

## 请立即采取行动：Exchange Online 服务即将停用基本身份验证

**[重要信息，请务必仔细阅读并尽快采取行动]** 2022/10

### 信息背景：

作为一种设置简单的身份验证方式，基本身份验证（也称旧式身份验证）一直被多种应用程序广泛使用，来完成到服务器、服务和 API 结点的连接。但基本身份验证在请求连接时会发送用户和密码，并将这些凭据保存在存储或设备上，导致凭据更容易被恶意捕获，增加了用户身份被盗等一系列安全风险。

为了提升企业和用户的安全性，微软决定自 2022 年 10 月 1 日起，在全球范围内对使用 Exchange Online 的用户逐步关闭基本身份验证，以更为高级的现代身份验证方式取代。微软自 2021 年 9 月起持续通过官方网站以及管理中心中的“消息中心”发布提醒(MC345821)，并将持续每月对依然使用基本身份验证的客户进行“消息中心”提醒。此文章也为提醒您预先做好准备。

目前针对国际版 Office 365 的 Exchange Online，已经全面关闭基本身份验证。本文后续内容，将主要针对世纪互联版 Office 365 的 Exchange Online 用户所需要了解的内容，以及需要采取的行动进行说明。

具体信息请仔细阅读以下内容。

### 变更时间表：

对于未使用基本身份验证的租户：

- 自 2022 年 10 月起，对于尚未使用基本身份验证的租户，会陆续在消息中心中收到 7 天后对该租户关闭基本身份验证的通知，关闭完成后将再次收到通知。

对于正在使用基本身份验证的租户：

- 使用由世纪互联运营的 Office 365 服务的租户将于 2023 年 3 月 31 日起全面关闭基本身份验证，在此之后，您无法以任何形式申请例外。
- 我们强烈推荐客户根据自身情况，提前对某些协议关闭基本身份验证，以便得到尽可能早的保护。您可以通过下面列出的步骤自己操作，或者申请相关技术支持。

### 可能的影响及其范围：

微软将关闭以下协议的基本身份验证：Exchange ActiveSync (EAS), POP, IMAP, Remote PowerShell, Exchange Web Services (EWS), Offline Address Book (OAB), Outlook for Windows/Mac。(SMTP 协议不受影响)。

关闭后，对上述受影响协议使用了基本身份验证的任何客户端(用户应用、脚本、集成等)都将无法连接 Exchange Online。应用将收到“HTTP 401 错误：用户名或密码错误”这样的信息。

### 您需要采取的动作：

#### 第一步 - 确定是否会受到影响

##### 1. 检查消息中心

从 2021 年底开始，我们开始向租户发送消息中心通知，总结基本身份验证在租户环境内的使用情况。如果您收到了使用情况的摘要，你可以了解在上个月内使用基本身份验证的用户数，以及他们使用的协议数，这表明某些内容或某人正在使用基本身份验证。

2. 通过 Azure Active Directory 登陆日志进一步了解基本身份验证的使用情况。

Azure AD Free 订阅可以查看过去 7 天的登陆日志；Azure AD P1/P2 可以查看过去 30 天的登陆日志。通过筛选客户端应用，对新式和旧式身份验证加以区分。其中，浏览器、移动应用和桌面客户端被视为新式身份验证，而其他应用（如 IMAP、POP 和 MAPI 等）则被视为旧式身份验证。您可以根据了解到的使用情况制定方案，来避免影响。

The screenshot shows the Azure AD login logs interface. At the top, there are filters for '日期: 前 24 小时', '日期显示形式: 本地', and '客户端应用: 已选定 2 个'. A dropdown menu titled '客户端应用' is open, showing two categories: '新式身份验证客户端' (Modern authentication clients) with options for '浏览器' (Browser) and '移动应用和桌面客户端' (Mobile and desktop clients); and '旧式身份验证客户端' (Legacy authentication clients) with options for 'Exchange ActiveSync' and 'Exchange Online Powershell'. Below the filter, a table of login events is visible with columns for '日期', '请求 ID', and '用'.

3. 通过 Outlook 客户端判断是否在使用基本身份验证。

按住 CTRL，右键单击系统托盘中的 Outlook 图标并选择“连接状态”来选中连接状态对话框。如 Authn 列显示为 Clear，说明 Outlook 在使用基本身份验证；如显示为 Bearer，则代表 Outlook 在使用新式身份验证。

The screenshot shows the 'Outlook Connection Status' dialog box. It has two tabs: 'General' and 'Local Mailbox'. The 'General' tab is active, showing an 'Activity' table with columns: 'Server name', 'Status', 'Protocol', 'Authn', 'Encrypt', 'RPCPort', 'Type', 'Req/Fail', and 'Avg Res'. The 'Authn' column shows 'Bearer\*' for all entries, indicating modern authentication is being used. A green arrow points to the 'Bearer\*' entry in the last row.

4. 在移动设备上确认身份验证方式：

在移动设备上，如果设备尝试用新式身份验证进行连接，会显示类似基于 Web 的登录页(下图左侧)。基本身份验证则显示为凭据输入对话框(下图右侧)。

The first screenshot on the left shows a Microsoft product series login page. It has the Microsoft logo and the text 'Microsoft 产品系列' and '登录'. Below that, it says '电子邮件、电话或Skype' and has a text input field. There are links for '没有帐户？创建一个！' and '无法访问你的帐户？'. At the bottom, there are '上一步' and '下一步' buttons, and a '登录选项' link.

The second screenshot on the right shows a 'Windows Security' dialog box titled 'Connecting to' and 'Enter your credentials'. It has input fields for 'User name', 'Password', and 'Domain:'. There is a checkbox for 'Remember my credentials' and 'OK' and 'Cancel' buttons at the bottom.

## 第二步 – 处置方式

如果您确认自己的租户将受到影响，请参照如下建议进行应对：

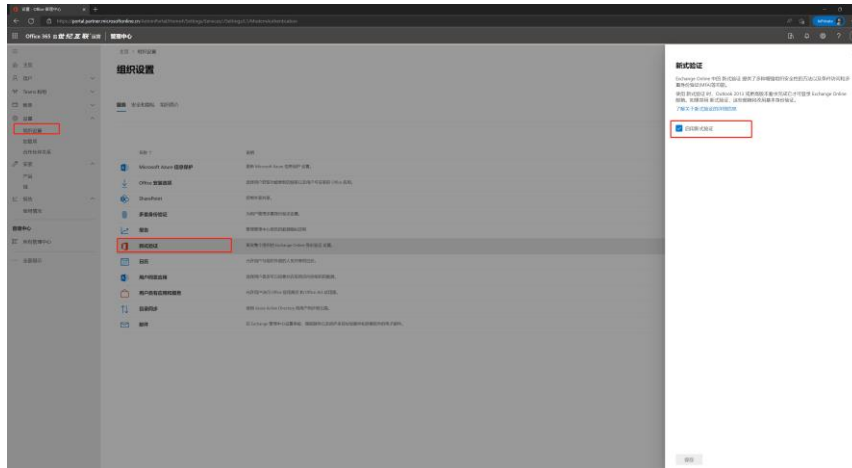
- 在目录中启用新式身份验证（2017 年 8 月 1 日以后创建的目录已默认启用）
  - 参考在[目录中启用新式身份验证](#)中的步骤为您的 Azure 目录启用新式身份验证。
  - 为 [Exchange Online 启用新式身份验证](#)
- 变更代码
  - 如果您使用受影响的协议编写自己的代码，请更新代码，使用 OAuth 2.0，或 Graph API。
  - 如果您使用的第三方应用程序在使用这些协议，请联系该第三方应用的开发人员。更新程序，以支持 OAuth 2.0 验证，或帮助用户切换到使用 OAuth 2.0 验证的应用程序。
- 对不同的客户端进行相应调整

协议/服务	受影响的客户端	调整项	参考文档/备注
Outlook	适用于 Windows 和 Mac 的所有 Outlook 版本	<ul style="list-style-type: none"> <li>✓ 适用于 Windows 的 Outlook 升级到 2013 或更高版本</li> <li>✓ 适用于 Mac 的 Outlook 升级到 2016 或更高版本</li> <li>✓ 如果使用适用于 Windows 的 Outlook 2013，请通过<a href="#">注册表项</a>启用新式身份验证</li> </ul>	
EWS	EWS 托管 API 应用程序-用于访问邮箱和日历数据	<ul style="list-style-type: none"> <li>✓ 修改 EWS 应用程序代码，使用 OAuth 新式身份验证访问 Exchange Online</li> <li>✓ 2018 年 7 月开始不再有 EWS 的功能更新。强烈建议使用基于 Graph API 的应用程序</li> </ul>	<a href="#">使用 OAuth 对 EWS 应用程序进行身份验证   Microsoft Docs</a> <a href="#">Outlook 邮件 API 概述 - Microsoft Graph   Microsoft Docs</a>
远程 PowerShell	Exchange 管理员 <a href="#">委派的管理员权限</a> 自动化管理工具	<ul style="list-style-type: none"> <li>✓ 使用 Exchange Online V2 PowerShell 模块</li> </ul>	详细了解 <a href="#">EXO V2 模块的自动化和基于证书的身份验证支持</a>
POP、IMAP 和 SMTP AUTH	已配置为使用 POP3 和 IMAP4 的客户端应用程序	<ul style="list-style-type: none"> <li>✓ 使用 OAuth 身份验证与 IMAP、POP 或 SMTP 协议连接来访问用户的电子邮件数据</li> <li>✓ 迁移到其他协议，POP3 和 IMAP4 提供对 Exchange Online 的基本电子邮件功能的访问，但不提供丰富的电子邮件、日历和联系人管理</li> </ul>	<a href="#">使用 OAuth 对 IMAP、POP 或 SMTP 连接进行身份验证</a>
Exchange ActiveSync	苹果、三星等移动设备原生	<ul style="list-style-type: none"> <li>✓ 使用适用于 iOS 和 Android 的 Outlook 应用或其他支持</li> </ul>	iOS 用户请在 Apple Store 下载，Android 用户优先在主要的国内

(EAS)	的电子邮件应用	新式身份验证的移动电子邮件应用	Andriod 应用市场下载 (请认准发布者 为“微软”) 另外, APK 单独下载 <a href="https://www.microsoft.com/zh-cn/download/details.aspx?id=103939">https://www.microsoft.com/zh-cn/download/details.aspx?id=103939</a>
-------	---------	-----------------	--

### 第三步 – 关闭基本身份验证

1. 确保经上述步骤后, 租户中以及 Exchange Online 已经启用新式身份验证, 且客户端支持并已启用新式身份验证。
2. 在不同场景下禁用基本身份验证。
  - 针对 Outlook for Windows, 为整个租户启用新式验证 **[强烈推荐]**  
设置-组织设置-启用新式验证



- [创建身份验证策略](#), 针对具体的协议和用户/组, 关闭基本身份验证
- 针对特定用户和组, 通过条件访问阻止旧式身份验证。支持“仅报告”模式进行登陆评估 (实时查看哪些用户使用旧式身份验证, 但并不会真正阻止连接)。

## 根据模板创建新策略(预览版) ...

 得到反馈?

自定义版本 **选择模板** 审阅 + 创建

基于你的响应, 我们建议使用以下模板

- |  |   |  |
|--|---|--|
| <input type="radio"/> 需要为管理员进行多重身份验证<br>需要对特权管理帐户进行多重身份验证, 以降低入侵风险。此策略将针对与“安全默认”相同的角色。<br><a href="#">查看策略摘要</a> | <input type="radio"/> 保护安全信息注册<br>保护用户注册 Azure AD 多重身份验证和自助服务密码的时间和方式。<br><a href="#">查看策略摘要</a>                      | <input checked="" type="radio"/> 阻止旧版身份验证<br>阻止可用于绕过多重身份验证的旧式身份验证终结点。<br><a href="#">查看策略摘要</a>                    |
| <input type="radio"/> Azure 管理需要多重身份验证<br>需要多重身份验证来保护对 Azure 资源的特权访问。<br><a href="#">查看策略摘要</a>                  | <input type="radio"/> 风险登录需要多重身份验证<br>如果检测到中或高登录风险, 则需要进行多重身份验证。(需要 Azure AD Premium 2 许可证)<br><a href="#">查看策略摘要</a> | <input type="radio"/> 需要为高风险用户更改密码<br>如果检测到高用户风险, 则需要用户更改其密码。(需要 Azure AD Premium 2 许可证)<br><a href="#">查看策略摘要</a> |

命名策略

CA003: 阻止旧版身份验证

策略状态

关闭  打开  仅报告

### 帮助和支持

如果您在此变更过程中有任何疑问或遇到任何问题, 您可以通过以下途径联系微软, 我们将竭诚为您提供技术支持:

- 如果您是 Premier/Unified 客户, 可以通过 [Service Hub](#) 提交 Ticket 或拨打 7\*24 支持电话 8008201859 或 4008201859。
- 如果您不是 Premier/Unified 客户, 可以通过 Admin Center 提交 Support Ticket 或拨打支持电话 400-089-0365 (针对世纪互联运营的 Office 365, 法定工作日 9: 00 – 18: 00)

其他官方参考文档:

<https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online>