# 為Secure Access中的Microsoft 365服務建立有效的「不解密」清單

## 目錄



## 簡介

本文描述建立不解密清單以繞過Microsoft 365域的有效方法，即通過Secure Access中的IPS解密。

## 問題

Microsoft 365流量通過SSL檢查引擎、代理或IPS時已知會導致問題。
Microsoft根據知識庫文章，建議繞過分類為「允許和最佳化」的域和IP:

https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

安全訪問中的當前Microsoft 365相容性功能僅適用於流量 通過代理。
因此，啟用此功能後，不會在代理級別對此流量應用解密或檢查，但是全域性IPS解密設定仍然適用。

啟用IPS解密和Microsoft 365相容性功能時，在以下情況下仍會解密網際網路目標流量：

- 全通道RAVPN
- 通過VPN隧道安全訪問Internet

Microsoft 365流量解密所導致的問題的典型症狀：

- 通過Outlook傳送電子郵件的速度緩慢
- sharepoint的效能問題
- 使用Teams時使用者體驗不佳

# 臨時解決方法

客戶必須繞過目的地為Allow和Optimize from IPS解密的域的流量：

手動建立此類清單相當繁瑣，因此Python指令碼可用於從Microsoft API動態提取清單：
https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

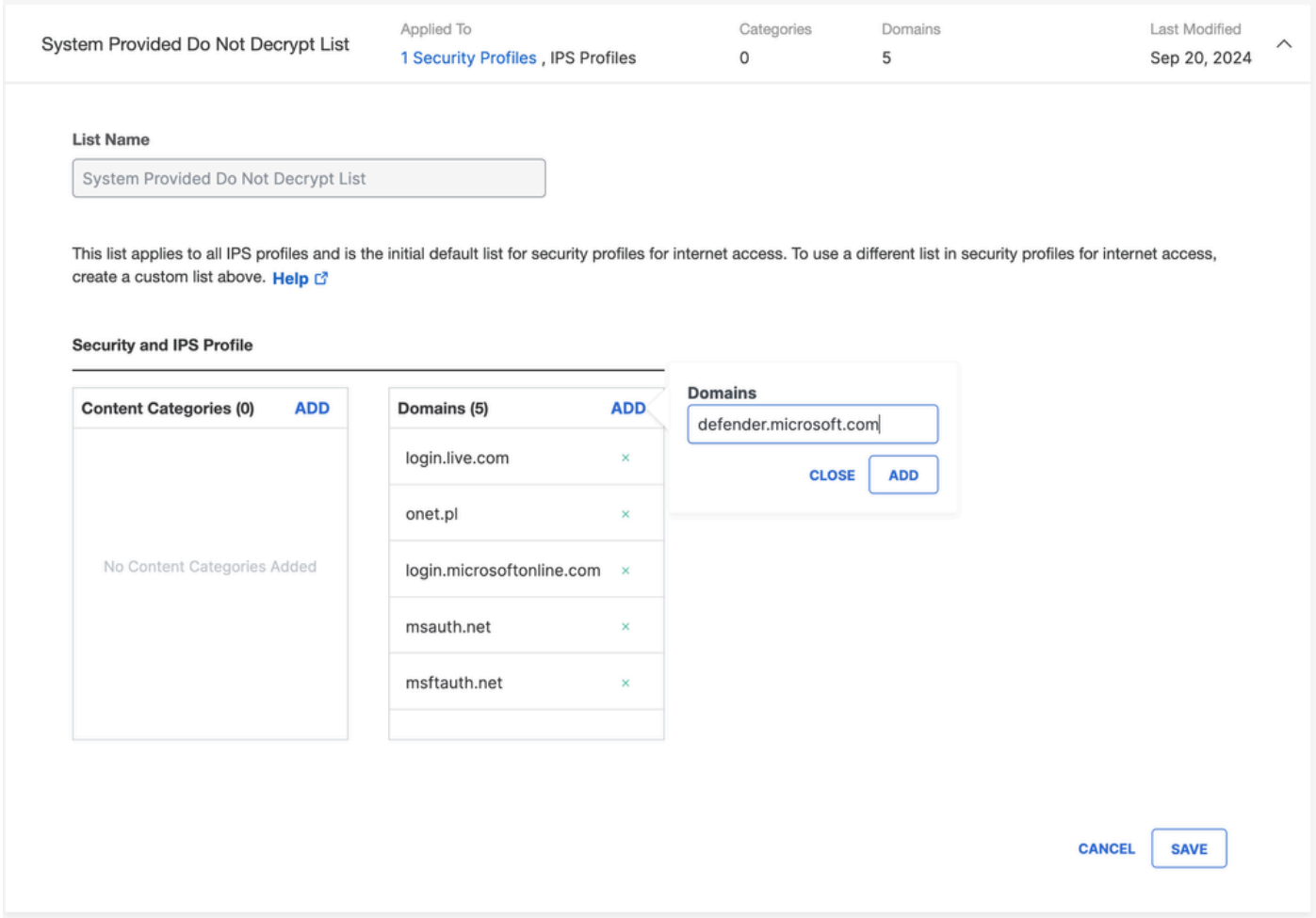
```
import requests

def get_fqdns(url):
    try:
        response = requests.get(url)
        response.raise_for_status()
        data = response.json()

        fqdns = []
        for item in data:
            if item.get('category') in ['Allow', 'Optimize']:
                for fqdn in item.get('urls', []):
                    fqdns.append(fqdn)

        return fqdns

    except requests.exceptions.RequestException as e:
        print(f"Error fetching data: {e}")
        return []

# URL to fetch the endpoint data
url = "https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946

# Get FQDNs and print them
fqdns = get_fqdns(url)
for fqdn in fqdns:
    print(fqdn)
```

2024年10月31日此指令碼的輸出示例：

```
outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
outlook.office365.com
smtp.office365.com
*.protection.outlook.com
*.mail.protection.outlook.com
*.mx.microsoft
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
```

```
teams.microsoft.com
*.sharepoint.com
*.officeapps.live.com
*.online.office.com
office.live.com
*.auth.microsoft.com
*.msftidentity.com
*.msidentity.com
account.activedirectory.windowsazure.com
accounts.accesscontrol.windows.net
adminwebservice.microsoftonline.com
api.passwordreset.microsoftonline.com
autologon.microsoftazuread-sso.com
becws.microsoftonline.com
ccs.login.microsoftonline.com
clientconfig.microsoftonline-p.net
companymanager.microsoftonline.com
device.login.microsoftonline.com
graph.microsoft.com
graph.windows.net
login.microsoft.com
login.microsoftonline.com
login.microsoftonline-p.com
login.windows.net
logincert.microsoftonline.com
loginex.microsoftonline.com
login-us.microsoftonline.com
nexus.microsoftonline-p.com
passwordreset.microsoftonline.com
provisioningapi.microsoftonline.com
*.protection.office.com
*.security.microsoft.com
compliance.microsoft.com
defender.microsoft.com
protection.office.com
purview.microsoft.com
security.microsoft.com
```

現在可以將清單清單中的域新增到系統提供的不解密清單：




您必須將FQDN新增到 系統提供的不解密列表，以便繞過IPS的解密。
自定義不解密清單只能應用於安全配置檔案。

## 解決方案

思科工程團隊正在努力增強Microsoft 365相容性功能，該功能將自動提取此清單，並允許管理員從安全訪問控制面板啟用旁路功能。

## 相關資訊

- Secure Access使用手冊
- 技術支援與下載 — Cisco Systems
- 安全存取解密和入侵防禦系統(IPS)工作流程疑難排解

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。