backup of all the emails sent and received, replicating Exchange mailboxes online to various databases in separate Microsoft data centers.

On the other hand, in case you delete an item by mistake, it is stored in a "Deleted Items" folder in Outlook.
When an item is deleted from the "Deleted Items" folder, it is moved to the "Recoverable Items" folder.

In Exchange Online, the retention period for deleted items is set to 14 days by default. Although this setting can be changed to a maximum of 30 days using PowerShell.

For example, to change the retention period of a mailbox to 30 days:

```powershell
Set-Mailbox -Identity "Buzon CCN1" -RetainDeletedItemsFor 30
```

To change the one in all user boxes:

```powershell
Get-Mailbox -ResultSize unlimited -Filter {{RecipientTypeDetails -eq 'UserMailbox'}} | Set-Mailbox -RetainDeletedItemsFor 30
```

In the case of accidentally deleted emails, after 14 days it is impossible to recover the file manually, and 30 days later not even Office 365 support guarantees to be able to recover it. Similarly, when an account is deleted, administrators have 30 days to request the restoration of the archive mailbox. After this period, recovery is no longer possible.

Finally, when one of the accounts contracted by the company is cancelled, Office 365 offers the possibility of recovering all the mail stored at the time of the deletion with the corresponding attachments, through its technical support service.

**Single Item recovery**

You can use Exchange Online PowerShell to enable or disable *single item recovery* in a mailbox. In Exchange Online, *single item recovery* is enabled by default when a new mailbox is created. Thus, messages that are permanently deleted (purged) by the user are retained in the "recoverable items" folder of the mailbox until the retention period of the deleted item expires. This allows the administrator to recover the messages purged by the user before the deleted item retention period expires. In addition, if a user or a process modifies a message, copies of the original item are also retained when *single item recovery* is enabled.

**Example:** enable *single item recovery* in the "CCN1 mailbox".

```powershell
Set-Mailbox -Identity "Buzon CCN1" -SingleItemRecoveryEnabled $true
```
Backups made by users in Outlook

In Exchange Online, the best way to provide a backup for users is to archive Exchange Online. It is not recommended to use Outlook to back up data to PST files due to loss of detectability and control of the content. See [4.1 Mailbox Types] for information on how to create mailboxes.

Local conservation and litigation hold

In-Place Hold

In Exchange Online, in-place hold includes a new model that allows to specify the following settings:

- **What to keep**: You can specify the items to be retained using query parameters such as keywords, senders and recipients, start and end dates, and also specify the types of message, such as mails or calendar items, that you want to put on retention.
- **Waiting time**: you can specify a duration for the waiting items.

**Example**: Create a local conservation, from PowerShell, with the name *Hold-CaseId012* and add the mailbox *joe@contoso.com* to the conservation.

```powershell
# New-MailboxSearch "Hold-CaseId012"-SourceMailboxes "joe@contoso.com" -InPlaceHoldEnabled $true
```

Litigation Hold

While in-place hold provides granular retention capability based on query parameters and the ability to set multiple suspensions, litigation hold only allows you to include all the suspended items. A duration period can also be specified for item retention when a mailbox is placed on litigation hold.

Litigation Hold uses the *LitigationHoldEnabled* property of a mailbox to put the contents of mailboxes on hold.

3.2.3.4 Mail flow rules

Mail flow rules (also known as transport rules) are used to identify and perform actions on messages that flow through the Exchange Online organization. Mail flow rules are similar to Inbox rules that are available in Outlook and Outlook Web App. The main difference is that mail flow rules act on messages while they are in transit and not after they are delivered to the mailbox.

They are accessed from the *Exchange Management Center*, [mail flow] menu.
A mail flow rule consists of conditions, exceptions, actions and properties:

- **Conditions**: identifies the messages to which you want to apply the actions. Some conditions examine message header fields (for example, the To, From, or Cc fields). Others examine message properties (for example, the subject, body, attachments, message size, or message classification).

- **Exceptions**: optionally, identifies the messages to which actions should not be applied.

- **Actions**: specifies what to do to messages that match the conditions of the rule and do not match any of the exceptions. Multiple actions are available, such as rejecting, deleting, or redirecting messages; adding more recipients; adding prefixes to the subject of the message; or inserting disclaimer notices in the message body.

- **Properties**: Specify other rules settings that are not conditions, exceptions, or actions. For example, the time period in which it is active.

### 3.2.4 Protection of services

#### 3.2.4.1 Email protection

Office 365 includes a variety of threat protection features.

**Exchange Online Protection (EOP)**

It is a cloud-based email filtering service that helps to protect your organization from spam and malware. Exchange Online Protection is included in Exchange Online and any Office 365 plan that encompasses Exchange Online.

Emails are automatically protected against spam and malware. Administrators do not need to configure and maintain the filtering technologies, which are enabled by default. However, they can make company-specific filter customizations in the Exchange administration center.

*If SharePoint Online is used as part of Office 365, malware protection is also automatically provided for files that are uploaded and stored in document libraries. This protection is provided by Microsoft’s anti-malware engine, which is also integrated into Exchange.

Below are the actions that can be performed in this regard through the Exchange Management Center, menu [protection].
**Malware filter**

Through the use of multiple anti-malware engines, EOP offers multi-layered protection designed to detect all known malware. The messages that are transported through the service are scanned for malware (viruses and spyware). If malware is detected, the message is removed. Notifications can also be sent to senders or administrators when an infected message is deleted and not delivered. You can also choose to replace infected attachments with default or custom messages that inform senders of the malware detection.

Malware filtering is automatically enabled throughout the organization using the default anti-malware policy. An administrator can view and edit, but not delete, the default anti-malware policy to better suit the needs of the organization. For greater granularity, you can also create **custom malware filter policies** and apply them to specific users, groups or domains in your organization. Custom policies always have priority over default ones.

1. Access the *Exchange Administration Center*, menu [protection\malware filter]. If there are no custom policies, only the default "Default" policy will be displayed.
2. To create a custom policy, click on the "New" icon. And then fill out the form.

3. Name and description.


   If malware is detected in an email attachment, the message will be quarantined and can only be released by an administrator. In this step you indicate if you want to inform users that their message has been quarantined, and the text of the warning.
5. Filter for common types of attachments

When enabled, emails with attachments of filtered file types will trigger the malware detection response (recommended).

![Filter for common types of attachments](image)

6. Customized notifications.

Whether to notify the sender (internal or external), the administrator and whether to customize and how the notification message.

![Customized notifications](image)

7. Who it applies to.

Specify the users, groups or domains for which this policy is valid by creating recipient-based rules.

![Who it applies to](image)

**Connection filtering**

To ensure that the e-mail sent by trusted people is not blocked, you can use the **connection filtering** policy to create a list of allowed IP addresses, also known as a safe sender list. You can also create a Blocked Senders List, which is a list of IP addresses, usually from known spammers, from which you never want to receive e-mails.

E-mails sent from an IP address on the block list are rejected, are not marked as spam, and no additional filtering takes place.
The connection filter policy setting applies to incoming messages only.

1. **Access** the *Exchange Administration Center*, menu [protection\connection filter].

2. **Modify** the "Default" policy to add new filter lists by clicking on the "Modify" icon.

3. **Specify** the IP address lists by clicking on the "Connection filtering" item.
IP addresses must be specified in the format nnn.nnn.nnn.nnn, where nnn is a number between 0 and 255. You can also specify CIDR ranges in the format nnn.nnn.nnn.nnn/rr, where rr is a number between 24 and 32.

It supports a maximum of 1273 entries, although to specify many IP addresses we recommend using PowerShell with the following command:

```
# Set-HostedConnectionFilterPolicy "CCN Connection Filter Policy" -IPAllowList @([Add]="192.168.2.10","192.169.3.0/24","192.168.4.1-192.168.4.5"; [Remove]="192.168.1.10")
```

4. Activate the check "Enable safe list", and "Save".

Microsoft subscribes to third-party sources from trusted senders. Using this safe list means that these trusted senders are not mistakenly marked as spam.

**Spam filter**

*Spam filter* settings include selecting the action to take when messages are identified as spam. The spam filtering policy settings apply only to incoming messages. There are two types:

- **Default**: Use to configure the spam filter for your entire organization. This policy cannot be renamed and is always enabled.
- **Custom**: Can be applied to specific users, groups or domains in your organization. Custom policies always are prioritary over the default.

1. Access the *Exchange Administration Center*, menu [protection\spam filter]. If there are no custom policies, only the "Default" policy will be displayed.

2. To create a custom policy, click on the "New" icon.
3. Enter name and description of the new policy.

4. Select the actions to be performed with bulk and spam.

The different types of actions to be carried out are:

- **Move message to the Spam folder**: Delivers the message to the Spam folder of the specified recipients.
- **Add X-header**: Sends the message to the specified recipients and adds X-header text to the message header to identify it as spam.
- **Prepend text over the subject line**: sends the message to the specified recipients but prepends text that was specified in the Prepend text to subject line entry box over the subject line.
- **Redirect the message to the e-mail address**: sends the message to a designated e-mail address instead of to the specified recipients. Specify the redirect address in the Redirect to this email address input field.
- **Delete message**: Deletes the entire message, including all the attached data.
- **Quarantine the message**: sends the message to the quarantine instead of the recipients. This action is the default for impersonation.

5. Select the threshold.

You can determine levels from which bulk mail will or will not be considered as spam, depending on the Bulk Complaint Level (BCL) of the message. You can choose a threshold value of 1 to 9, where 1 marks most bulk email as spam and 9 allows most bulk email to be delivered.
Microsoft uses internal and third-party sources to identify bulk mail and determine the appropriate BCL.


Always mark e-mails from the following senders or domains as spam.

Sometimes our filters can make a mistake, or the systems may need time to catch up. In these cases, the anti-spam policy allows you to create lists of allowed and blocked that invalidate the classification made by the filter. This option should be used sparingly, as the lists may become too large, and temporarily, as the filtering systems should work properly.
7. Establish allowed lists.

Always deliver e-mails from the following senders or domains to your inbox.

**WARNING:** Do not add domains owned by the organization or popular domains (for example, microsoft.com) to the list of allowed domains. This is considered a high-risk action, as it creates opportunities for dubious senders to send you mail that would otherwise be filtered out.

8. Specify international spam filtering.
9. Configure advanced spam filtering (ASF) options.

Advanced spam filtering (ASF) options give administrators the ability to inspect different content attributes of a message. The presence of these attributes in the message increases the spam score of the message (which increases the likelihood that it will be identified as spam):

Or mark it as spam:

```
Incrementar puntuación de correo no deseado
Especifique si se incrementará la puntuación de correo para los mensajes que incluyen estos tipos de vínculos o direcciones URL:

Vínculos de imagen a sitios remotos:
- [Desactivado]

Dirección IP numérica en URL:
- [Desactivado]

Redireccionamiento de direcciones URL a otro puerto:
- [Desactivado]

URL para sitios web .biz o .info:
- [Desactivado]

Marcar como correo no deseado
Especifique si se marcarán los mensajes que incluyen estas propiedades como correo no deseado:

Mensajes vacíos:
- [Desactivado]

JavaScript o VEScript en HTML:
- [Desactivado]

Etiquetas Frame o IFrame en HTML:
- [Desactivado]

Etiquetas Object en HTML:
- [Desactivado]

Etiquetas Embed en HTML:
- [Desactivado]

Etiquetas Form en HTML:
- [Desactivado]

Errores web en HTML:
- [Desactivado]

Aplicar lista de palabras confidenciales:
- [Desactivado]

Registro de SPF error:
- [Desactivado]

Filtrado de Id. del remitente condicional: error:
- [Desactivado]

Recibido masivo de correo electrónico no deseado de NDR:
- [Desactivado]
```
It is recommended to activate these advanced options in "Test Mode" and analyze the results before moving them into a production environment.

10. Specify to whom the policy applies.

Outgoing Spam

1. Access the Exchange Management Center, menu [protection\ outgoing spam].
2. Modify the "Default" policy by clicking on the "Modify" icon.
3. Specify preferences.

Notification for when a sender is restricted is now part of the Security and Compliance Center (SCC) alert platform. It is recommended to use this second option if you have the appropriate license. See section [3.2.2 System Monitoring] of the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide.

Quarantine

The quarantined items should be reviewed. You can release one or more messages to selected users or to all users. If an item was incorrectly detected as spam, a false positive can also be reported.

1. Access the Exchange Administration Center, menu [protection\quarantine].
It informs us that there is a new management page through the Security and Compliance Center. You can access it through the [Threat Management\Review] menu and the "Quarantine" widget, or through the url: https://protection.office.com/quarantine.

DKIM

DKIM (DomainKeys Identified Mail) is an authentication process that can help to protect both senders and recipients from spoofing and phishing emails.

DKIM signatures must be added to your organization’s domains so that recipients know that e-mail messages actually come from users in your organization and have not been modified after they are sent.

Office 365 automatically sets up DKIM for the initial "onmicrosoft.com" domains. That means that you don’t need to do anything to set up DKIM for any initial domain name.

The steps for setting up DKIM in Office 365 are:

1. Publish two CNAME logs for your custom domain in DNS.
2. Enable the DKIM signature for your custom domain in Office 365


1. Access the Exchange Administration Center, menu [protection].
2. Enable message signing for this domain with DKIM signatures.

Select the domain and press "Enable" on the right panel.

**Advanced Threat Protection (ATP)**

To deal with external threats and unknown risks, Office 365's "Advanced Exchange Online Threat Protection" (ATP) helps to protect mailboxes from sophisticated attacks in real time, eliminating the need to install additional virus scanning software. Every e-mail attachment or link that passes through the Exchange server is automatically evaluated for suspicious activity, and malicious content is neutralized before an attack occurs.

**Requirements**

ATP is included in Office 365 Enterprise E5, Office 365 Education A5 and Microsoft 365 Business, and can be added to other plans. See Microsoft documentation at:


**Protecting files with Microsoft Office 365 Advanced Threat Protection (ATP)**

It is a cloud-based e-mail filtering service that helps to protect the organization from viruses and malware by providing effective zero-day protection. It also includes features to protect the organization from harmful links in real time. ATP has rich URL tracking and reporting capabilities that provide administrators with information about the type of attacks that are occurring in the organization.
1. **Access the [advanced threats] menu. Either from the Exchange Administration Center:**

   ![Exchange Administration Center](image1)

   Or, for an enhanced threat management and viewing experience, it is more recommended the access through the Office 365 Security and Compliance, [Threat Management] menu.

   ![Office 365 Security and Compliance](image2)

   Clicking on "Configure secure ATP attachments" or "Configure ATP for SPO, ODB, Teams" links to the same panel accessed directly from the Exchange Management Center:

   ![Exchange Management Center](image3)
2. Click on “Activate ATP for SharePoint, OneDrive y Microsoft Teams”.

If a file in any SharePoint, OneDrive or Microsoft Teams library is identified as malicious, ATP will prevent users from opening or downloading it.

3. Configure a secure ATP attachment policy for specific users or groups in order to help to prevent users from opening or sharing e-mail attachments with malicious content.

3.1 Enter the name and description of the policy.

3.2 Specify response type on unknown malware in secure attachments.

Warning:
- The actions of Monitoring, Replacing and Blocking can cause considerable delays in the delivery of e-mails.
- *Dynamic Delivery* is only available to recipients with hosted mailboxes
- If the *Block*, *Replace* or *Dynamic delivery* options are chosen and malware is detected in the attachment, the message containing the attachment will be quarantined and only an administrator can release it.

> **Desactivado:** los datos adjuntos no se analizarán en busca de malware.
> **Supervisar:** seguir enviando el mensaje después de detectar el malware. Realizar un seguimiento de los resultados del análisis.
> **Bloquear:** bloquear el correo electrónico actual y los futuros y los datos adjuntos con malware detectado.
> **Sustituir:** bloquear los datos adjuntos con el malware detectado, seguir enviando el mensaje.
> **Entrega dinámica:** entrega el mensaje sin datos adjuntos inmediatamente y vuelve a adjuntarlos una vez finalizado el examen.

*Any option except "Deactivated" is recommended.*

3.3. Enable redirection and specify e-mail account for notification.

3.4. Specify who is affected by the policy.
4. Review policy in the policy panel.

ATP anti-phishing protection

ATP phishing protection, which is part of Office 365 Advanced Threat Protection, can help to protect the organization from phishing attacks based on spoofing and other phishing attacks. ATP is required for its use.

Although there is a basic anti-phishing policy for the online protection of Office 365 Exchange, with a limited set of anti-phishing protection.

Create an anti-phishing policy

Every organization in Office 365 has a default anti-phishing policy that applies to all users. Multiple custom anti-phishing policies can be created that can cover specific users, groups or domains within the organization. Any custom policies that are created take precedence over the default policy. Adding, editing, and deleting anti-phishing policies is done from the Office 365 Security and Compliance Center.
1. Access the Office 365 Security and Compliance Center, [Threat Management] menu, and then the "Phishing Protection" option.

2. On the "Phishing Protection" page, click on the "Create" button.

3. Enter name and description.
4. Specify the recipients or domains in the organization to which this anti-phishing policy will apply, or to which it will be excluded (for example, you can apply this policy on the organization's executive team).

5. Review and press the "Create this directive" button.

6. Then edit the anti-phishing policy.

**Edition of an anti-phishing policy**

When editing the *anti-phishing* policy, you can choose from several options, as described in the table below:

<table>
<thead>
<tr>
<th>This configuration</th>
<th>This result is obtained</th>
<th>Use it when desired:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applied to</strong></td>
<td>It defines the recipients whose incoming e-mails will be subject to the rules of the Policy. You can create conditions and exceptions for recipients associated with the Policy. For example, you can create a global policy for your organization by applying the rule to all recipients in your domain. You can also create exception rules, such as a rule that...</td>
<td>Each Policy must be associated with a set of users, for example, users in a particular group or domain.</td>
</tr>
</tbody>
</table>
doesn't scan e-mail messages from a specific group of recipients.

**Choose actions**

Choose the action that will be performed when Office 365 detects an attempt to impersonate users within an organization or from an outside organization. These actions are applied to any incoming e-mail that has been identified by Office 365 as an impersonation attempt for users who are under the protection of this Anti-Phishing Policy.

**Quarantined message.** The e-mail will be sent to the Office 365 quarantine. If this option is chosen, the email will not be sent to the original recipient.

**Move the message to the recipients' spam folder.** The e-mail will be sent to the recipients' spam folder. When you choose this option, the e-mail is still sent to the original recipient, but is not placed in the recipient's inbox.

**Do not apply any action.** The e-mail will be delivered to the original recipient's inbox. No other action will be taken on the e-mail.

When you want to perform an action on messages that Office 365 has determined to be an attempt to spoof internal or external domains as defined in the policy.

Follow the steps below to edit the policy from the *Office 365 Security and Compliance Center.*

1. Double-click on the policy name to edit it.
2. **Edit the impersonation policy.**

3. **Add users to be protected.**

   Add up to 60 internal and external users you want to protect from impersonation by attackers. We recommend that you add users with key roles in your organization.
4. Add users to be protected.

In most cases it is enough to activate the check "Automatically include domains belonging to me".

5. Configure "Actions to be performed".

Select an action if the email is sent by an impersonated user or impersonated domain.
Click "Activate phishing security tips", to display an email warning to the recipient, if the message is detected as a phishing attack.

It is recommended to activate the 3 checks.

6. Activate "Mailbox Intelligence".

Mailbox intelligence analyses the mail flow patterns of cloud-based users to determine which contacts are communicating most frequently. This helps to identify more easily when an e-mail could be from an attacker who is impersonating one of those contacts.
7. Add trusted domains and senders.

Messages from sender’s e-mail addresses and domains added here will never be classified as spoofing attacks. Therefore, the actions and settings of this policy will not apply to messages from these senders and domains.

8. Review settings and Save.
9. Edit the advanced impersonation threshold.
Secure Office 365 ATP links

Secure links help to prevent users from following links in e-mails and documents to websites considered as malicious. From this page you can configure policies that determine how all users in your organization, or only certain users, interact with secure links.

Access the secure links page

Through the Exchange Management Center, menu [advanced threats\safe links].

Although it is preferable to access through the Security and Compliance Center, menu: [Advanced Threats\Panel]
Or directly through the url: https://protection.office.com/safelinksconverged.

It is important to note that ATP Secure Link policies can be configured to scan URLs in e-mail and URLs in Office documents. From this point of view, it is recommended to follow the actions below.

Review and edit the default ATP secure link policy

1. Select the "Default" policy and click on the "Edit" icon.

2. Add blocked urls.

When the user clicks on a blocked url, they will be redirected to a web page where they will be told why it is blocked.
The "**" can be used as a wildcard symbol (up to a maximum of 3 per url).

3. **Activate the following parameters and "Save".**
Create secure ATP link policies for certain recipients

The next step is to define additional policies that will apply to specific recipients. For example, you can specify exceptions to the default policy by defining an additional policy.

1. In the main secure links panel, click on the "New" policy icon.

2. Specify the name and description of the policy.

   nueva directiva de vínculos a prueba de errores

   Nombre:
   OPP-directiva de vínculos seguros 1

   Descripción:
   OPP-directiva de vínculos seguros 1

3. Select "Activated" in the actions to be performed for unknown, potentially malicious URLs in messages.

   Selecciona las acciones a realizar para las direcciones URL desconocidas potencialmente malintencionadas en los mensajes.
   ○ Desactivado
   ○ Activado: las direcciones URL se mencionarán y se compararán con una lista de vínculos malintencionados conocidos cuando el usuario haga clic en el vínculo.

4. Select "Activated" in the following real-time analysis checks and apply to the entire organization.

   - Aplicar un análisis de URL en tiempo real para vínculos sospechosos y vínculos que apuntan a archivos.
   - Espere a que el análisis de URL se complete antes de entregar el mensaje.
   - Aplique vínculos seguros a los mensajes que se envíen en la organización.
5. Activate "Do not allow users to click to the original URL from the warning page if it is blocked".


*Urls* added to the "do not rewrite" list are excluded from ATP secure link analysis for the recipients you specify.

7. Specify to whom this policy applies and "Save".

3.2.4.2 Protection against denial of service

Office 365 provides advanced threat detection and mitigation systems to protect the underlying infrastructure from *denial of service* (DoS) attacks and prevent customer service disruption.

Azure's DDoS defense system is designed not only to withstand attacks from the outside, but also from other Azure tenants. Exchange Online and SharePoint Online request limitation mechanisms are part of a multi-layered approach to defend itself against DoS attacks.

Refer to the guide [CCN-STIC-884A - Secure Configuration Guide for Azure] for more information on *Azure’s DDoS defense system*. 
4. OTHER SECURITY CONCERNS

4.1 Types of mailboxes

There are several types of mailboxes in Exchange, the following explains what they are and later on we will see how they are created and managed.

- **User mailbox.** This is the traditional user mailbox so that Active Directory users can send and receive mail.
- **Archive mailbox.** The archive mailbox works as an auxiliary mailbox to a primary mailbox, enabling the possibility of having an online history. The mailbox archive can be a good option to replace or reduce the use of PSTs on the network.
- **Resource mailbox:** The resource mailbox is a special type of mailbox representing a board or equipment. The idea is that these can be included within a meeting and automate or facilitate the booking of these resources. This type of mailbox uses a disabled account in Active Directory and has specific properties different from a user mailbox.
- **Shared mailbox.** The shared mailbox is oriented to scenarios where we need a "generic" mailbox. For example, a multi-user Project mailbox. This mailbox would use a disabled account in Active Directory so there is no need to manage a password and it would not be possible to log in with the associated user.
- **Public folder mailbox.** This is a special type of "PublicFolder" mailbox where both hierarchy and content of these public folders are stored (which could be distributed in several mailboxes).
- **Remote mailbox.** This mailbox is used in a hybrid organization where there are mailboxes hosted On premises and others in Office 365. When a remote mailbox is created, an enabled user is configured for mail with an associated cloud mailbox.
- **Site mailbox.** This mailbox could be used when there is integration with Sharepoint, the idea is that the content is distributed in the most efficient type of storage; in Sharepoint the document part and in Exchange the e-mail part.

Access the Exchange Administration Center, [Recipients] menu.

a. **User mailbox**
   1. Access the Exchange Administration Center, [Recipients] menu.
   2. Select a user mailbox.
3. The right panel displays the **mailbox features** and allows you to enable or disable them.

   - **Enable or disable unified Messaging.** Unified Messaging combines voice and e-mail messaging into one mailbox that can be accessed from many different devices. Users can read or listen messages from their e-mail Inbox or from any phone if they use Outlook Voice Access.

   - **Enable or disable Exchange ActiveSync:** Exchange ActiveSync is an Exchange synchronization protocol that is optimized to work with high latency networks and low bandwidth. It allows mobile phone users to access their e-mail, calendar, contacts and tasks and allows them to still have access to this information when working offline.

   - **Enable or disable OWA (Outlook Web App) for Mobile Devices.**

   - **Convert to shared mailbox.** Shared mailbox is created.

   - **Enable or disable Local File.** Archive mailbox is created.

   - **Enable or disable OWA.**

b. **In-place archive mailbox.**

   To activate the "In-place File":

   1. Access the *Exchange Administration Center*, *[Recipients \mailbox]* menu.
   2. Select the main mailbox on which you want to activate the archiving.
   3. If it is not already enabled, click on the "Enable" link in the right panel of the mailbox features and then click on "Yes".
Once enabled, two new options will appear: "Disable | See details".

For the archiving details:

1. Access the mailbox features panel, as shown in the figure above.
2. Click on "See details".

An archive mailbox has its own archive quota and archive warning quota, it has no relation to the user mailbox storage quota.

c. **Shared mailbox.**

It is important to activate the "Shared Mailbox Audit" to allow traceability in these mailboxes, as described later in this section.

Create the "shared mailbox":

1. Access the *Exchange Administration Center, menu* [recipients\shared].
2. Press the "+" icon.
3. Complete form.

**Edit a shared mailbox**

1. **Access the Exchange Administration Center, menu** [recipients\shared].
2. **Double click on the name of the shared mailbox.**
3. **Edit the properties of the mailbox.**
So, for example, if we want to allow the delegate to send an email from this shared mailbox, we have to add their name to the "Send as" list. From the recipient's perspective, the mail is sent through this shared mailbox.

**Manage the shared mailbox in Outlook**

A delegated user can manage mails on behalf of the shared mailbox as follows:

1. Log on to Outlook Web App and click on the *User Account Management* icon in the upper-right panel.

2. *Click on “Open another mailbox”*. 

3. Enter the name of the shared mailbox.
4. Outlook opens with all the items in the shared mailbox.

Now you can send e-mails, read the received ones, etc.

Another way to send a mail on behalf of a shared mailbox without leaving the delegated user panel is:

1. Open Outlook with the identity of the delegated user.
2. Choose "New Mail".
3. If the "From" field does not appear at the top of the message, in options choose "Show sender"

Enable Audit on a Shared Mailbox

See section [3.1.2.2 Activity log].

4.2 Device access and quarantine rules

Many different clients can be used to access information in an Exchange Online mailbox. These clients include desktop programs such as Microsoft Outlook, Outlook on the Web (formerly known as Outlook Web App), and mobile clients, such as phones, tablets, and other mobile devices.

1. From the Exchange Administration Center, menu [mobile\mobile device access], you can access the Exchange ActiveSync settings:
2. Press the "Edit" button:

Note: It is recommended to set the value "Quarantine" or "Block Access" for devices that are not managed by a rule or personal exemption.

4.3 Mailbox policies for mobile devices

In Office 365, mobile mailbox policies can be created to apply a common set of policies or security settings to a collection of users. A default mobile device mailbox policy is created in each Office 365 organization.

Mobile device mailbox policies can be used to manage different configuration parameters. For example:

- Request a password.
- Specify the minimum password length.
- Allow a numeric PIN or require special characters in the password.
- Designate how long a device can remain inactive before asking the user to enter the password again.
- Delete a device after a specified number of incorrect password attempts.

It is accessed from the Exchange Administration Center, [mobile\mailbox policies for mobile devices] menu.

4.4 Shared use Policy

People in the organization may want to share calendars with individual business associates, friends or family. Sharing policies control how users share their calendars with others in the organization.

It is accessed from the Exchange Administration Center, menu [organization\shared use].
## Centro de administración de Exchange

### Uso compartido

Uso compartido de la organización

Habilita el uso compartido de la información de disponibilidad de calendario, y otro tipo de información, entre las organizaciones federadas de Exchange. [Más información]

<table>
<thead>
<tr>
<th>ACTIVADA</th>
<th>NOMBRE</th>
<th>DOMINIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No hay ningún elemento para mostrar en esta vista.

### Uso compartido individual

Uso compartido individual

Permite a los usuarios compartir información de calendario y contactos con organizaciones externas. [Más información]

<table>
<thead>
<tr>
<th>ACTIVADA</th>
<th>NOMBRE</th>
<th>DOMINIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Directivo predeterminado de uso compartido (P): Anónimo. Compartir con todos los dominios.
## 5. GLOSSARY AND ABBREVIATIONS

The following describes several security terms, acronyms and abbreviations used in this guide:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASF</td>
<td><em>Advanced Spam Filtering.</em></td>
</tr>
<tr>
<td>ATP</td>
<td>Microsoft Office 365 Advanced Threat Protection (ATP). It is a cloud-based email filtering service that helps to protect the organization from viruses and malware. ATP is included in Office 365 Enterprise E5, Office 365 Education A5 and Microsoft 365 Business, and can be added to other plans.</td>
</tr>
<tr>
<td>CNAME</td>
<td>A CNAME or <em>Canonical Name</em> record is a type of record that can be found in a DNS and allows the user to specify the alias of a domain name.</td>
</tr>
<tr>
<td>DKIM</td>
<td><em>DomainKeys Identified Mail.</em> It is an authentication process that can help to protect both senders and recipients from spoofing and phishing e-mails.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>E-mail box.</td>
</tr>
<tr>
<td>Outlook on the Web</td>
<td>Formerly known as Outlook Web App (OWA). It includes a web-based e-mail client, a calendar tool, a contact manager and a task manager.</td>
</tr>
<tr>
<td>Phishing</td>
<td><em>Impersonation.</em> Attack characterized by attempts to acquire sensitive information by fraud.</td>
</tr>
<tr>
<td>PST</td>
<td>These are Outlook data files (.pst), which are stored on the PC, and contain messages and other Outlook items.</td>
</tr>
<tr>
<td>Recipient</td>
<td>In an Exchange organization, it refers to people and resources. A <em>recipient is an</em> email-enabled object in AD to which Microsoft Exchange can deliver or route messages.</td>
</tr>
<tr>
<td>ENS Control</td>
<td>Configuration</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>op</td>
<td>Operational Framework</td>
</tr>
<tr>
<td>op.acc</td>
<td>Access Control</td>
</tr>
<tr>
<td>op.acc.1</td>
<td>Identification</td>
</tr>
<tr>
<td></td>
<td>The use of accounts and the assignment of licenses to users has been configured. Following the recommendations of Office 365 based on the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365]</td>
</tr>
<tr>
<td>Op.acc.2</td>
<td><strong>Entry Requirements</strong></td>
</tr>
<tr>
<td></td>
<td>The <em>permission levels</em> for the organization's resources - owners, members and visitors - have been checked.</td>
</tr>
<tr>
<td>Op.acc.3</td>
<td><strong>Segregation of functions and tasks</strong></td>
</tr>
<tr>
<td></td>
<td>Exchange Online roles and role groups have been properly assigned.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence collected:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence collected:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Op.acc.4</td>
<td>Access rights management process</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Role assignment policies have been created and/or edited.</td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Op.acc.5</th>
<th>Authentication mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to applications that do not use modern authentication has been blocked. Following the recommendations of section 3.1.1.5 Authentication Mechanisms in the [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide</td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Op.acc.6</th>
<th>Local access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor authentication is enabled, and an appropriate credential management policy is in place. Conditional access policies or rules have been configured in ADFS, as described in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].</td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Op.acc.6</td>
<td>Local access</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>A record of successful and unsuccessful access attempts to the system is available. As mentioned in the section on activity records.</td>
<td></td>
</tr>
</tbody>
</table>

**Evidence collected:**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

**Comments:**

**Op.acc.6 Local access**

*Network Location* has been activated to allow access only from certain IP addresses. And the access limitation to the administrators.

**Evidence collected:**

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

**Comments:**

**Op.acc.7 Remote Access**

Conditional access policies have been configured for remote access, as described in the guide [CCN-STIC-885A - Secure Configuration Guide for Office 365].

**Evidence collected:**

<table>
<thead>
<tr>
<th></th>
<th>Si</th>
<th>No</th>
</tr>
</thead>
</table>

**Comments:**
<table>
<thead>
<tr>
<th>op.exp</th>
<th>Exploitation</th>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>op.exp.6</td>
<td><strong>Protection against malware</strong></td>
<td>□ Yes □ No</td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>The requirements for ZAP (Zero-hour auto purge) operation are met, as described in section 3.1.2.1 Protection against malware [CCN-STIC-885A - Secure Configuration Guide for Office 365] guide.</td>
<td>Evidence collected:</td>
<td>Comments:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□ Yes □ No</td>
<td></td>
</tr>
</tbody>
</table>

| op.exp.6     | **Protection against malware**                                                                  | It applies: | It complies: |
|              | Real-time threat detection, accessible from the *Office 365 Security and Compliance Center*, is recommended. | □ Yes □ No  | □ Yes □ No  |
|              | *For these tasks the organization must have *Office 365 Advanced Threat Protection* (Office 365 ATP). | Evidence collected: | Comments: |
|              |                                                                                                 | □ Yes □ No  |             |

<p>| op.exp.8     | <strong>Recording user activity</strong>                                                                     | Aplica: | Cumple: |
|              | The audit log has been activated.                                                               | □ Yes □ No | □ Yes □ No |
|              |                                                                                                 | Evidencias Recogidas: | Observaciones: |
|              |                                                                                                 | □ Yes □ No |             |</p>
<table>
<thead>
<tr>
<th>op.exp.8</th>
<th><strong>Recording user activity</strong></th>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It has been verified that the audit of shared mailboxes is activated.</td>
<td></td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evidence collected:</td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>op.exp.10</td>
<td><strong>Protection of activity records</strong></td>
<td>It applies:</td>
<td>It complies:</td>
</tr>
<tr>
<td></td>
<td>Consultation of the activity record has been secured by establishing the appropriate roles.</td>
<td></td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td></td>
<td>Likewise, the point is the search within the record and its correct operation.</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evidence collected:</td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>op.exp.10</td>
<td><strong>Protection of activity records</strong></td>
<td>It applies:</td>
<td>It complies:</td>
</tr>
<tr>
<td></td>
<td><em>Journaling</em> rules have been created to conform to the organization’s compliance policies.*</td>
<td></td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evidence collected:</td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Comments:</td>
<td></td>
</tr>
<tr>
<td>op.mon</td>
<td>System monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alerts have been set up in the <em>Office 365 Security and Compliance Center</em>.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp</th>
<th>Protective Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>mp.info</td>
<td>Protection of information</td>
</tr>
<tr>
<td>mp.info.2</td>
<td>Rating of information</td>
</tr>
<tr>
<td>Retention policies have been implemented.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.info.2</th>
<th>Rating of information</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Sensitivity labels</em> have been applied.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.info.2</th>
<th>Rating of information</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Sensitivity labels</em> have been applied.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence collected:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evidence collected:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>mp.info.3</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.info.9</th>
<th><strong>Backup copies</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Retention policies have been applied to manage the storage time of documents and mail.</td>
<td><strong>It applies:</strong></td>
<td><strong>It complies:</strong></td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
<td>☐ Yes ☐ No</td>
<td>Comments:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.info.9</th>
<th><strong>Backup copies</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The use of <strong>Single Item Recovery</strong> is controlled.</td>
<td><strong>It applies:</strong></td>
<td><strong>It complies:</strong></td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
<td>☐ Yes ☐ No</td>
<td>Comments:</td>
</tr>
<tr>
<td>mp.info.9</td>
<td><strong>Backup copies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copies have been made with the Exchange archive.</td>
<td>It applies: ☐ Yes ☐ No</td>
<td>It complies: ☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td>Evidence collected: ☐ Yes ☐ No</td>
<td>Comments:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.info.9</th>
<th><strong>Backup copies</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><em>In-place conservation or litigation hold</em> have been applied.</td>
<td>It applies: ☐ Yes ☐ No</td>
</tr>
<tr>
<td>Evidence collected: ☐ Yes ☐ No</td>
<td>Comments:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.info</th>
<th><strong>Mail flow rules</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail flow rules have been created for the Exchange Online’s organization.</td>
<td>It applies: ☐ Yes ☐ No</td>
</tr>
<tr>
<td>Evidence collected: ☐ Yes ☐ No</td>
<td>Comments:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.s</th>
<th><strong>Protection of services</strong></th>
</tr>
</thead>
</table>

---

**Secure Setup Guide for Exchange Online**
<table>
<thead>
<tr>
<th>mp.s.1</th>
<th><strong>E-mail protection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Malware filters have been applied.</td>
</tr>
<tr>
<td></td>
<td>It applies:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>It complies:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>mp.s.1</td>
<td><strong>E-mail protection</strong></td>
</tr>
<tr>
<td></td>
<td>Connection filters have been applied.</td>
</tr>
<tr>
<td></td>
<td>It applies:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>It complies:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>mp.s.1</td>
<td><strong>E-mail protection</strong></td>
</tr>
<tr>
<td></td>
<td><em>Both incoming and outgoing spam</em> filters have been applied.</td>
</tr>
<tr>
<td></td>
<td>It applies:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>It complies:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>□ Yes □ No</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
<tr>
<td>mp.s.1</td>
<td>E-mail protection</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td><em>Quarantined</em> emails have been checked.</td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.s.1</th>
<th>E-mail protection</th>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DKIM authentication process have been configured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.s.1</th>
<th>E-mail protection</th>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Advanced Threat Protection (ATP) and anti-phishing ATP have been configured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evidence collected:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mp.s.1</td>
<td><strong>E-mail protection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ATP secure links policies have been checked.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>It applies: Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>It complies: Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evidence collected: Yes No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mp.s.8</th>
<th><strong>Protection against denial of service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The information detailed in the [CCN-STIC-884A - Secure Configuration Guide for Azure] guide on Azure's DDoS defense system has been taken into account.</td>
</tr>
<tr>
<td></td>
<td>It applies: Yes No</td>
</tr>
<tr>
<td></td>
<td>It complies: Yes No</td>
</tr>
<tr>
<td></td>
<td>Evidence collected: Yes No</td>
</tr>
<tr>
<td></td>
<td>Comments:</td>
</tr>
</tbody>
</table>

**OTHER SECURITY CONCERNS**

<table>
<thead>
<tr>
<th>ActiveSync</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveSync has been configured for mobile devices.</td>
</tr>
<tr>
<td>It applies: Yes No</td>
</tr>
<tr>
<td>It complies: Yes No</td>
</tr>
<tr>
<td>Evidence collected: Yes No</td>
</tr>
<tr>
<td>Comments:</td>
</tr>
</tbody>
</table>
## Mailbox policies for mobile devices

Mailbox policies have been created for mobile devices.

<table>
<thead>
<tr>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes □ No</td>
<td>□ Yes □ No</td>
</tr>
</tbody>
</table>

Evidence collected:

| □ Yes □ No |

Comments:

## Shared use policies

Share use policies have been created.

<table>
<thead>
<tr>
<th>It applies:</th>
<th>It complies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Yes □ No</td>
<td>□ Yes □ No</td>
</tr>
</tbody>
</table>

Evidence collected:

| □ Yes □ No |

Comments: