Configure Microsoft O365 Tenant Restriction in SWA

Contents

Introduction

This document describes the process of configuring Configure Microsoft O365 Tenant Restriction in Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Access ToGraphic User Interface (GUI)of SWA
- Administrative Access to the SWA.

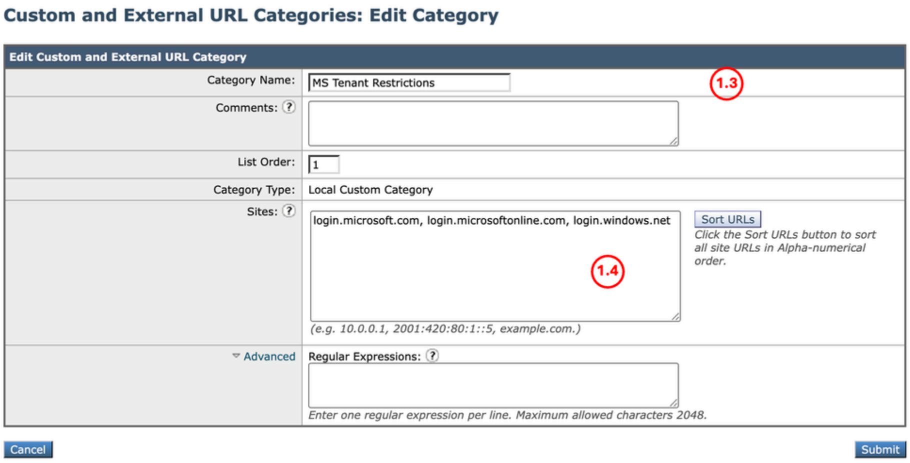
Components Used

This document is not restricted to specific software and hardware versions.

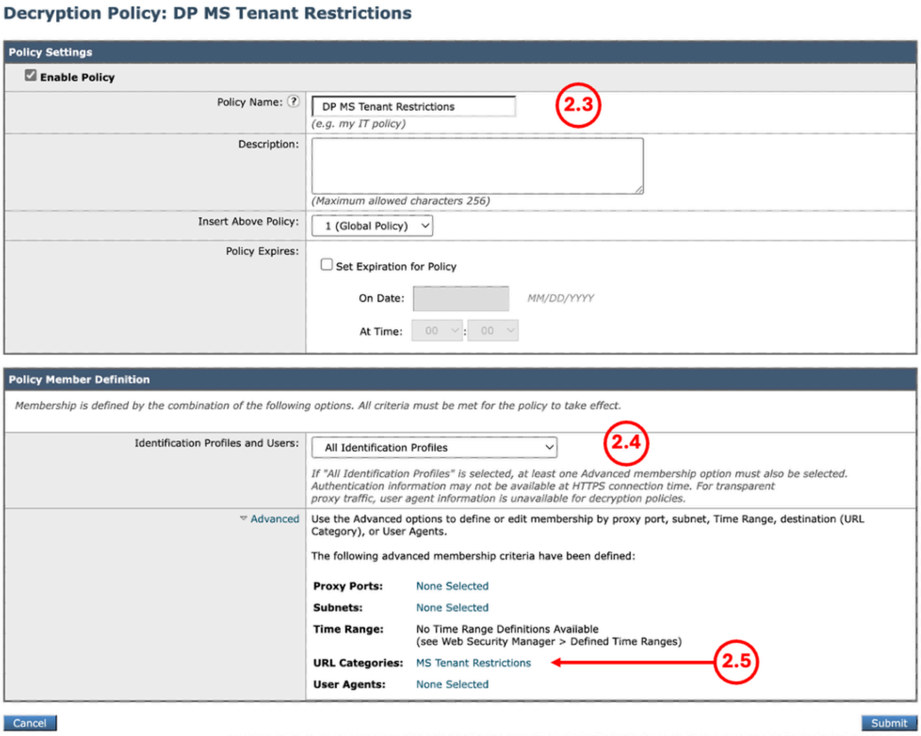
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration Steps

Step 1. Create a Custom URL Category for the website.	**Step 1.1.** From the GUI Navigate to **Web Security Manage**r and choose **Custom and External URL Categories**. **Step 1.2.** Click **Add Category** to create a new Custom URL Category.

	Step 1.3. Enter **Name** for the new category. **Step 1.4.** Define these URLs in the **Sites** section: `login.microsoft.com, login.microsoftonline.com, login.windows.net` **Step 1.5.Submit** the changes.  Custom and External URL Categories: Edit Category Edit Custom and External URL Category Category Name: MS Tenant Restrictions Comments: ? List Order: 1 Category Type: Local Custom Category Sites: ? login.microsoft.com, login.microsoftonline.com, login.windows.net (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.) Click the Sort URLs button to sort all site URLs in Alpha-numerical order. Advanced Regular Expressions: ? Enter one regular expression per line. Maximum allowed characters 2048. *Image - Custom URL Category* **Tip**: For more information about how to configure Custom URL Categories, kindly visit: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Step 2. Decrypt the traffic.	**Step 2.1.** From the GUI, Navigate to **Web Security Manager** and choose **Decryption Policies** **Step 2.2.** Click **Add Policy**. **Step 2.3.** Enter **Name** for the new policy. **Step 2.4.** Select the **Identification Profile** that you need this policy applies to. **Tip**: If you bypassed the Authentications for Microsoft URLs and you are configuring this policy for All users, choose: **All Identification Profiles** > **All Users** **Step 2.5.** From **Policy Member Definition** section, Click **URL Categories** links to add the Custom URL Category. **Step 2.6.** Select the URL Category that was created in **Step 1**.

Step 2.7. Click **Submit**.



Decryption Policy: DP MS Tenant Restrictions

Policy Settings

☑ Enable Policy

Policy Name: DP MS Tenant Restrictions (e.g. my IT policy)

Description: (Maximum allowed characters 256)

Insert Above Policy: 1 (Global Policy)

Policy Expires: □ Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: 00 : 00

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: All Identification Profiles

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

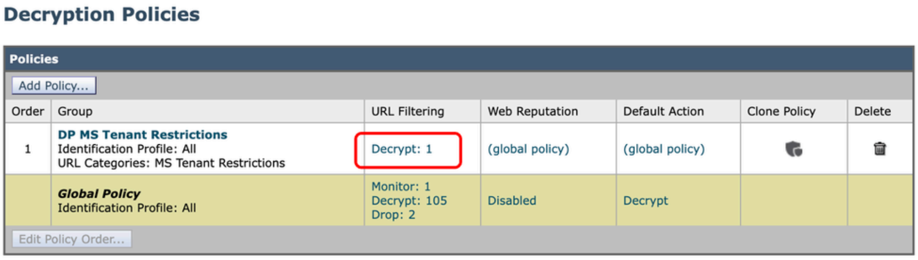
Advanced: Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports:	None Selected
Subnets:	None Selected
Time Range:	No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories:	MS Tenant Restrictions
User Agents:	None Selected

Image - Configure Decryption Policy

Step 2.8. In **Decryption Policies** page, click the link from **URL Filtering** for the new policy.



Decryption Policies

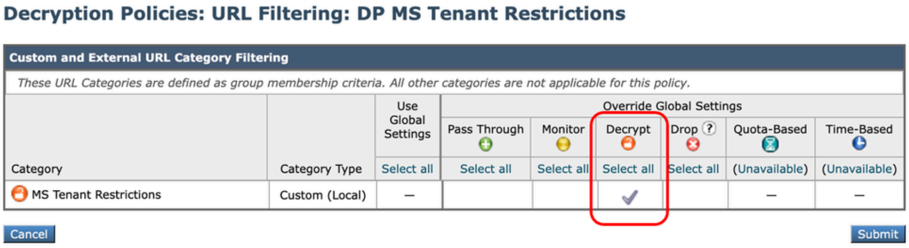
Policies

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	**DP MS Tenant Restrictions** Identification Profile: All URL Categories: MS Tenant Restrictions	Decrypt: 1	(global policy)	(global policy)		🗑
	Global Policy Identification Profile: All	Monitor: 1 Decrypt: 105 Drop: 2	Disabled	Decrypt		

Image - Edit URL Filtering Action

Step 2.9. Choose **Decrypt** as the action for Custom URL Category.

Step 2.10. Click **Submit**.



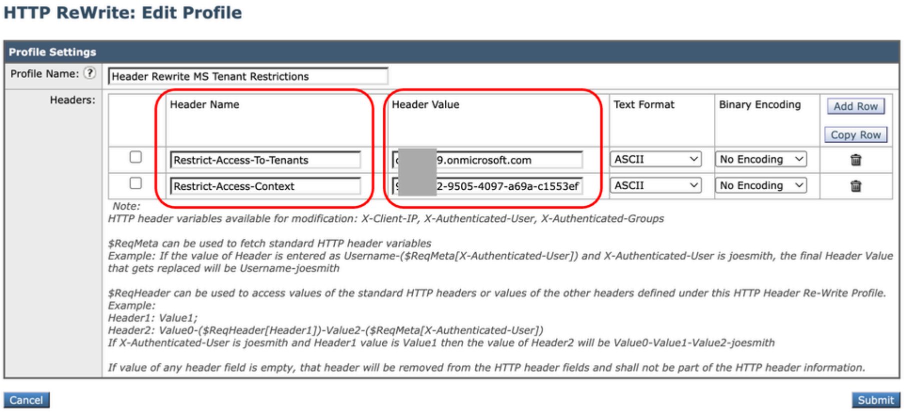
Decryption Policies: URL Filtering: DP MS Tenant Restrictions

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

			Override Global Settings					
		Use Global Settings	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Category	Category Type	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
MS Tenant Restrictions	Custom (Local)	–			✓		–	–

Image - Decrypt the Custom URL Category

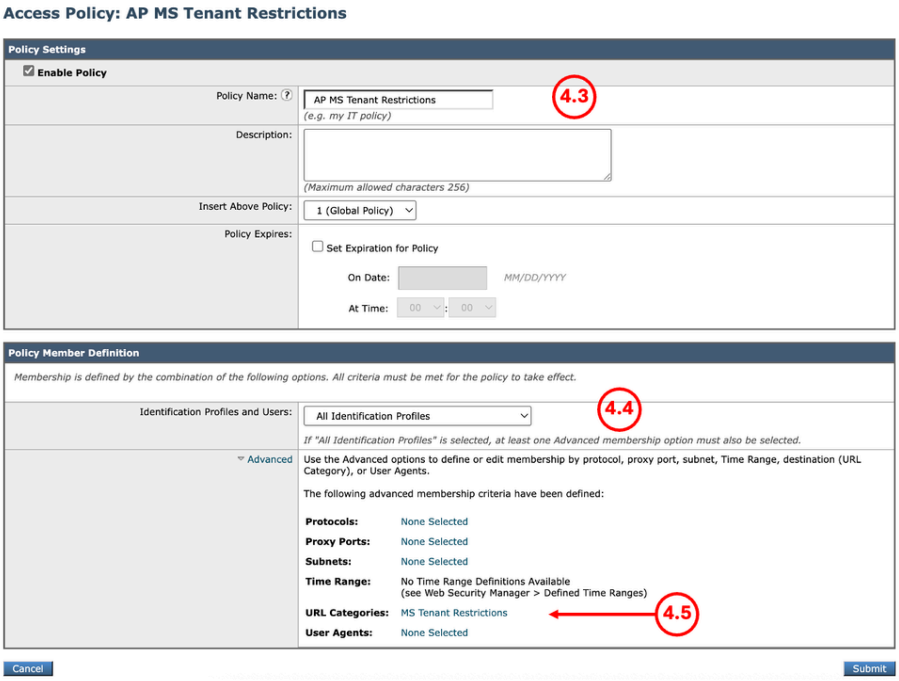
Step 3. Create HTTP Rewrite Profile.	**Step 3.1.** From the GUI, Navigate to **Web Security Manager** and choose **HTTP ReWrite Profiles**. **Step 3.2.** Click **Add Profile**. **Step 3.3.** Enter **Name** for the new profile. **Step 3.4.** Use **Restrict-Access-To-Tenants** for the first **Header Name**. **Step 3.5.** For the **Restrict-Access-To-Tenants** setting, use a value of <permitted tenant list>, which must be a comma-separated list of the tenants that users are allowed to access. **Step 3.6.** Click **Add Row** **Step 3.7.** Use **Restrict-Access-Context** as the second **Header Name**. **Step 3.8.** For the **Restrict-Access-Context** setting, use the value of a single directory ID to specify the tenant that is defining the tenant restrictions.. **Step 3.9.** Click **Submit**.  HTTP ReWrite: Edit Profile Profile Settings Profile Name: Header Rewrite MS Tenant Restrictions Headers: Header Name / Header Value / Text Format / Binary Encoding □ Restrict-Access-To-Tenants / [redacted]9.onmicrosoft.com / ASCII / No Encoding □ Restrict-Access-Context / [redacted]2-9505-4097-a69a-c1553ef / ASCII / No Encoding *Note:* *HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups* *$ReqMeta can be used to fetch standard HTTP header variables* *Example: If the value of Header is entered as Username-($ReqMeta[X-Authenticated-User]) and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith* *$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.* *Example:* *Header1: Value1;* *Header2: Value0-($ReqHeader[Header1])-Value2-($ReqMeta[X-Authenticated-User])* *If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith* *If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.* *Image - Add HTTP ReWrite Profile* **Tip**: For more information about Tenant Restriction and how to collect your tenant information, kindly visit: Microsoft Learn - Restrict access to a tenant.
Step 4. Create Access Policy.	**Step 4.1.** From the GUI, Navigate to **Web Security Manager** and choose **Access Policies** **Step 4.2.** Click **Add Policy**. **Step 4.3.** Enter **Name** for the new policy. **Step 4.4.** Select the **Identification Profile** that you need this policy applies to. **Tip**: If you bypassed the Authentications for Microsoft URLs and

you are configuring this policy for All users, choose: **All Identification Profiles** > **All Users**.

Step 4.5. From **Policy Member Definition** section, Click **URL Categories** links to add the Custom URL Category.

Step 4.6. Select the URL Category that was created in **Step 1**.

Step 4.7. Click **Submit**.



Access Policy: AP MS Tenant Restrictions

Policy Settings

☑ **Enable Policy**

Policy Name: ?	AP MS Tenant Restrictions *(e.g. my IT policy)*
Description:	*(Maximum allowed characters 256)*
Insert Above Policy:	1 (Global Policy)
Policy Expires:	□ Set Expiration for Policy On Date: MM/DD/YYYY At Time: 00 : 00

Policy Member Definition

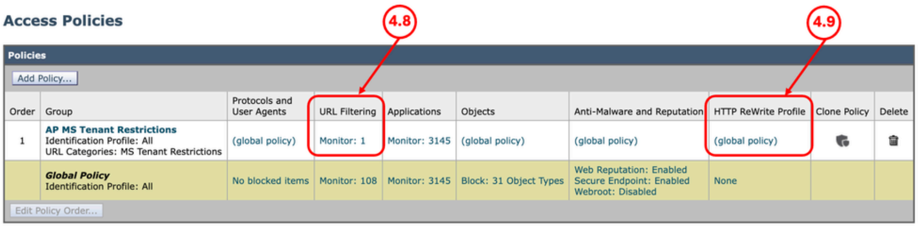
Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:	All Identification Profiles *If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.*
Advanced	Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined: **Protocols:** None Selected **Proxy Ports:** None Selected **Subnets:** None Selected **Time Range:** No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges) **URL Categories:** MS Tenant Restrictions **User Agents:** None Selected

Image - Create Access Policy

Step 4.8. In **Access Policies** page, make sure the action of the **URL Filtering** is set to **Monitor**.

Step 4.9. Click on the link in **HTTP ReWrite Profile** to add the HTTP Header Profile to this policy.



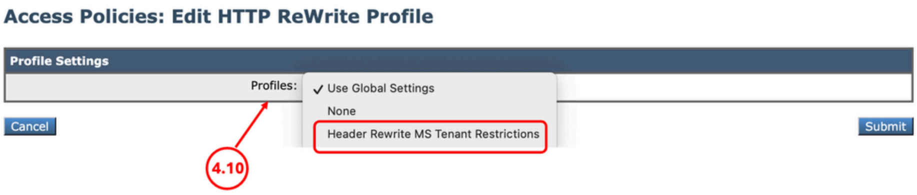
Access Policies

Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	**AP MS Tenant Restrictions** Identification Profile: All URL Categories: MS Tenant Restrictions	(global policy)	Monitor: 1	Monitor: 3145	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 3145	Block: 31 Object Types	Web Reputation: Enabled Secure Endpoint: Enabled Webroot: Disabled	None		

Image - Access Policy Properties

Step 4.10. Choose the **HTTP ReWrite Profiles**, created in Step [3].

	 Access Policies: Edit HTTP ReWrite Profile Profile Settings Profiles: ✓ Use Global Settings None Header Rewrite MS Tenant Restrictions Cancel Submit 4.10 *Image - Add HTTP ReWrite Profile* **Step 4.11.** Click **Submit**. **Step 4.12. Commit** Changes.

Reporting and Logs

Logs

You can add custom field to the access logs or the W3C logs to view the HTTP header rewrite profile name.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%]	**x-http-rewrite-profile-name**	HTTP header rewrite profile name.

Reporting

You can generate Web Tracking report to view the reports of the traffic by the AccessPolicy name.

Use these steps to generate the reports:

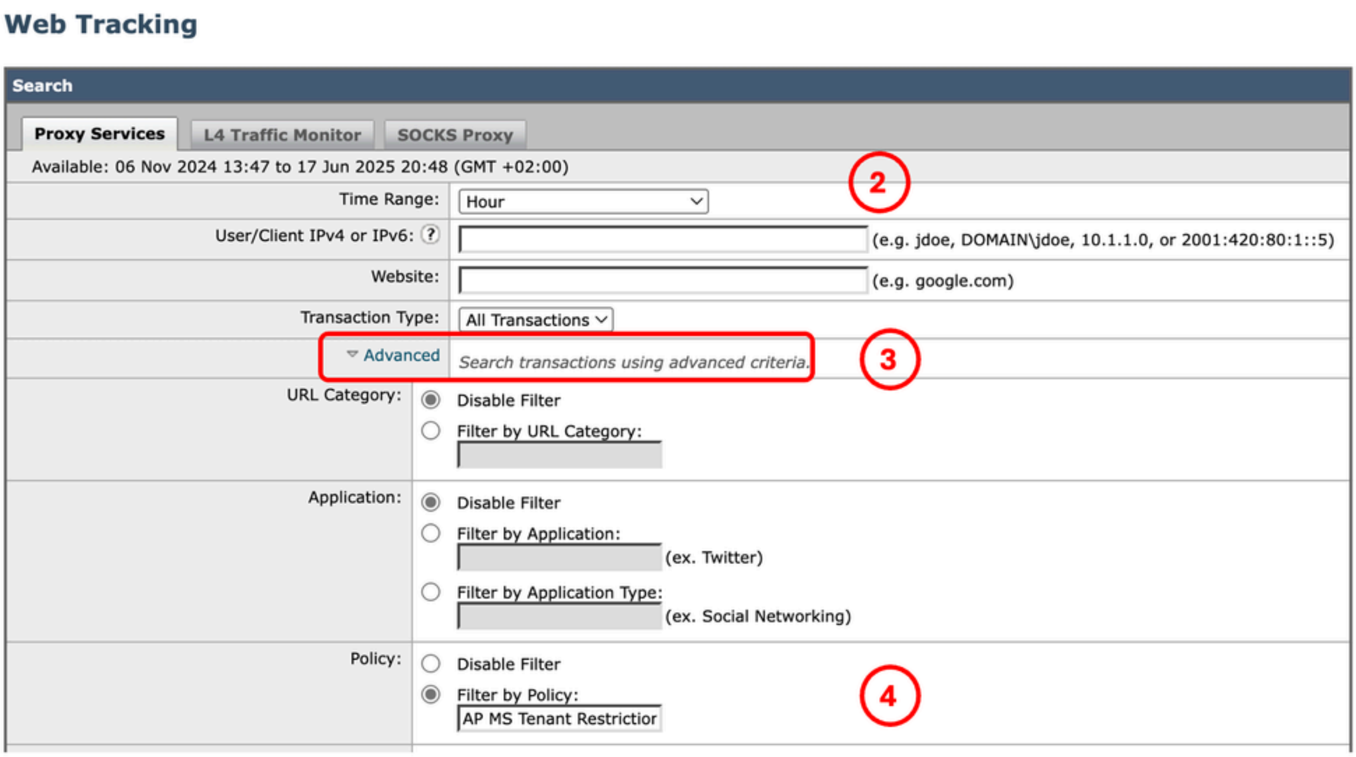
Step 1. From the GUI, select **Reporting** and choose **Web Tracking**.

Step 2. Choose your desired **Time Range.**

Step 3. Click the **Advanced** link to search transactions using advanced criteria.

Step 4. In the **Policy** section, select **Filter by Policy** and type the name of the **Access Policy** that was created previously.

Step 5. Click **Search** to review the report.



Web Tracking

Search

Proxy Services | L4 Traffic Monitor | SOCKS Proxy

Available: 06 Nov 2024 13:47 to 17 Jun 2025 20:48 (GMT +02:00)

Time Range:	Hour
User/Client IPv4 or IPv6:	(e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)
Website:	(e.g. google.com)
Transaction Type:	All Transactions
Advanced	Search transactions using advanced criteria.
URL Category:	● Disable Filter ○ Filter by URL Category:
Application:	● Disable Filter ○ Filter by Application: (ex. Twitter) ○ Filter by Application Type: (ex. Social Networking)
Policy:	○ Disable Filter ● Filter by Policy: AP MS Tenant Restrictior

Image - Web Tracking Report

Related Information

- User Guide for AsyncOS 15.2 for Cisco Secure Web Appliance
- Cisco Secure Email and Web Virtual Appliance Installation Guide
- Configure Custom URL Categories in Secure Web Appliance - Cisco
- Use Secure Web Appliance Best Practices
- Configure Firewall for Secure Web Appliance
- Configure Decryption Certificate in Secure Web Appliance
- Configure and Troubleshoot SNMP in SWA
- Configure SCP Push Logs in Secure Web Appliance with Microsoft Server
- Enable Specific YouTube Channel/Video and Block Rest of YouTube in SWA
- Understand HTTPS Accesslog Format in Secure Web Appliance
- Access Secure Web Appliance Logs
- Bypass Authentication in Secure Web Appliance
- Block Traffic in Secure Web Appliance
- Bypass Microsoft Updates Traffic in Secure Web Appliance