Create Effective Do Not Decrypt List for Microsoft 365 Services in Secure Access

Contents

Introduction

This document describes the effective way of creating a Do Not Decrypt list to bypass Microsoft 365 domains from IPS decryption in Secure Access.

Problem

Microsoft 365 traffic is know to cause problems when being passed through SSL inspection engines, proxy or IPS.
Microsoft suggests bypassing domains and IPs categorized as Allow and Optimize, based on KB article:

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

Current Microsoft 365 Compatibility feature in Secure Access is is only applicable for traffic passing through the proxy.
As a result, when this feature is enabled, no decryption or inspection is applied to this traffic on the proxy level, however global IPS decryption settings still apply.

When IPS decryption and Microsoft 365 Compatibility Feature are enabled, Internet destined traffic is still decrypted in scenarios:

- Full Tunnel RAVPN
- Secure Internet Access via VPN tunnel

Typical symptoms of problems caused by decryption of Microsoft 365 traffic:

- slow email delivery via Outlook
- performance problems with Sharepoint
- bad user experience when using Teams

Interim Workaround

Customers must bypass traffic destined to domains categorized as **Allow** and **Optimize** from IPS decryption:

Creating such list manually is rather a cumbersome task, hence the Python script can be used to pull the list dynamically from Microsoft API:
https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

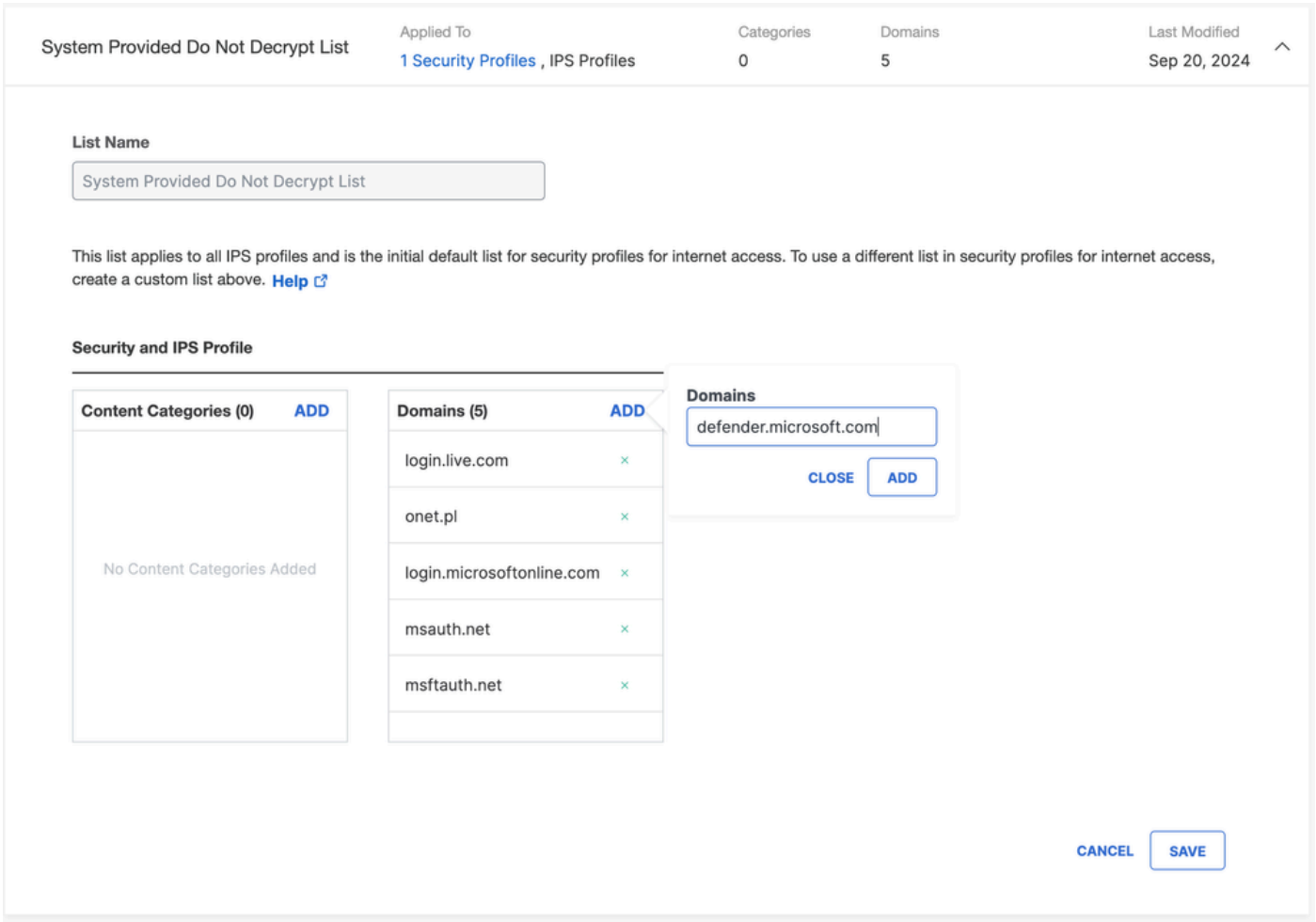
```
import requests

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)
```

Example outputof this script as of October 31st 2024:

```
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
```

Domains from the list list can be now added to **System Provided Do Not Decrypt List:**



You must add the FQDNs in **System Provided Do Not Decrypt List**, in order to bypass decryption for IPS. Custom Do Not Decrypt list can only by applied to Security Profiles.

Solution

Cisco Enginering Team is working on enhancing the Microsoft 365 compatibility feature, which would pull this list automatically and allows admin to enable the bypass functionality from Secure Access Dashboard.

Related Information

- **Secure Access User Guide**
- **Technical Support & Downloads - Cisco Systems**

- **Troubleshoot Secure Access Decryption and Intrusion Prevention System (IPS) Workflow**