SWA에서 Microsoft O365 테넌트 제한 구성

목차

소개

이 문서에서는 SWA(Secure Web Appliance)에서 Microsoft O365 테넌트 제한 구성을 구성하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- SWA의 그래픽 사용자 인터페이스(GUI)에 액세스
- SWA에 대한 관리 액세스.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

컨피그레이션 단계

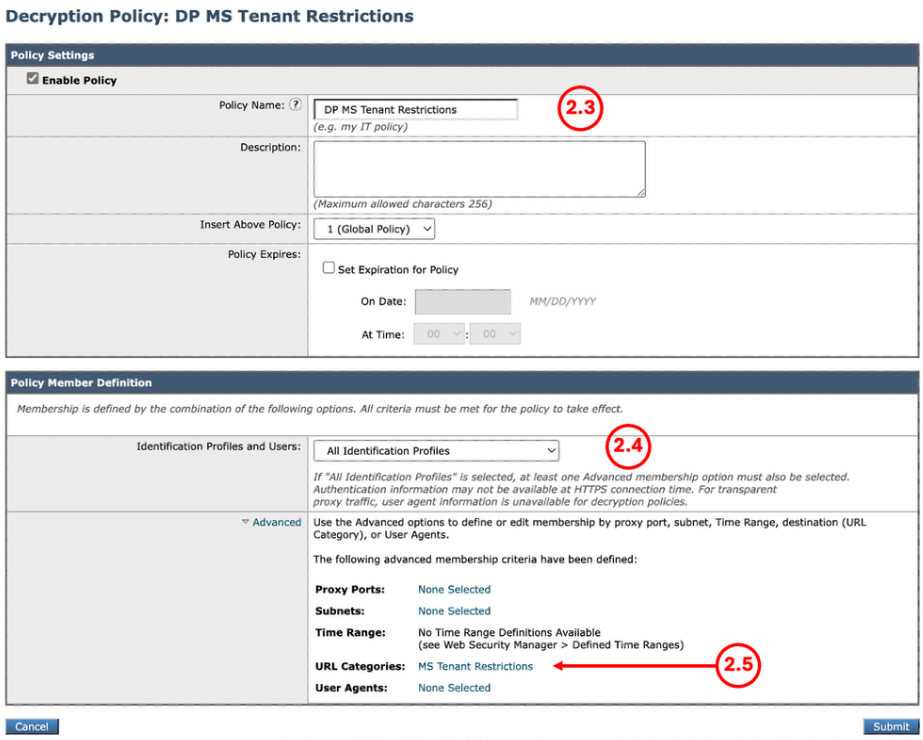
1단계. 웹 사이트에 대한 맞춤형 URL 카테고리를 생성합니다.	1.1단계. GUI에서 Web Security Manager(Web Security Manager)로 이동하여 Custom(사용자 지정) 및 External URL Categories(외부 URL 범주)를 선택합니다.

	1.2단계. Add Category(카테고리 추가)를 클릭하여 새 맞춤형 URL 카테고리를 생성합니다. 1.3단계. 새 범주의 이름을 입력합니다. 1.4단계. Sites(사이트) 섹션에서 다음 URL을 정의합니다. `login.microsoft.com, login.microsoftonline.com, login.windows.net` 1.5단계. 변경 사항을 제출합니다. **Custom and External URL Categories: Edit Category** Edit Custom and External URL Category Category Name: MS Tenant Restrictions (1.3) Comments: List Order: 1 Category Type: Local Custom Category Sites: login.microsoft.com, login.microsoftonline.com, login.windows.net (1.4) Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.) Advanced — Regular Expressions: Enter one regular expression per line. Maximum allowed characters 2048. Cancel Submit 이미지 - 사용자 지정 URL 범주 팁: 맞춤형 URL 카테고리를 구성하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html을 참조하십시오.
2단계. 트래픽을 해독합니다.	2.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하고 Decryption Policies(암호 해독 정책)를 선택합니다 2.2단계. Add Policy(정책 추가)를 클릭합니다. 2.3단계. 새 정책의 Name을 입력합니다. 2.4단계. 이 정책을 적용할 ID 프로필을 선택합니다. 팁: Microsoft URL에 대한 인증을 우회하고 모든 사용자에 대해 이 정책을 구성하는 경우 All Identification Profiles(모든 식별 프로필) > All Users(모든 사용자)를 선택합니다.

2.5단계. Policy Member Definition(정책 멤버 정의) 섹션에서 URL Categories(URL 카테고리) 링크를 클릭하여 Custom URL Category(맞춤형 URL 카테고리)를 추가합니다.

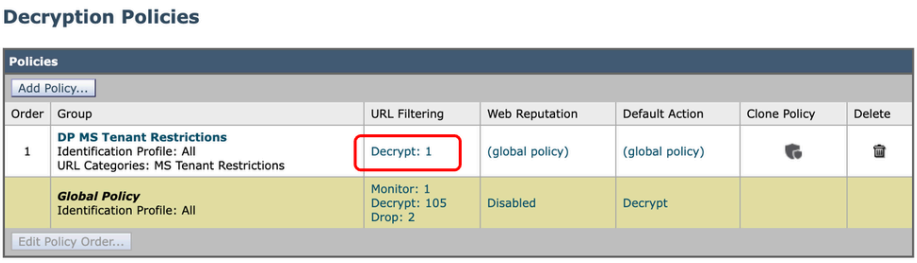
2.6단계.1단계에서 생성한 URL 카테고리를 선택합니다.

2.7단계. Submit(제출)을 클릭합니다.



이미지 - 암호 해독 정책 구성

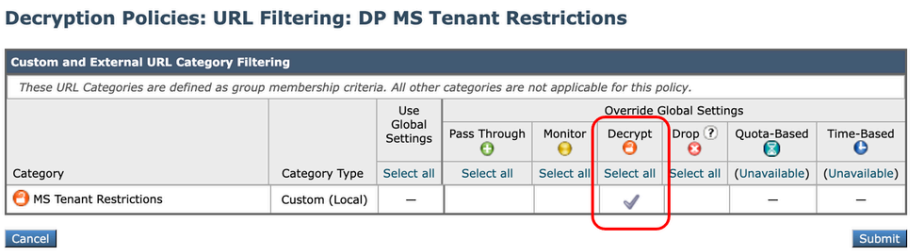
2.8단계. Decryption Policies(암호 해독 정책) 페이지에서 새 정책의 URL Filtering(URL 필터링)에서 링크를 클릭합니다.



이미지 - URL 필터링 작업 편집

2.9단계. Custom URL Category(맞춤형 URL 카테고리)에 대한 작업으로 Decrypt(해독)를 선택합니다.

2.10단계. Submit(제출)을 클릭합니다.

<table>
<tr>
<td></td>
<td> 

이미지 - 사용자 지정 URL 카테고리 암호 해독</td>
</tr>
<tr>
<td>3단계. HTTP 재작성 프로파일을 생성합니다.</td>
<td>3.1단계. GUI에서 Web Security Manager(웹 보안 관리자)로 이동하고 HTTP ReWrite Profiles(HTTP 재작성 프로필)를 선택합니다.

3.2단계. Add Profile(프로필 추가)을 클릭합니다.

3.3단계. 새 프로파일의 이름을 입력합니다.

3.4단계. 첫 번째 헤더 이름에 Restrict-Access-To-Tenants를 사용합니다.

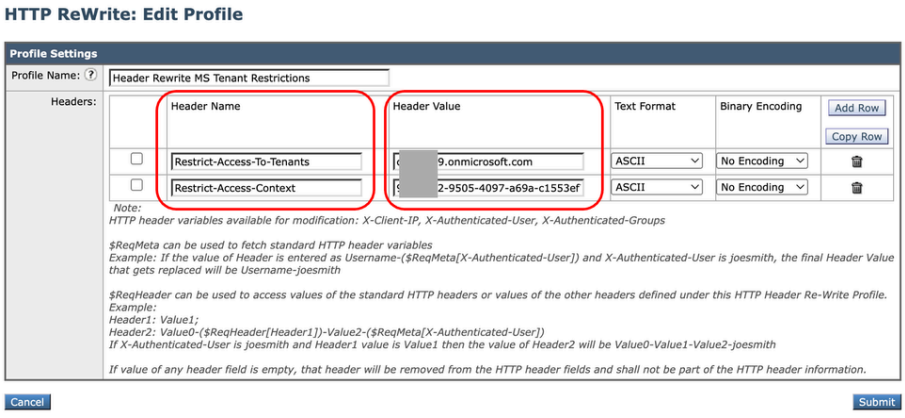
3.5단계. Restrict-Access-To-Tenants 설정의 경우 <permitted tenant list> 값을 사용합니다. 이 값은 사용자가 액세스할 수 있는 테넌트의 쉼표로 구분된 목록이어야 합니다.

3.6단계. Add Row(행 추가)를 클릭합니다

3.7단계. 두 번째 헤더 이름으로 Restrict-Access-Context를 사용합니다.

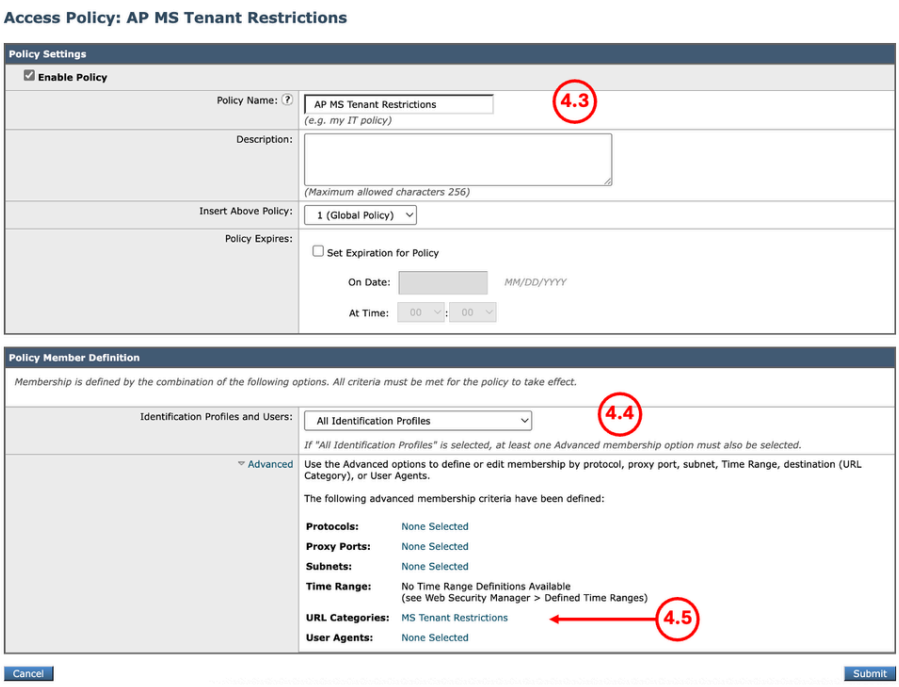
3.8단계. Restrict-Access-Context 설정의 경우 단일 디렉토리 ID 값을 사용하여 테넌트 제한을 정의하는 테넌트를 지정합니다.

3.9단계. Submit(제출)을 클릭합니다.

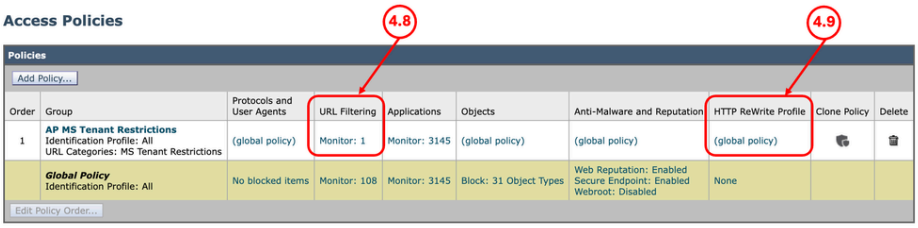
 

이미지 - HTTP ReWrite 프로필 추가

팁: 테넌트 제한 및 테넌트 정보 수집 방법에 대한 자세한 내</td>
</tr>
</table>

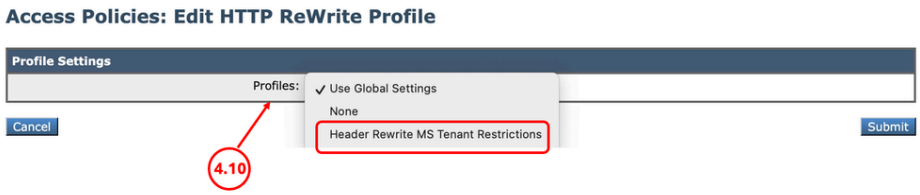
	용은 다음 사이트를 참조하십시오. Microsoft Learn - 테넌트에 대한 액세스 제한
4단계. 액세스 정책을 생성합니다.	4.1단계. GUI에서 Web Security Manager로 이동하고 Access Policies(액세스 정책)를 선택합니다 4.2단계. Add Policy(정책 추가)를 클릭합니다. 4.3단계. 새 정책의 Name을 입력합니다. 4.4단계. 이 정책을 적용할 ID 프로필을 선택합니다. 팁: Microsoft URL에 대한 인증을 우회하고 모든 사용자에 대해 이 정책을 구성하는 경우 All Identification Profiles(모든 식별 프로필) > All Users(모든 사용자)를 선택합니다. 4.5단계. Policy Member Definition(정책 멤버 정의) 섹션에서 URL Categories(URL 카테고리) 링크를 클릭하여 Custom URL Category(맞춤형 URL 카테고리)를 추가합니다. 4.6단계.1단계에서 생성한 URL 카테고리를 선택합니다. 4.7단계. Submit(제출)을 클릭합니다.  이미지 - 액세스 정책 생성 4.8단계. Access Policies(액세스 정책) 페이지에서 URL Filtering(URL 필터링)의 작업이 Monitor(모니터링)로 설정되어 있는지 확인합니다.

4.9단계. HTTP ReWrite Profile(HTTP 재작성 프로파일)에서 링크를 클릭하여 HTTP 헤더 프로파일을 이 정책에 추가합니다.



이미지 - 액세스 정책 속성

4.10단계. [3]단계에서 생성한 HTTP ReWrite Profiles를 선택합니다.



이미지 - HTTP ReWrite 프로필 추가

4.11단계. Submit(제출)을 클릭합니다.

4.12단계. 변경사항을 커밋합니다.

보고 및 로그

로그

HTTP 헤더 재작성 프로필 이름을 보려면 액세스 로그 또는 W3C 로그에 사용자 지정 필드를 추가할 수 있습니다.

액세스 로그의 형식 지정자	W3C 로그의 로그 필드	설명
%]	x-http-rewrite-profile-name	HTTP 헤더 재작성 프로파일 이름

보고

웹 추적 보고서를 생성하여 AccessPolicy 이름으로 트래픽의 보고서를 볼 수 있습니다.

다음 단계를 사용하여 보고서를 생성합니다.

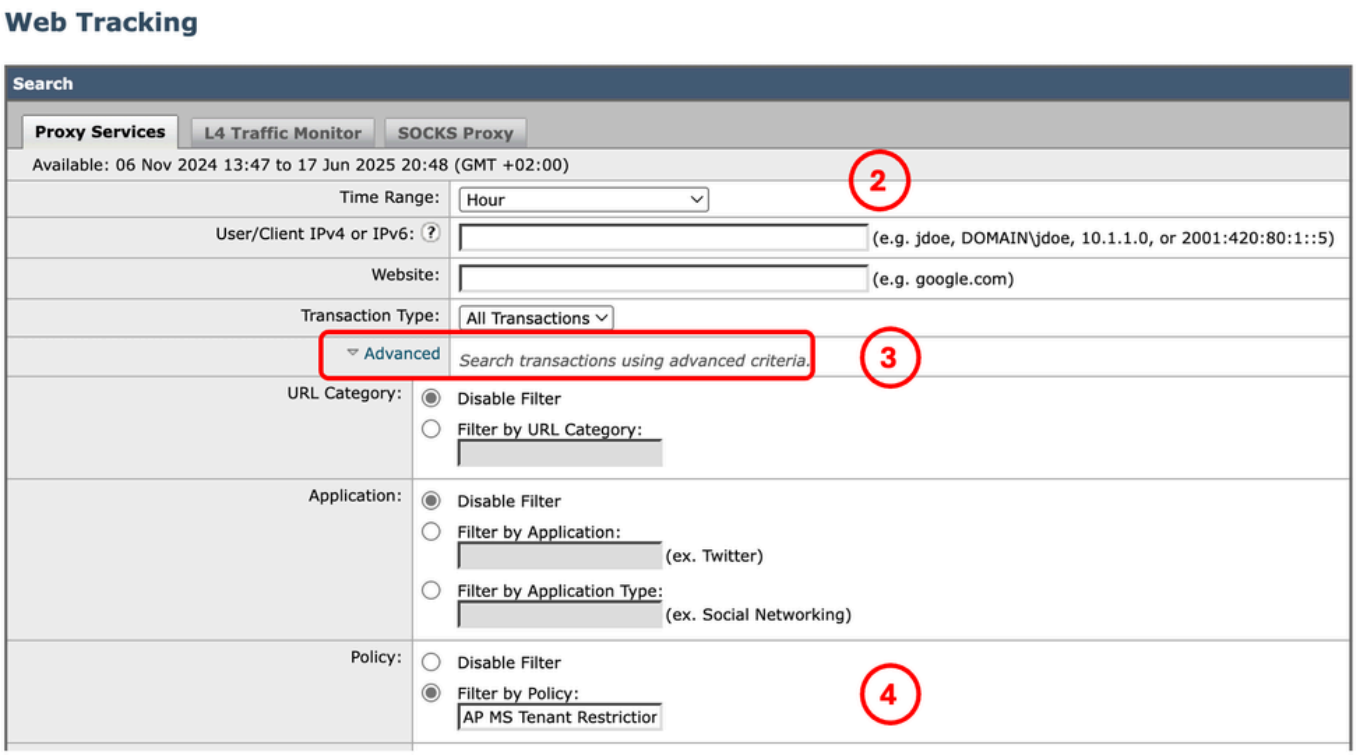
1단계. GUI에서 Reporting(보고)을 선택하고 Web Tracking(웹 추적)을 선택합니다.

2단계. 원하는 시간 범위를 선택합니다.

3단계. 고급 링크를 눌러 고급 기준을 사용하여 트랜잭션을 검색합니다.

4단계. Policy(정책) 섹션에서 Filter by Policy(정책으로 필터링)를 선택하고 이전에 생성한 액세스 정책의 이름을 입력합니다.

5단계. 검색을 눌러 보고서를 검토합니다.



이미지 - 웹 추적 보고서

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서
- Cisco Secure Email and Web Virtual Appliance 설치 설명서
- Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco
- Secure Web Appliance 모범 사례 사용
- Secure Web Appliance용 방화벽 구성
- Secure Web Appliance에서 암호 해독 인증서 구성
- SWA에서 SNMP 구성 및 문제 해결
- Microsoft Server를 사용하여 Secure Web Appliance에서 SCP 푸시 로그 구성
- SWA에서 특정 YouTube 채널/비디오 활성화 및 나머지 YouTube 차단
- Secure Web Appliance의 HTTPS 액세스 로그 형식 이해
- Secure Web Appliance 로그 액세스

- Secure Web Appliance에서 인증 우회
- Secure Web Appliance에서 트래픽 차단
- Secure Web Appliance에서 Microsoft 업데이트 트래픽 우회

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.