

FMC를 통한 Firepower Threat Defense용 고급 AnyConnect VPN 구축

초판: 2020년 4월 7일

최종 변경: 2020년 4월 28일

FMC를 통한 Firepower Threat Defense용 고급 AnyConnect VPN 구축

이 문서에서는 동적 스플릿 터널링 및 LDAP 특성 맵을 포함하여 Cisco FMC에서 FlexConfig를 사용하여 Cisco FTD용 고급 AnyConnect VPN을 구축하는 방법을 설명합니다.

동적 스플릿 터널링

다음 주제에서는 Cisco FTD(Firepower Threat Defense)의 동적 스플릿 터널링과 Cisco FMC(Firepower Management Center) 6.4에서 FlexConfig를 사용하여 이를 설정하는 방법을 설명합니다. 이 설정은 동적 스플릿 터널링을 직접 지원하지 않는 후속 릴리스에 적용할 수 있습니다.

동적 스플릿 터널링 정보

정적 스플릿 터널링에는 원격 액세스 VPN 터널에 포함하거나 해당 터널에서 제외해야 하는 호스트 및 네트워크의 IP 주소를 정의하는 작업이 포함됩니다. 동적 스플릿 터널링을 정의하면 스플릿 터널링을 개선할 수 있습니다.

동적 스플릿 터널링을 사용하면 DNS 도메인 이름에 따라 스플릿 터널링을 미세 조정할 수 있습니다. FQDN(Fully Qualified Domain Name)과 연결된 IP 주소는 지역에 따라 변경되거나 단순히 다를 수 있으므로 DNS 이름을 기반으로 스플릿 터널링을 정의하면 원격 액세스 VPN 터널에 포함하거나 포함하지 않아야 하는 트래픽에 대한 추가 동적 정의를 제공합니다. 제외된 도메인 이름에 대해 반환된 주소가 VPN에 포함된 주소 풀 내에 있으면 해당 주소가 제외됩니다.

제외된 도메인은 차단되지 않습니다. 대신 해당 도메인에 대한 트래픽은 VPN 터널 외부에서 유지됩니다. 예를 들면 공용 인터넷에서 Cisco WebEx로 트래픽을 전송하여 VPN 터널에서 보호된 네트워크 내의 서버를 대상으로 하는 트래픽에 대한 대역폭을 확보할 수 있습니다.

버전 7.0 이상부터는 FMC UI를 사용하여 이 기능을 구성할 수 있습니다. 자세한 내용은 [FMC에서 관리하는 FTD에 대한 AnyConnect 동적 스플릿 터널 구성](#)을 참고하십시오. 이전 버전의 FMC의 경우 FlexConfig를 사용하여 동적 스플릿 터널링 설정, 2 페이지에 설명된 대로 FlexConfig를 사용하여 구성해야 합니다.

FlexConfig를 사용하여 동적 스플릿 터널링 설정

동적 스플릿 터널 설정은 **dynamic-split-exclude-domains** 유형의 사용자 지정 AnyConnect 특성을 생성한 다음 이 특성을 RA VPN 연결 프로파일에서 사용하는 그룹 정책에 추가하는 작업을 기반으로 합니다.

또한 **dynamic-split-include-domains** 사용자 지정 특성을 생성하여 터널에 포함할 도메인을 정의할 수도 있습니다. 그러지 않으면 도메인이 IP 주소에 따라 제외됩니다. 이 예에는 도메인을 제외하는 작업을 살펴봅니다.

시작하기 전에

이 설정에는 AnyConnect 4.5 이상이 필요합니다.

이 예에서는 원격 액세스 VPN이 이미 설정되어 올바르게 작동한다고 가정합니다. 여기에는 동적 스플릿 터널링 특성을 추가할 그룹 정책을 생성하는 작업도 포함됩니다. FlexConfig를 사용하여 그룹 정책을 생성하지 마십시오. FlexConfig는 기존 그룹 정책을 편집하는 용도로만 사용하십시오.

동적 제외 목록을 정의할 때는 고정 IP 주소 기반 스플릿 터널링을 설정하지 않아도 됩니다. 그러나 동적 포함 목록을 생성하려면 스플릿 터널링을 활성화하고 일부 IP 주소를 제외해야 합니다. 도메인을 포함하는 동적 스플릿 터널링은 포함하지 않으면 IP 주소 기반 스플릿 터널 상황에서 제외되는 트래픽을 포함하는 경우에만 의미가 있습니다.

프로시저

단계 1 동적 스플릿 터널링 사용자 지정 특성을 생성한 후 VPN 터널에서 제외하고 대신 공용 인터넷을 통해 전송해야 하는 도메인 이름을 이 특성에 할당하는 `deploy-once/append` FlexConfig 개체를 생성합니다.

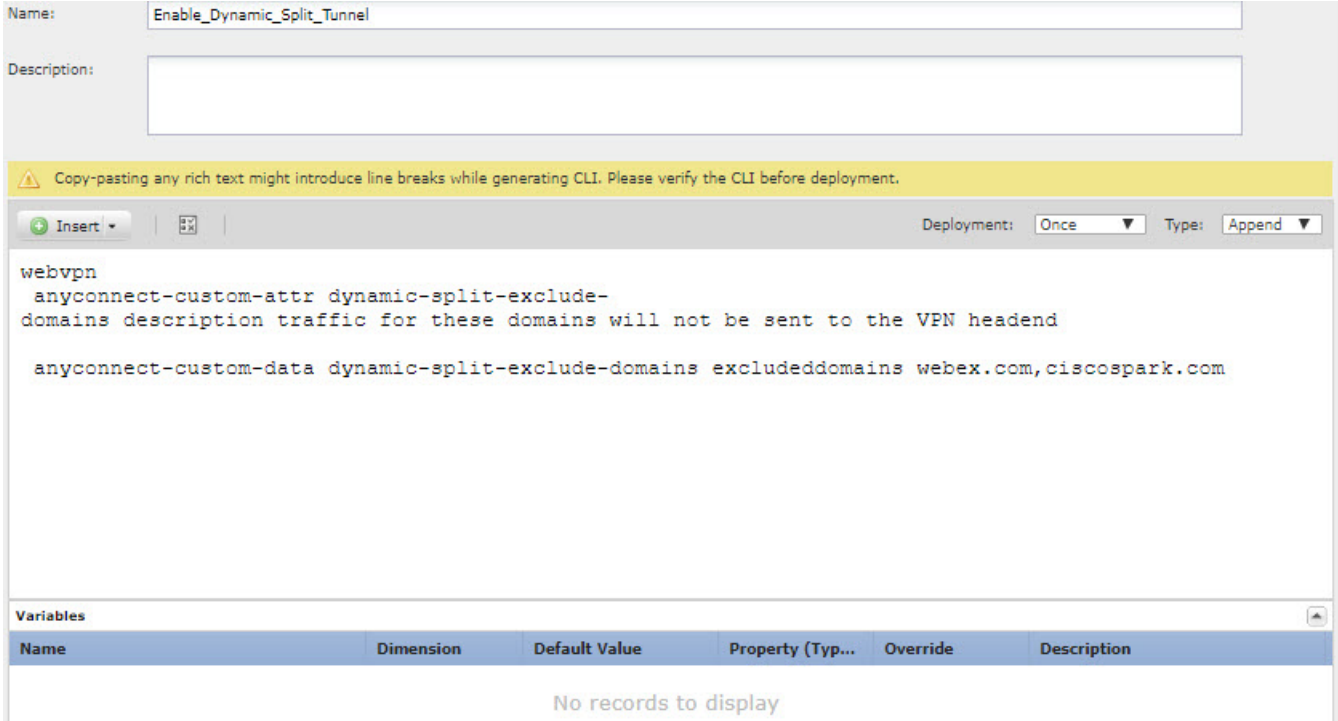
- a) **Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- b) 목차에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- c) **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 `Enable_Dynamic_Split_Tunnel`입니다.
- **Deployment(구축)** - **Once(한 번)**를 선택합니다. 이러한 명령은 한 번만 설정하면 됩니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.
- **Object body(개체 본문)** - 개체 본문에 **dynamic-split-exclude-domains** 유형의 특성을 생성하는 데 필요한 명령을 입력한 다음 제외할 특성 이름 및 도메인 이름 목록에 해당하는 데이터를 추가합니다. 예를 들어 `excludeddomains`라는 특성을 만들고 `webex.com` 및 `ciscospark.com` 도메인을 제외하려는 경우 명령은 다음과 같습니다. 설명은 선택 사항이지만 포함하는 경우 별도의 명령이 아닌 **anyconnect-custom-attr** 명령의 일부입니다. 도메인 이름의 경우 쉽표로 구분하고 공백은 포함하지 않습니다.

```
webvpn
anyconnect-custom-attr dynamic-split-exclude-domains description traffic for these
domains will not be sent to the VPN headend
```

```
anyconnect-custom-data dynamic-split-exclude-domains excludeddomains
webex.com,ciscospark.com
```

개체는 다음과 비슷해야 합니다.



단계 2 (권장) 사용자 지정 그룹 정책을 사용하는 경우 deploy-once/append FlexConfig 개체를 생성하여 그룹 정책에서 동적 스플릿 터널 사용자 지정 특성을 설정합니다.

사용자 지정 그룹 정책에 대한 변경 사항은 무효화되지 않으므로 변경 사항을 한 번 구축해야 합니다. 여러 그룹 정책을 사용하는 경우 단일 FlexConfig 개체를 사용하여 각 정책에 사용자 지정 특성을 차례로 추가할 수 있습니다. 또는 그룹 정책당 하나의 FlexConfig 개체를 생성할 수 있습니다. 결과는 동일하므로 FlexConfig 정책 모듈화에 대한 고유의 요구 사항에 따라 선택합니다.

FlexConfig 개체 페이지에서 **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 Add_Dynamic_Split_Tunnel_Sales와 같습니다.
- **Deployment(구축)** - **Once(한 번)**를 선택합니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다.
- **Object body(개체 본문)** - 개체 본문에 사용자 지정 특성을 그룹 정책에 추가하는 데 필요한 명령을 입력합니다. 예를 들어 생성한 특성의 이름이 excludeddomains이고 그룹 정책의 이름이 "sales" 라면 명령은 다음과 같습니다.

```
group-policy sales attributes
anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

개체는 다음과 비슷해야 합니다.

단계 3 (권장하지 않음.) 이름이 DfltGrpPolicy인 기본 그룹 정책을 사용하는 경우 `deploy-everytime/append` FlexConfig 개체를 생성하여 그룹 정책에서 동적 스플릿 터널 사용자 지정 특성을 구성합니다.

구축할 때마다 기본 정책에 대한 모든 사용자 지정 변경 사항이 무효화되므로 이 개체를 매번 구축해야 합니다.

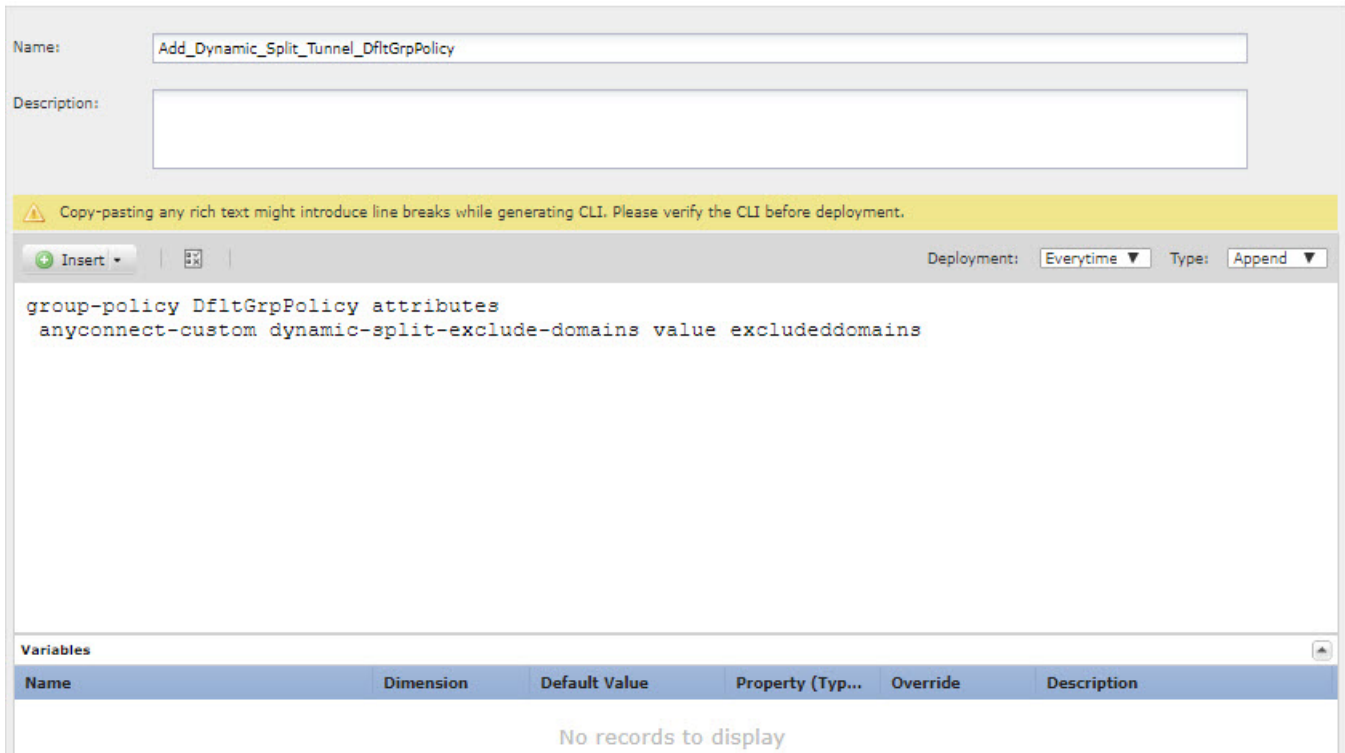
DfltGroupPolicy를 사용하는 대신 사용자 지정 그룹 정책을 생성하는 것이 좋습니다.

FlexConfig 개체 페이지에서 **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 `Add_Dynamic_Split_Tunnel_DfltGrpPolicy`입니다.
- **Deployment(구축) - Everytime(항상)**을 선택합니다. 이러한 명령은 한 번만 설정하면 됩니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다. 기본 그룹 정책의 사용자 지정 특성이 무효화된 후 명령을 전송해야 합니다.
- **Object body(개체 본문)** - 개체 본문에 사용자 지정 특성을 그룹 정책에 추가하는 데 필요한 명령을 입력합니다. 예를 들어 생성한 특성의 이름이 `excludeddomains`라면 명령은 다음과 같습니다.

```
group-policy DfltGrpPolicy attributes
anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

개체는 다음과 비슷해야 합니다.



단계 4 이러한 개체를 구축하는 FlexConfig 정책을 생성합니다.

- a) **Devices**(디바이스) > **FlexConfig**를 선택합니다.
- b) **New Policy**(새 정책)를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

- c) Ctrl 키를 누른 채 목차의 **User Defined**(사용자 정의) 폴더에서 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs**(선택된 추가 FlexConfigs) 목록에 추가해야 합니다.

- d) 끌어다 놓기를 사용하여 개체의 순서가 올바른지 확인합니다.

사용자 지정 특성 개체를 생성하는 개체는 그룹 정책에 해당 특성을 할당하는 개체 앞에 있어야 합니다. 그렇지 않으면 아직 존재하지 않는 사용자 지정 특성을 추가하려고 하면 오류가 발생합니다.

사용자 지정 그룹 정책을 구성하는 단일 개체가 있는 경우 목록은 다음과 같이 표시됩니다.

Selected Appended FlexConfigs	
#.	Name
1.	Enable_Dynamic_Split_Tunnel
2.	Add_Dynamic_Split_Tunnel_Sales

- e) **Save**(저장)를 클릭합니다.

- f) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 Save(저장) 아래에 있는 **Policy Assignments**(정책 할당) 링크를 클릭하여 할당합니다.
- g) **Preview Config**(구성 미리보기)를 클릭하고, **Preview**(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 동적 스플릿 터널 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
webvpn
  anyconnect-custom-attr dynamic-split-exclude-domains description traffic for these
  domains will not be sent to the VPN headend
  anyconnect-custom-data dynamic-split-exclude-domains excludeddomains
  webex.com,ciscospark.com
  group-policy sales attributes
  anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

단계 5 변경 사항을 배포합니다.

단계 6 구성을 확인합니다.

- 각 FTD 디바이스에서 명령이 설정되었는지 확인할 수 있습니다. 디바이스에 대한 SSH 세션 또는 FMC의 CLI 툴을 사용합니다(**System**(시스템) > **Health**(상태) > **Monitor**(모니터)를 선택한 후 디바이스를 클릭한 다음 **Advanced Troubleshooting**(고급 문제 해결)을 클릭하고 **Threat Defense CLI** 탭 선택). 다음은 설정을 표시하는 명령입니다.
 - **show running-config webvpn**
 - **show running-config anyconnect-custom-data**
 - **show running-config group-policy name**, 여기서 *name*은 sales와 같은 그룹 정책 이름으로 교체됩니다.
- AnyConnect 클라이언트에서 시스템이 올바르게 작동하는지 확인할 수 있습니다. 클라이언트 통계를 열면 **Dynamic Tunnel Exclusions**(동적 터널 제외) 필드에 제외할 도메인 이름 목록이 표시됩니다.

FlexConfig를 사용하여 동적 스플릿 터널링 제거

스플릿 터널링을 더 이상 사용하지 않으려면 FlexConfig 개체를 생성하여 기능을 구축한 디바이스에서 설정을 제거해야 합니다. FlexConfig 정책에서 FlexConfig 개체를 제거하는 것만으로는 충분하지 않습니다.

프로시저

단계 1 사용자 지정 특성을 사용하는 각 그룹 정책에서 사용자 지정 특성을 제거하는 `deploy-once/append` FlexConfig 개체를 생성한 다음 해당 특성을 삭제합니다.

특성을 삭제하려면 먼저 사용자 지정 정책에서 특성을 제거해야 합니다. 현재 사용 중인 특성을 삭제하려고 하면 사용자가 차단되고 구축 오류가 표시됩니다. 따라서 이 개체가 올바르게 작동하려면 명령을 올바른 순서로 삽입해야 합니다.

- a) **Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- b) 목차에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- c) **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 `Disable_Dynamic_Split_Tunnel`입니다.

- **Deployment(구축) - Once(한 번)**를 선택합니다. 이러한 명령은 한 번만 설정하면 됩니다.

- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.

- **Object body(개체 본문)** - 개체 본문에 사용자 지정 특성을 사용하는 각 그룹 정책에서 사용자 지정 특성을 제거한 다음 사용자 지정 특성을 삭제하는 데 필요한 명령을 입력합니다. 예를 들어 `sales` 그룹 정책에서 사용자 지정 특성을 사용하고 이 특성의 이름이 `excludeddomains` 인 경우 명령은 다음과 같습니다.

```
group-policy sales attributes
  no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn
  no anyconnect-custom-attr dynamic-split-exclude-domains
```

개체는 다음과 비슷해야 합니다.

FlexConfig를 사용하여 동적 스플릿 터널링 제거

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Type:

```
group-policy sales attributes
no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn

no anyconnect-custom-attr dynamic-split-exclude-domains
```

Variables

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

단계 2 FlexConfig 정책을 편집하여 동적 스플릿 터널링 개체를 제거하고 설정을 제거하는 개체를 추가합니다.

- Devices(디바이스) > FlexConfig를 선택합니다.
- FlexConfig 정책을 편집합니다.
- Selected Appended FlexConfigs**(선택된 추가 FlexConfig) 목록에서 각 동적 스플릿 터널 개체(사용자 지정 특성을 활성화한 다음 해당 특성을 그룹 정책에 추가하는 개체)에 대한 삭제 아이콘을 클릭합니다.
- 목차의 **User Defined**(사용자 정의) 폴더에서 동적 스플릿 터널링을 비활성화하는 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.

목록은 다음과 같이 표시됩니다.

Selected Append FlexConfigs	
#.	Name
1.	Disable_Dynamic_Split_Tunnel

- Save(저장)를 클릭합니다.
- Preview Config**(구성 미리보기)를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변

경 사항에서 생성된 명령도 함께 표시됩니다. 동적 스플릿 터널 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
group-policy sales attributes
 no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn
 no anyconnect-custom-attr dynamic-split-exclude-domains
```

단계 3 변경 사항을 배포합니다.

AnyConnect 설정용 LDAP 특성 맵

AD(Active Directory)/LDAP를 사용하여 원격 액세스 VPN 사용자를 인증하는 경우 LDAP 특성 맵을 사용하여 AD/LDAP 서버에서 반환되는 특성에 따라 AnyConnect 설정 및 동작을 조정할 수 있습니다.

LDAP 특성 맵 정보

LDAP 특성 맵에서는 AD(Active Directory)/LDAP 서버에 있는 특성을 Cisco 특성 이름과 동일시합니다. 그런 다음 원격 액세스 VPN 연결을 설정하는 동안 AD/LDAP 서버에서 FTD 디바이스에 인증을 반환하면 FTD 디바이스에서 이 정보를 사용하여 AnyConnect 클라이언트가 연결을 완료하는 방법을 조정할 수 있습니다.

예를 들어 AD/LDAP **memberOf** 특성을 Cisco **Group-Policy** 특성에 매핑할 수 있습니다. 그런 다음 AD/LDAP에서 가져올 수 있는 값을 VPN에 대해 정의한 RA VPN 그룹 정책의 이름과 동일시합니다. FTD 디바이스에서 사용자에게 대한 그룹 정책 특성을 찾으면 AnyConnect에서 해당 그룹 정책 이름을 사용하여 RA VPN에 연결하려고 합니다.

LDAP 특성 맵을 생성한 후에는 AD/LDAP 서버 설정에 연결합니다. 따라서 AD/LDAP 서버별로 맵이 다를 수 있습니다. 맵은 RA VPN 연결 프로파일 또는 그룹 정책에 직접 연결되지 않습니다.

LDAP 인증에 지원되는 Cisco 특성 목록은 ASA 8.4/8.6 설정 가이드, https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ref_extserver.html#pgfId-1773708에서 확인할 수 있습니다.

버전 6.7 이상부터는 FMC UI를 사용하여 이 기능을 구성할 수 있습니다. 자세한 내용은 **FTD에 대한 LDAP 인증 및 권한 부여를 사용하여 RA VPN 구성**을 참조하십시오. 이전 버전의 FMC의 경우 LDAP 특성 맵을 통해 그룹 정책 사용 제어, 9 페이지에 설명된 대로 FlexConfig를 사용하여 구성해야 합니다.

LDAP 특성 맵을 통해 그룹 정책 사용 제어

LDAP 특성 맵의 일반적인 용도는 사용자의 AD/LDAP 그룹 멤버십을 기반으로 사용자에게 할당되는 그룹 정책을 제어하는 것입니다. 이를 위해 **memberOf** AD/LDAP 특성 값을 Cisco **Group-Policy** 특성 값에 매핑합니다.

정리하면 LDAP 맵을 사용하기 위해서는 다음을 수행해야 합니다.

1. **ldap attribute-map** *name* 명령을 사용하여 맵을 만듭니다. 여기서 *name*은 특성 이름이 아닌 맵 이름입니다.
2. **map-name** *ldap_attribute_name Cisco_attribute_name* 명령을 사용하여 이름으로 이름에 따라 AD/LDAP 특성을 Cisco 특성에 매핑합니다.
3. **map-value** *ldap_attribute_name ldap_value Cisco_value* 명령을 사용하여 AD/LDAP 특성에 표시되어야 하는 값을 Cisco 특성의 관련 값에 매핑합니다.
4. **ldap-attribute-map** *name* 명령을 사용하여 하나 이상의 AD/LDAP 서버에 LDAP 특성 맵을 연결합니다. AD/LDAP 서버에 맵을 추가하는 명령과 맵 자체를 생성하는 명령 사이에는 미묘한 차이가 있습니다. 유일한 차이점은 전체 명령이 하이픈으로 연결되는 반면, 맵을 생성하는 기본 명령은 단순히 **ldap**라는 점입니다. 맵을 연결하기 위해 올바른 모드로 전환하려면 **aaa-server** *name host server_address* 명령을 사용해야 합니다.

다음 절차에서는 해당 프로세스를 포괄적으로 설명합니다.

시작하기 전에

이 절차는 모든 AnyConnect 버전에 사용할 수 있습니다.

이 예에서는 원격 액세스 VPN이 이미 구성되어 올바르게 작동한다고 가정합니다. VPN에서는 AD/LDAP를 인증 서버로 사용해야 하며, 해당 서버가 설정되어 있어야 합니다. 또한 모든 그룹 정책을 사전에 설정해야 합니다. FlexConfig에서 설정하지 마십시오.

목표는 다음 RA VPN 그룹 정책에 사용자를 매핑하는 것입니다.

- APP-SSL-VPN 관리자(AD/LDAP) 사용자는 LabAdminAccessGroupPolicy라는 그룹 정책을 사용해야 합니다.
- 엔지니어링(AD/LDAP) 사용자는 VPNAccessGroupPolicy라는 그룹 정책을 사용해야 합니다.

프로시저

단계 1 특성/값 매핑을 포함하여 LDAP 맵을 생성하는 deploy-Once/append FlexConfig 개체를 생성합니다. 이 개체는 맵만 생성하며 AD/LDAP 서버에는 맵을 할당하지 않습니다.

- a) **Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- b) 목차에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- c) **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.
 - **Name(이름)** - 개체 이름입니다. 예를 들면 Create_LDAP_Map_for_VPN_Access입니다.
 - **Deployment(구축)** - **Once(한 번)**를 선택합니다. 이러한 명령은 한 번만 설정하면 됩니다.
 - **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.

- **Object body**(개체 본문) - 개체 본문에 LDAP 맵을 생성하는 데 필요한 명령을 입력하고, AD/LDAP 특성을 Cisco 특성에 매핑한 다음 해당 특성의 값(AD/LDAP에서 반환됨)을 Cisco 특성의 의미 있는 값에 매핑합니다.

다음 예에서

- **LDAP_Map_for_VPN_Access**는 LDAP 특성 맵의 이름입니다. 원하는 이름을 사용할 수 있습니다.
- **memberOf**는 서버 자체에 정의된 AD/LDAP 특성의 이름입니다. 이는 임의의 문자열이 아닙니다.
- **Group-Policy**는 Cisco 특성의 이름이며 임의의 문자열이 아닙니다.
- **CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com**은 인증 중 AD/LDAP에서 **memberOf** 특성에 반환할 것으로 예상하는 값입니다. 이 문자열은 AD/LDAP 서버가 설정된 방식을 기반으로 합니다. 이 문자열은 사용자가 APP-SSL-VPN Managers 사용자 그룹의 구성원임을 나타냅니다.
- **LabAdminAccessGroupPolicy**는 FMC에 정의하여 RA VPN 연결 프로파일에서 사용 중인 그룹 정책의 이름입니다. 이 문자열은 기존 그룹 정책의 이름과 일치해야 합니다.
- **CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com**은 **memberOf** 특성에 반환될 것으로 예상되는 값입니다. 이 문자열은 사용자가 Engineering 사용자 그룹의 구성원임을 나타냅니다.
- **VPNAccessGroupPolicy**는 이미 존재하며 RA VPN에서 사용되는 그룹 정책의 이름입니다.


이 설정을 위한 명령은 다음과 같습니다.

```
ldap attribute-map LDAP_Map_for_VPN_Access
  map-name memberOf Group-Policy
  map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
  LabAdminAccessGroupPolicy
  map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com
  VPNAccessGroupPolicy
```

개체는 다음과 비슷해야 합니다.

Name:

Description:

 Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Type:

```
ldap attribute-map LDAP_Map_for_VPN_Access
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers, CN=Users, OU=stbu, DC=example, DC=com
LabAdminAccessGroupPolicy
map-value memberOf CN=Engineering, CN=Users, OU=stbu, DC=example, DC=com VPNAccessGroupPolicy
```

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

단계 2 AD/LDAP 서버에 맵을 할당하는 deploy-everytime/append FlexConfig 개체를 생성합니다.

AD/LDAP 영역을 Firepower Management Center에서 직접 정의하므로 구축할 때마다 해당 영역에 대한 FlexConfig 변경 사항이 제거됩니다. 따라서 각 구축 작업이 끝날 때마다 다시 설정해야 합니다.

FlexConfig 개체 페이지에서 **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 Attach_LDAP_Map_for_VPN_Access입니다.
- **Deployment(구축)** - **Everytime(항상)**을 선택합니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다.
- **Object body(개체 본문)** - 개체 본문에서 RA VPN에 사용되는 AD 서버에 맵을 할당하는 데 필요한 명령을 입력합니다.

다음 예에서

- **LDAP_Map_for_VPN_Access**는 이전 FlexConfig 개체에서 생성한 LDAP 특성 맵의 이름입니다.
- **ad_realm**은 RA VPN에서 사용 중인 AD/LDAP 영역의 이름이고, **10.100.10.10**은 영역에 있는 서버의 IP 주소입니다. 이 예에서는 서버가 하나뿐이라고 가정합니다. 추가 서버가 있는 경우 각 서버에 **aaa-server** 및 후속 **ldap-attribute-map** 명령을 반복해야 합니다. 영역 이름은 사용자가 선택한 이름으로 사용할 수 있지만 이 명령의 경우 수정하려는 RA VPN 연결에서 생성하고 사용한 영역의 이름과 정확히 일치해야 합니다. 마찬가지로 서버 주소도 영역 내에 실제로 구성된 주소여야 합니다.

이 설정을 위한 명령은 다음과 같습니다.

```
aaa-server ad-realm host 10.100.10.10
  ldap-attribute-map LDAP_Map_for_VPN_Access
exit
```

개체는 다음과 비슷해야 합니다.

단계 3 이러한 개체를 구축하는 FlexConfig 정책을 생성합니다.

- Devices(디바이스) > FlexConfig**를 선택합니다.
- New Policy(새 정책)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

- Ctrl 키를 누른 채 목차의 **User Defined(사용자 정의)** 폴더에서 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs(선택된 추가 FlexConfigs)** 목록에 추가해야 합니다.

- 끝어다 놓기를 사용하여 개체의 순서가 올바른지 확인합니다.

LDAP 특성 맵을 생성하는 개체는 AD/LDAP 서버에 맵을 할당하는 개체 앞에 있어야 합니다. 그렇지 않으면 아직 존재하지 않는 LDAP 특성 맵을 할당하려고 할 때 오류가 발생합니다.

목록은 다음과 같이 표시됩니다.

Selected Append FlexConfigs	
#.	Name
1.	Create_LDAP_Map_for_VPN_Access
2.	Attach_LDAP_Map_for_VPN_Access

- e) **Save(저장)**를 클릭합니다.
- f) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 **Save(저장)** 아래에 있는 **Policy Assignments(정책 할당)** 링크를 클릭하여 할당합니다.
- g) **Preview Config(구성 미리보기)**를 클릭하고, **Preview(미리보기)** 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. LDAP 특성 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI #####Flex-config Appended CLI ###
ldap attribute-map LDAP_Map_for_VPN_Access

map-name memberOf Group-Policy

map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
LabAdminAccessGroupPolicy

map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com VPNAccessGroupPolicy

aaa-server ad-realm host 10.100.10.10

ldap-attribute-map LDAP_Map_for_VPN_Access

exit
```

단계 4 변경 사항을 배포합니다.

단계 5 구성을 확인합니다.

각 FTD 디바이스에서 명령이 설정되었는지 확인할 수 있습니다. 디바이스에 대한 SSH 세션 또는 FMC의 CLI 툴을 사용합니다(**System(시스템) > Health(상태) > Monitor(모니터)**)를 선택한 후 디바이스를 클릭한 다음 **Advanced Troubleshooting(고급 문제 해결)**을 클릭하고 **Threat Defense CLI** 탭 선택). 다음은 설정을 표시하는 명령입니다.

- **show running-config aaa-server AD/LDAP** 서버 설정을 표시합니다.
- **show running-config ldap** 특성 맵을 표시합니다.

LDAP 특성 맵 제거

LDAP 특성 맵을 더 이상 사용하지 않으려면 FlexConfig 개체를 생성하여 기능을 구축한 디바이스에서 설정을 제거해야 합니다. FlexConfig 정책에서 FlexConfig 개체를 제거하는 것만으로는 충분하지 않습니다.

그러나 문제가 발생하는 경우 신속하게 해결하려면 AD/LDAP 서버에 맵을 할당하는 FlexConfig 개체를 제거하고 변경 사항을 구축하면 됩니다. 구축 프로세스는 관리되는 기능에 대한 모든 수정 사항을 제거하므로 서버에 맵을 할당하는 **ldap-attribute-map** 명령도 제거됩니다. 따라서 맵은 디바이스 설정에 계속 존재하지만 AD/LDAP 서버에는 사용되지 않습니다.

다음 절차에서는 맵 제거 방법을 설명합니다.

프로시저

단계 1 LDAP 특성 맵을 삭제하는 `deploy-once/append FlexConfig` 개체를 생성합니다.

일반적으로 특정 개체를 삭제하려면 이 개체를 사용하는 명령을 먼저 제거해야 합니다. 그러나 AD/LDAP 영역은 관리되는 기능이므로 구축 작업에서 해당 명령이 이미 제거되었습니다. 따라서 특성 맵만 삭제하면 됩니다.

- a) **Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- b) 목차에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- c) **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들어 `Delete_LDAP_Map_for_VPN_Access`를 입력합니다.
- **Deployment(구축) - Once(한 번)**를 선택합니다. 이러한 명령은 한 번만 설정하면 됩니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다. 이는 LDAP 특성 맵을 사용하는 명령을 제거하는 데 구축 작업을 사용하므로 특히 중요합니다.
- **개체 본문** - 개체 본문에 LDAP 특성 맵을 삭제하는 데 필요한 명령을 입력합니다. 맵 내용을 제거할 필요는 없습니다. 맵을 삭제하면 해당 맵의 내용도 제거됩니다. 예를 들어 맵 이름이 `LDAP_Map_for_VPN_Access`인 경우 명령은 다음과 같습니다.

```
no ldap attribute-map LDAP_Map_for_VPN_Access
```

개체는 다음과 비슷해야 합니다.

Name:

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Type:

```
no ldap attribute-map LDAP_Map_for_VPN_Access
```

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

단계 2 FlexConfig 정책을 편집하여 LDAP 특성 맵을 생성 및 할당하는 개체를 제거한 후 맵을 삭제하는 개체를 추가합니다.

- Devices(디바이스) > FlexConfig를 선택합니다.
- FlexConfig 정책을 편집합니다.
- Selected Appended FlexConfigs(선택된 추가 FlexConfig)에서 LDAP 특성 맵을 생성하고 할당하는 개체의 삭제 아이콘을 클릭합니다.
- 목차의 User Defined(사용자 정의) 폴더에서 맵을 삭제하는 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 Selected Appended FlexConfigs 목록에 추가해야 합니다.

목록은 다음과 같이 표시됩니다.

Selected Append FlexConfigs	
#.	Name
1.	Delete_LDAP_Map_for_VPN_Access

- Save(저장)를 클릭합니다.
- Preview Config(구성 미리보기)를 클릭하고, Preview(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 이 예에서는 다음과 유사한 내용이 표시됩니다.


```
###Flex-config Appended CLI ###
no ldap attribute-map LDAP_Map_for_VPN_Access
```

단계 3 변경 사항을 배포합니다.

AnyConnect 아이콘 및 로고 사용자 지정

Windows 및 Linux 클라이언트 시스템에서 AnyConnect 앱의 아이콘과 로고를 맞춤화할 수 있습니다. 아이콘의 이름은 미리 정의되어 있으며 업로드하는 이미지의 파일 유형 및 크기에 대한 특정 제한이 있습니다.

GUI를 맞춤화하기 위해 고유한 실행 파일을 구축할 경우 어떠한 파일명도 사용할 수 있지만, 이 예에서는 맞춤화된 프레임워크를 구축하지 않고 단순히 아이콘과 로고를 교체한다고 가정합니다.

대체할 수 있는 여러 이미지가 있으며 파일 이름은 플랫폼에 따라 다릅니다. 맞춤화 옵션, 파일 이름, 유형 및 크기에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide*(Cisco AnyConnect Secure Mobility Client 관리자 가이드)에서 AnyConnect 클라이언트 및 설치 프로그램의 맞춤화 및 현지화에 대한 챕터를 참조하십시오. 예를 들어 4.8 클라이언트 챕터는 다음에서 사용할 수 있습니다.

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html



참고 관리에 사용하는 툴과 관계없이 모든 FTD 디바이스에서 이러한 사용자 지정을 수행할 수 있습니다. 그러나 이러한 명령에 대한 FlexConfig는 FMC에서만 작동합니다.

시작하기 전에

이 예의 목적을 위해 Windows 클라이언트의 다음 이미지를 교체합니다. 이미지가 최대 크기와 다른 경우 시스템에서는 자동으로 이를 최대 크기로 조정하고 필요한 경우 이미지를 늘립니다.

- app_logo.png

이 애플리케이션 로고 이미지는 애플리케이션 아이콘이며 최대 크기는 128 x 128 픽셀입니다.

- company_logo.png

이 기업 로고 이미지는 트레이 플라이아웃 및 Advanced(고급) 대화 상자의 왼쪽 위 모서리에 표시됩니다. 최대 크기는 97 x 58 픽셀입니다.

- company_logo_alt.png

다른 기업 로고 이미지는 About(정보) 대화 상자의 오른쪽 아래 모서리에 표시됩니다. 최대 크기는 97 x 58 픽셀입니다.

이러한 파일을 업로드하려면 FTD 디바이스가 액세스할 수 있는 서버에 파일을 배치해야 합니다. TFTP, FTP, HTTP, HTTPS 또는 SCP 서버를 사용할 수 있습니다. 이러한 파일에서 이미지를 가져오는 URL에는 서버 설정에 필요한대로 경로 및 사용자 이름/비밀번호가 포함될 수 있습니다. 이 예에서는 TFTP를 사용합니다.

프로시저

단계 1 맞춤형 아이콘 및 로고를 사용해야 하는 RA VPN 헤드엔드 역할을 하는 각 FTD 디바이스에 이미 지 파일을 업로드합니다.

- a) SSH 클라이언트를 사용하여 디바이스 CLI에 로그인합니다.
- b) CLI에서 **system support diagnostic-cli** 명령을 입력하여 진단 CLI 모드를 시작합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdvl>
```

참고 메시지를 읽어보십시오! **Ctrl+a**를 누른 다음 **d**를 눌러 진단 CLI에서 나와 일반 FTD CLI 모드로 돌아와야 합니다.

- c) 명령 프롬프트를 참고합니다. 일반 CLI에서는 > 만 사용하는 반면, 진단 CLI의 사용자 EXEC 모드에서는 호스트 이름 +>를 사용합니다. 이 예에서는 ftdvl>입니다. #를 종료 문자로 사용하는 특별한 권한 EXEC 모드를 시작해야 합니다(예 : ftdvl #). 프롬프트에 이미 #이 있는 경우 이 단계를 건너 뛩니다. 그렇지 않으면 **enable** 명령을 입력하고 비밀번호를 입력하지 않고 비밀번호 프롬프트에서 Enter를 누릅니다.

```
ftdvl> enable
Password:
ftdvl#
```

- d) **copy** 명령을 사용하여 각 파일을 호스팅 서버에서 FTD 디바이스의 disk0으로 복사합니다. disk0:/anyconnect-images/와 같은 하위 디렉토리에 이들을 배치할 수 있습니다. **mkdir** 명령을 사용하여 새 폴더를 생성할 수 있습니다.

예를 들어 TFTP 서버의 IP 주소가 10.7.0.80이고 새 디렉토리를 생성하려는 경우 명령은 다음과 유사합니다. 첫 번째 예 이후에는 **copy** 명령에 대한 응답이 생략됩니다.

```
ftdvl# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdvl# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)
```

```
ftdvl1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdvl1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

단계 2 클라이언트 시스템에 설치할 때 진단 CLI의 **import webvpn** 명령을 사용하여 AnyConnect에 이러한 이미지를 다운로드하도록 지시합니다.

```
import webvpn AnyConnect-customization type resource platform win name filename
disk0:/directoryname/filename
```

이 명령은 Windows용입니다. Linux의 경우 **win** 키워드를 클라이언트에 따라 **linux** 또는 **linux-64**으로 대체합니다.

예를 들어 이전 단계에서 업로드한 파일을 가져오고 진단 CLI에 아직 있다고 가정합니다.

```
ftdvl1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdvl1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdvl1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

참고 이 단계는 FlexConfig를 사용하여 수행할 수 있습니다. `deploy-once/append FlexConfig` 개체에 **import webvpn** 명령을 입력하고 FlexConfig 정책에 해당 개체를 추가한 다음 FlexConfig 정책을 관련 FTD 디바이스에 할당하면 됩니다. 그러나 이미지를 업로드하려면 각 디바이스에서 진단 CLI 권한이 있는 EXEC 모드로 전환해야 하므로 이미지를 동시에 가져오는 것이 실용적입니다.

단계 3 컨피그레이션을 확인합니다.

- 가져온 파일을 확인하려면 진단 CLI의 특별 권한 EXEC 모드에서 **show import webvpn AnyConnect-customization** 명령을 사용하십시오.
- 이미지가 클라이언트에 다운로드되었는지 확인하려면 사용자가 클라이언트를 실행할 때 이미지가 표시되어야 합니다. Windows 클라이언트에서 다음 폴더를 확인할 수도 있습니다. 여기서 `%PROGRAMFILES%`는 일반적으로 `c:\Program Files`로 확인됩니다.
`%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\`

다음에 수행할 작업

기본 이미지로 돌아가려면 맞춤형 각 이미지에 대해(진단 CLI 특별 권한 EXEC 모드에서) **revert webvpn** 명령을 사용합니다. 이 작업은 `deploy-once/append FlexConfig`에서 수행할 수 있습니다. RA VPN을 얼마간 실행한 후 이 작업을 수행할 수 있으므로 더 이 방법이 더 합리적입니다. FlexConfig를 사용하면 각 디바이스에 SSH 연결을 손쉽게 구축하고 단일 구축 작업을 통해 작업을 완료할 수 있습니다. 명령은 다음과 같습니다.

```
revert webvpn AnyConnect-customization type resource platform win name filename
```

`import webvpn`에서와 마찬가지로 해당 클라이언트 플랫폼을 맞춤화한 경우, `win`을 `linux` 또는 `linux-64`로 대체하고 가져온 각 이미지 파일 이름에 대해 명령을 개별적으로 실행합니다. 예를 들면 다음과 같습니다.

```
ftdvl1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png
```

```
ftdvl1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png
```

```
ftdvl1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

FlexConfig를 사용하여 AnyConnect 모듈 및 프로파일 설정

AnyConnect 패키지에는 다양한 기능을 위한 모듈(예: AMP Enabler)이 포함되며, 이러한 모듈은 RA VPN 연결에 추가 서비스를 제공하는 데 선택적으로 사용할 수 있습니다. 각 모듈에는 요구 사항에 따라 모듈이 작동하도록 편집할 수 있는 프로파일이 포함되어 있습니다. FTD에서 이러한 모듈 및 프로파일을 활성화하려면 FlexConfig를 사용해야 합니다.

사용할 모듈만 설정해야 합니다. 각 모듈에는 고유의 프로파일 편집기가 있으며, 이 프로파일 편집기는 Windows 시스템에서 다운로드하여 설치할 수 있는 AnyConnect 프로파일 편집기 패키지에 포함되어 있습니다.

AnyConnect 패키지 파일에는 모든 모듈이 포함되므로 모듈 자체는 업로드하지 않습니다. 원격 액세스 VPN 설정에서 작동하도록 모듈 동작을 사용자 지정하려면 모듈에서 사용하는 프로파일만 업로드하면 됩니다.

버전 6.7 이상부터는 FMC UI를 사용하여 이 기능을 구성할 수 있습니다. 자세한 내용은 [Cisco Secure Firewall Management Center를 사용하여 위협 방어에 보안 클라이언트 모듈 설정을 참조하십시오](#).

버전 6.4~6.6에서는 FlexConfig를 사용하여 FTD에서 애플 VPN을 사용하도록 설정할 수 있습니다. 이 구성에 다음 절차를 사용합니다.

시작하기 전에

클라이언트 프로파일을 업로드하려면 다음을 수행해야 합니다.

- 독립형 AnyConnect “프로파일 편집기 - Windows/독립형 설치 관리자(MSI)”를 다운로드하여 설치합니다. 설치 파일은 Windows 전용이며 파일 이름은 `tools-anyconnect-profileeditor-win-<version>-k9.msi`, where `<version>`입니다. 여기서 `<version>`은 AnyConnect 버전입니다. 예를 들면 `tools-anyconnect-win-4.8.03036-profileeditor-k9.msi`입니다. 또한 프로파일 편집기를 설치하기 전에 Java JRE 1.6 이상도 설치해야 합니다. software.cisco.com의 AnyConnect Secure Mobility Client 범주에서 AnyConnect 프로파일 편집기를 가져옵니다.
- 프로파일 편집기를 사용하여 필요한 프로파일을 생성합니다. 자세한 내용은 편집기의 온라인 도움말을 참조하십시오.

이 예에서는 프로파일을 업로드하고 모든 모듈을 활성화합니다. 이 예에서는 이미 작동 중인 RA VPN이 있고 FMC를 사용하여 모든 그룹 정책을 생성했다고 가정합니다.

프로시저

단계 1 사용자 지정 모듈 프로파일을 사용해야 하는 RA VPN 헤드엔드 역할을 하는 각 FTD 디바이스에 프로파일을 업로드합니다.

- a) SSH 클라이언트를 사용하여 디바이스 CLI에 로그인합니다.
- b) CLI에서 **system support diagnostic-cli** 명령을 입력하여 진단 CLI 모드를 시작합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdv1>
```

참고 메시지를 읽어보십시오! **Ctrl+a**를 누른 다음 **d**를 눌러 진단 CLI에서 나와 일반 FTD CLI 모드로 돌아와야 합니다.

- c) 명령 프롬프트를 참고합니다. 일반 CLI에서는 > 만 사용하는 반면, 진단 CLI의 사용자 EXEC 모드에서는 호스트 이름 +>를 사용합니다. 이 예에서는 ftdv1>입니다. #를 종료 문자로 사용하는 특별 권한 EXEC 모드를 시작해야 합니다(예 : ftdv1 #). 프롬프트에 이미 #이 있는 경우 이 단계를 건너 뛩니다. 그렇지 않으면 enable 명령을 입력하고 비밀번호를 입력하지 않고 비밀번호 프롬프트에서 Enter를 누릅니다.

```
ftdv1> enable
Password:
ftdv1#
```

- d) **copy** 명령을 사용하여 각 파일을 호스팅 서버에서 FTD 디바이스의 disk0으로 복사합니다. 해당 파일은 disk0:/modules/와 같은 하위 디렉터리에 저장할 수 있습니다. **mkdir** 명령을 사용하여 새 폴더를 생성할 수 있습니다.

예를 들어 TFTP 서버의 IP 주소가 10.7.0.80이고 새 디렉토리를 생성하려는 경우 명령은 다음과 유사합니다. 첫 번째 예 이후에는 **copy** 명령에 대한 응답이 생략됩니다.

```
ftdv1# mkdir disk0:modules

Create directory filename [modules]? yes

Created dir disk0:/modules

ftdv1# copy /noconfirm tftp://10.7.0.80/amp.asp
disk0:/modules/amp.asp

Accessing tftp://10.7.0.80/amp.asp...!!!
Writing file disk0:/modules/amp.asp...
!
676 bytes copied in 0.0 secs (812800 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/ACManifestUmbrella-01.xml
disk0:/modules/ACManifestUmbrella-01.xml
ftdv1# copy /noconfirm tftp://10.7.0.80/feedback.fsp
disk0:/modules/feedback.fsp
ftdv1# copy /noconfirm tftp://10.7.0.80/iseposture.isp
disk0:/modules/iseposture.isp
```

```
ftdvl# copy /noconfirm tftp://10.7.0.80/nam.nsp
disk0:/modules/nam.nsp
ftdvl# copy /noconfirm tftp://10.7.0.80/networkvisibility.nvmsp
disk0:/modules/networkvisibility.nvmsp
ftdvl# copy /noconfirm tftp://10.7.0.80/websecurity.wso
disk0:/modules/websecurity.wso
ftdvl# copy /noconfirm tftp://10.7.0.80/vpn.xml
disk0:/modules/vpn.xml
```

단계 2 각 모듈의 프로파일을 식별하고 RA VPN의 각 그룹 프로파일에 대해 모듈을 활성화하는 deploy-everytime/append FlexConfig 개체를 생성합니다.

- Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- 목차에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 Enable_AnyConnect_Module_Profiles입니다.
- **Deployment(구축) - Everytime(항상)**을 선택합니다. FMC에서 적극적으로 관리하는 기능을 변경하고 있으므로 각 구축 작업 중에 변경 사항이 제거됩니다. 따라서 변경 사항을 구축할 때마다 다시 설정해야 합니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다.
- **Object body(개체 본문)** - 개체 본문에서 프로파일을 식별하고 모듈을 활성화한 후 프로파일을 사용해야 하는 각 그룹 정책에 프로파일을 적용하는 데 필요한 명령을 입력합니다. 설정해야 하는 명령은 다음과 같습니다.

- **anyconnect profiles** *profile_name file_location*

이 명령은 webvpn 설정 모드에서 프로파일 이름과 FTD 디바이스 디스크에 있는 프로파일의 전체 경로 및 파일 이름을 지정합니다. 이 명령을 사용하면 AnyConnect 및 해당 모듈에서 프로파일을 사용할 수 있습니다.

- **anyconnect modules value** *module_name*

이 명령은 그룹 정책 webvpn 설정 모드에서 그룹 정책에 활성화할 AnyConnect 모듈을 지정합니다. 해당 모듈을 사용해야 하는 각 그룹 정책에서 이 명령을 사용해야 합니다. 여러 개의 모듈을 공백 없이 쉼표로 구분하여 지정할 수 있습니다.

- 가능한 모듈 이름은 다음과 같습니다.

- **dart-** AnyConnect DART(Diagnostics and Reporting Tool)
- **nam-** AnyConnect Network Access Manager
- **vpngina-** AnyConnect SBL(Start Before Logon)
- **websecurity-** AnyConnect Web Security 모듈
- **telemetry-** AnyConnect Telemetry 모듈
- **posture-** AnyConnect Posture 모듈
- **ampenabler-** AnyConnect AMP Enabler

- **iseposture**- AnyConnect ISE Posture
- **umbrella**- AnyConnect Umbrella
- **anyconnect profiles value profile_name type module_name**

이 명령은 그룹 정책 webvpn 설정 모드에서 **anyconnect modules** 명령으로 활성화한 모듈에 사용할 프로파일을 지정합니다. **feedback** 모듈은 예외이며 먼저 활성화하지 않아도 됩니다. 모듈 이름은 **anyconnect modules** 명령에서 사용하는 것과 동일하지만 **vpngina**는 예외이며 해당 유형은 **user**입니다.

예를 들어 다음 명령은 G10이라는 그룹 정책에 대해 이전에 업로드한 모듈을 설정합니다. 추가 그룹 정책이 있는 경우 각 그룹 정책에 대해 **group-policy** 명령으로 시작하는 명령 집합을 반복해야 합니다.

```
webvpn
  anyconnect profiles ACManifestUmbrella-01.xml
disk0:/modules/ACManifestUmbrella-01.xml
anyconnect profiles amp.asp disk0:/modules/amp.asp
anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp
anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp
anyconnect profiles nam.nsp disk0:/modules/nam.nsp
anyconnect profiles networkvisibility.nvmsp disk0:/modules/networkvisibility.nvmsp

anyconnect profiles vpn.xml disk0:/modules/vpn.xml
anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso
group-policy GP10 attributes
  webvpn
    anyconnect modules value
ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity
    anyconnect profiles value amp.asp type ampenabler
    anyconnect profiles value feedback.fsp type feedback
    anyconnect profiles value iseposture.isp type iseposture
    anyconnect profiles value nam.nsp type nam
    anyconnect profiles value networkvisibility.nvmsp type nvm
    anyconnect profiles value ACManifestUmbrella-01.xml type umbrella
    anyconnect profiles value websecurity.wso type websecurity
    anyconnect profiles value vpn.xml type user
```

개체는 다음과 비슷해야 합니다.

FlexConfig를 사용하여 AnyConnect 모듈 및 프로파일 설정

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Type:

```
webvpn
anyconnect profiles ACManifestUmbrella-01.xml disk0:/modules/ACManifestUmbrella-01.xml
anyconnect profiles amp.asp disk0:/modules/amp.asp
anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp
anyconnect profiles ise posture.isp disk0:/modules/ise posture.isp
anyconnect profiles nam.nsp disk0:/modules/nam.nsp
anyconnect profiles networkvisibility.nvm sp disk0:/modules/networkvisibility.nvm sp
anyconnect profiles vpn.xml disk0:/modules/vpn.xml
anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso
group-policy GP10 attributes
webvpn
anyconnect modules value ampenabler, dart, ise posture, nam, nvm, umbrella, vpngina, websecurity
anyconnect profiles value amp.asp type ampenabler
anyconnect profiles value feedback.fsp type feedback
```

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

단계 3 이 개체를 구축하는 FlexConfig 정책을 생성합니다.

- Devices**(디바이스) > **FlexConfig**를 선택합니다.
- New Policy**(새 정책)를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

- 목차의 **User Defined**(사용자 정의) 폴더에서 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs** 목록에 추가해야 합니다.

목록은 다음과 같이 표시됩니다.

Selected Append FlexConfigs	
#.	Name
1.	Enable_AnyConnect_Module_Profiles

- Save**(저장)를 클릭합니다.
- 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 **Save**(저장) 아래에 있는 **Policy Assignments**(정책 할당) 링크를 클릭하여 할당합니다.
- Preview Config**(구성 미리보기)를 클릭하고, **Preview**(미리보기) 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 이러한 명령의 경우 다음과 유사한 내용이 표시됩니다.

```
###Flex-config Appended CLI ###
webvpn

anyconnect profiles ACManifestUmbrella-01.xml disk0:/modules/ACManifestUmbrella-01.xml

anyconnect profiles amp.asp disk0:/modules/amp.asp

anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp

anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp

anyconnect profiles nam.nsp disk0:/modules/nam.nsp

anyconnect profiles networkvisibility.nvmisp disk0:/modules/networkvisibility.nvmisp

anyconnect profiles vpn.xml disk0:/modules/vpn.xml

anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso

group-policy GP10 attributes

webvpn

anyconnect modules value ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity

anyconnect profiles value amp.asp type ampenabler

anyconnect profiles value feedback.fsp type feedback

anyconnect profiles value iseposture.isp type iseposture

anyconnect profiles value nam.nsp type nam

anyconnect profiles value networkvisibility.nvmisp type nvm

anyconnect profiles value ACManifestUmbrella-01.xml type umbrella

anyconnect profiles value websecurity.wso type websecurity

anyconnect profiles value vpn.xml type user
```

단계 4 변경 사항을 배포합니다.

다음에 수행할 작업

관리형 기능을 변경하고 있으므로 모듈 설정을 제거하려면 FlexConfig 정책에서 FlexConfig 개체를 삭제 한 다음 설정을 다시 구축하기만 하면 됩니다. 구축 작업을 수행하면 설정 변경 사항이 제거됩니다.

디바이스에서 프로파일을 제거하려면 각 디바이스의 CLI에 로그인하여 진단 CLI에서 권한 있는 EXEC 모드로 **delete** 명령을 사용해야 합니다.

모바일 디바이스의 애플리케이션 기반(앱별) 원격 액세스 VPN

Android 또는 iOS를 실행하는 휴대폰과 같이 모바일 디바이스를 지원하는 경우, 지원되는 애플리케이션만 VPN 터널을 사용하도록 MDM(Mobile Device Manager) 애플리케이션을 사용하여 VPN 액세스 권한을 세부적으로 조정할 수 있습니다. 원격 액세스 VPN을 승인된 애플리케이션으로 제한하면 VPN 헤드엔드에 대한 로드를 줄일 뿐만 아니라 이러한 모바일 디바이스에 설치된 악성 애플리케이션으로부터 기업 네트워크를 보호할 수 있습니다.

앱별 원격 액세스 VPN을 사용하려면 타사 MDM 애플리케이션을 설치하고 설정해야 합니다. MDM에서는 VPN 터널을 통해 사용할 수 있는 승인된 애플리케이션 목록을 정의합니다. 선택한 타사 MDM을 구성하고 사용하는 방법에 대한 설명은 이 문서에서 다루지 않습니다.

버전 7.0 이상부터는 FMC UI를 사용하여 이 기능을 구성할 수 있습니다. 자세한 내용은 [Cisco Secure Firewall Management Center를 사용하여 모바일 디바이스에서 애플리케이션 기반 원격 액세스 VPN\(앱별 VPN\) 구성](#)을 참조하십시오.

버전 6.4~6.7에서는 FlexConfig를 사용하여 FTD에서 앱별 VPN을 사용하도록 설정할 수 있습니다. 다음 주제에서는 MDM에서 모바일 디바이스에 정책을 적용할 수 있도록 FlexConfig를 사용하여 FTD 헤드엔드에서 앱별 VPN을 활성화하는 방법을 설명합니다.

애플리케이션 기반(앱별) VPN 정보

AnyConnect를 사용하여 모바일 디바이스에서 VPN 연결을 설정하면 개인 애플리케이션의 트래픽을 포함한 모든 트래픽이 VPN을 통해 라우팅됩니다.

기업 애플리케이션만 VPN을 통해 라우팅하려면 기업 이외의 트래픽을 VPN에서 제외하도록 Per App VPN을 사용하여 VPN을 통해 터널링할 애플리케이션을 선택하면 됩니다.

perapp AnyConnect 사용자 지정 특성을 사용하여 Per App VPN을 구성합니다. 이 특성을 원격 액세스 VPN 그룹 프로파일에 추가하면 터널이 명시적으로 식별된 애플리케이션으로 자동으로 제한됩니다. 다른 모든 애플리케이션의 트래픽은 터널에서 자동으로 제외됩니다.

Per App VPN을 구성하면 다음과 같은 주요 이점이 있습니다.

- **Performance(성능)** - VPN의 트래픽을 기업 네트워크로 이동해야 하는 트래픽으로 제한합니다. 따라서 RA VPN의 헤드엔드에서 리소스를 확보합니다.
- **Protection(보호)** - 승인된 애플리케이션의 트래픽만 허용되므로 사용자가 모바일 디바이스에 무단으로 설치할 수 있는 승인되지 않은 악성 애플리케이션으로부터 회사 터널을 보호합니다. 이러한 애플리케이션은 터널에 포함되지 않으므로 해당 애플리케이션의 트래픽은 헤드엔드로 전송되지 않습니다.

모바일 엔드포인트에서 실행 중인 MDM(Mobile Device Manager)은 애플리케이션에 앱별 VPN 정책을 적용합니다.

모바일 앱의 애플리케이션 ID 확인

모바일 디바이스의 애플리케이션 기반 VPN을 허용하도록 FTD 헤드 엔드를 설정하려면 터널에서 허용할 앱을 결정해야 합니다.

사용자의 모바일 디바이스에서 서비스를 제공하도록 선택한 MDM(Mobile Device Manager)에서 앱별 정책을 구성하는 것이 좋습니다. 그러면 헤드엔드 설정이 훨씬 간소화됩니다.

대신 헤드엔드에서 허용되는 앱 목록을 설정하려면 각 엔드포인트 유형에서 각 애플리케이션의 애플리케이션 ID를 확인해야 합니다.

iOS에서 번들 ID라고 하는 애플리케이션 ID는 역방향 DNS 이름입니다. 별표(*)를 와일드카드로 사용할 수 있습니다. 예를 들어 *.*는 모든 애플리케이션을 나타내고, com.cisco.*는 모든 Cisco 애플리케이션을 나타냅니다.

애플리케이션 ID를 확인하려면 다음을 수행합니다.

- **Android** - 웹 브라우저에서 Google Play로 이동하여 앱 카테고리를 선택합니다. 허용할 애플리케이션을 클릭하거나 마우스로 가리킨 다음 URL을 확인합니다. 앱 ID는 UR의 id= 매개변수에 있습니다. 예를 들어 다음 URL은 Facebook Messenger에 대한 것으로, 앱 ID는 com.facebook.orca입니다.

<https://play.google.com/store/apps/details?id=com.facebook.orca>

Google Play를 통해 사용할 수 없는 애플리케이션(예: 사용자가 만든 애플리케이션)의 경우 패키지 이름 뷰어 애플리케이션을 다운로드하여 앱 ID를 추출하십시오. 이러한 애플리케이션은 대부분 사용 가능하며 그중 하나에서 필요한 기능을 제공할 수 있지만 Cisco에서는 이러한 애플리케이션을 보증하지 않습니다.

- **iOS** - 번들 ID를 직접 가져올 수 있는 방법이 없습니다. 다음은 번들 ID를 찾는 한 가지 방법입니다.

1. Chrome과 같은 데스크톱 웹 브라우저를 사용하여 애플리케이션 이름을 검색합니다.

2. 검색 결과에서 Apple App Store에서 앱을 다운로드할 수 있는 링크가 있는지 확인합니다. 예를 들어 Facebook Messenger는 다음과 유사합니다.

<https://apps.apple.com/us/app/messenger/id454638411>

3. id 문자열 뒤의 숫자를 복사합니다. 이 예에서는 **454638411**입니다.

4. 새 브라우저 창을 열고 다음 URL 끝에 이 숫자를 추가합니다.

<https://itunes.apple.com/lookup?id=>

이 예의 경우 <https://itunes.apple.com/lookup?id=454638411>입니다.

5. 일반적으로 1.txt라는 텍스트 파일을 다운로드하라는 메시지가 표시됩니다. 파일을 다운로드합니다.

6. WordPad와 같은 텍스트 편집기에서 파일을 열고 bundleId를 검색합니다. 대표적인 예는 다음과 같습니다.

"bundleId": "com.facebook.Messenger"

이 예에서 번들 ID는 com.facebook.Messenger입니다. 이 ID를 앱 ID로 사용합니다.

애플리케이션 ID 목록이 생성되면 [애플리케이션 기반\(앱별\) VPN 터널 설정, 28 페이지](#)에 설명된 대로 정책을 설정할 수 있습니다.

애플리케이션 기반(앱별) VPN 터널 설정

MDM(Mobile Device Manager) 소프트웨어 솔루션을 설치하고 구성하면 FTD 헤드엔드 디바이스에서 애플리케이션 기반(앱별) VPN을 활성화할 수 있습니다. 헤드엔드에서 활성화되면 MDM 소프트웨어에서 VPN을 통해 기업 네트워크로 터널링되는 애플리케이션을 제어하기 시작합니다.

시작하기 전에

이 기능을 사용하려면 AnyConnect Plus 또는 Apex 라이선스가 필요합니다. Android 및 iOS 디바이스에서만 작동합니다.

이 예에서는 원격 액세스 VPN이 이미 설정되어 올바르게 작동한다고 가정합니다.

타사 Mobile Device Manager가 이미 설치되고 구성되어 있어야 합니다. FTD 헤드엔드 디바이스가 아닌 MDM 자체의 VPN에서 허용되는 애플리케이션을 구성합니다. 대신 FTD에서 간단히 앱별 VPN을 활성화한 다음 MDM을 사용하여 앱별 정책을 구성하고 구현하는 것이 모범 사례입니다. 다음 예에서는 FTD 헤드엔드에서 애플리케이션을 지정하는 대신 이 방법을 사용한다고 가정합니다.

프로시저

단계 1 software.cisco.com에서 **Cisco AnyConnect Enterprise Application Selector(Cisco AnyConnect 엔터프라이즈 애플리케이션 선택기)**를 다운로드합니다. 이 애플리케이션은 **AnyConnect Secure Mobility Client v4.x** 범주에 있습니다.

애플리케이션 jar 파일을 실행하려면 Java 7을 실행 중이어야 합니다.

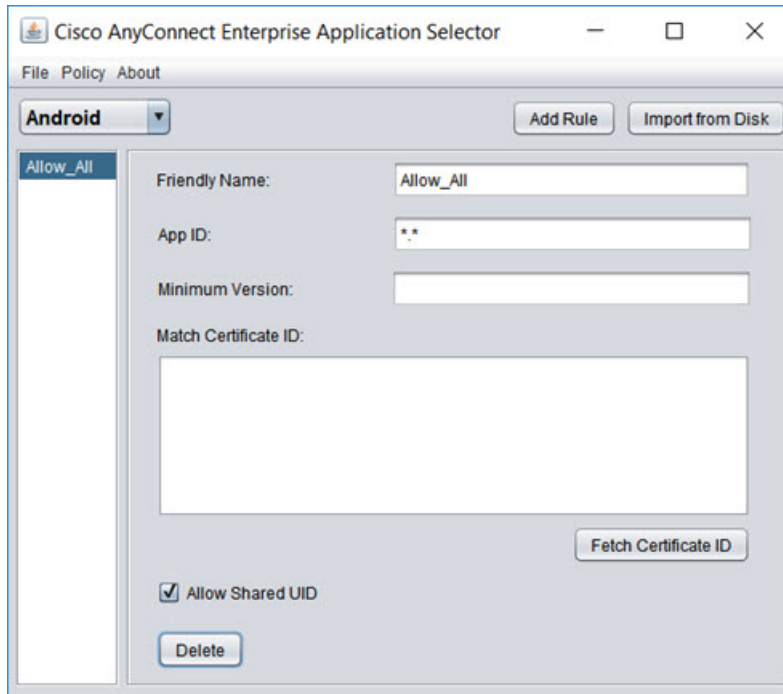
단계 2 AnyConnect 엔터프라이즈 애플리케이션 선택기를 사용하여 Per App VPN 정책을 정의합니다.

간단한 '모두 허용' 정책을 생성한 후 MDM 설정에 허용되는 앱을 정의하는 것이 좋습니다. 그러나 헤드엔드에서 목록을 허용하고 제어할 애플리케이션 목록을 지정할 수 있습니다. 특정 애플리케이션을 포함하려면 고유한 식별 이름과 애플리케이션의 앱 ID를 사용하여 각 애플리케이션에 별도의 규칙을 생성합니다. 앱 ID 가져오기에 대한 자세한 내용은 [모바일 앱의 애플리케이션 ID 확인, 27 페이지](#)를 참조하십시오.

다음 절차에서는 Android 및 iOS 플랫폼을 모두 지원하는 '모두 허용' 정책을 생성하는 방법을 설명합니다.

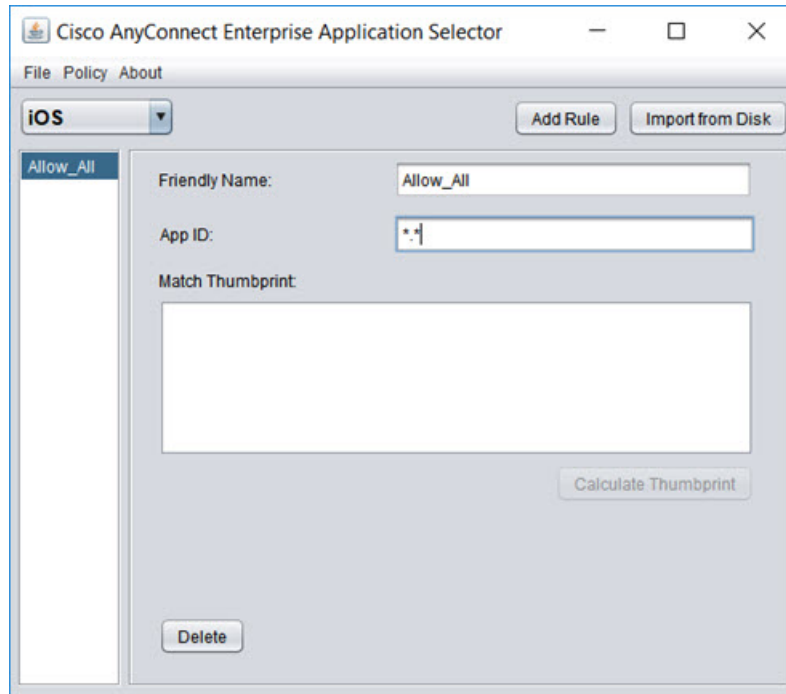
a) AnyConnect 엔터프라이즈 애플리케이션 선택기에서 플랫폼 유형으로 **Android**를 선택한 후 다음 옵션을 입력합니다.

- **Friendly Name(식별 이름)** - **Allow_All**과 같이 의미 있는 이름입니다.
- **App ID(앱 ID)** - 가능한 모든 애플리케이션과 일치하도록 *.*를 입력합니다.
- 다른 필드는 모두 무시하십시오. 이러한 필드는 정확한 애플리케이션 및 버전에 대한 정책을 세분화하는 데 사용됩니다.



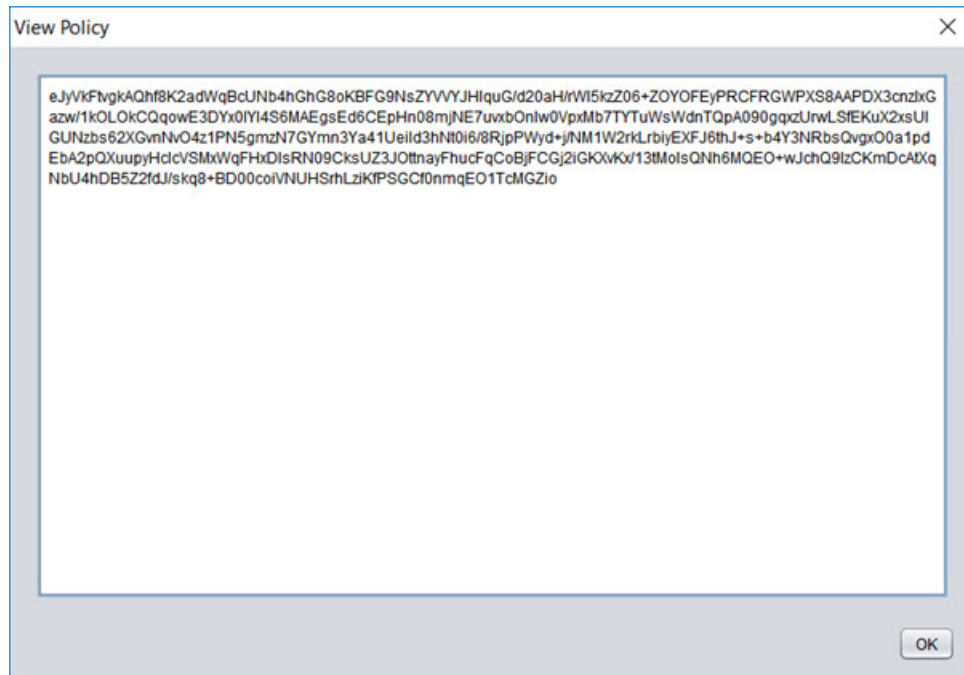
b) iOS를 플랫폼 유형으로 선택하고 다음 옵션을 입력합니다.

- **Friendly Name**(식별 이름) - **Allow_All**과 같이 의미 있는 이름입니다.
- **App ID**(앱 ID) - 가능한 모든 애플리케이션과 일치하도록 ******를 입력합니다.
- 다른 필드는 모두 무시하십시오.



- c) **Policy(정책) > View Policy(정책 보기)**를 선택합니다.

읽을 수 없는 base64 문자열이 표시됩니다. 이 문자열에는 암호화된 XML 파일이 포함되어 있으며, 생성한 정책을 보기 위해 FTD 시스템에서 이 파일의 압축을 풉니다. 다음 단계에서 이 문자열의 복사본을 사용합니다.



단계 3 perapp 사용자 지정 특성을 생성하고 AnyConnect 엔터프라이즈 애플리케이션 선택기에서 생성한 앱별 base64 정책을 특성에 할당하는 deploy-once/append FlexConfig 개체를 생성합니다.

- a) **Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- b) 목차에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- c) **Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 Per_App_Allow_All_Policy입니다.
- **Deployment(구축) - Once(한 번)**를 선택합니다. 이러한 명령은 한 번만 설정하면 됩니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다. 명령은 직접 지원 기능용 명령이 전송된 후에 디바이스에 전송됩니다.
- **Object body(개체 본문)** - 개체 본문에 **perapp** 유형의 특성을 생성하는 데 필요한 명령을 입력한 다음 특성 이름 및 base64 정책 문자열에 해당하는 데이터를 추가합니다. 데이터 요소는 420자로 제한됩니다. 따라서 base64 문자열이 이보다 길면 문자열을 분할하여 여러 개의 **anyconnect-custom-data** 명령을 사용해야 합니다. 지정된 변수에 대해 여러 데이터 명령을 사용하면 두 번째 및 후속 명령이 첫 번째 데이터 문자열에 간단히 추가됩니다. base64 문자열을 정확히 420자로 잘라내거나 처리하기 쉬운 청크로 잘라낼 수 있습니다. 예를 들어 perAppPolicy라는 특성을 만들고 Allow_All 정책을 사용하려는 경우 명령은 다음과 같습니다. 설명은 선택 사항이지만 포함하는 경우 별도의 명령이 아닌 **anyconnect-custom-attr** 명령의 일부입니다. (이 예에서는 가독성을 높이기 위해 줄 바꿈 되어 있습니다.)

```
webvpn
  anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
  anyconnect-custom-data perapp perAppPolicy
  eJyVkfTvgkAQhf8K2adWqBcUNb4hGhG8oKBFG9NsZYVYJHlquG/d20aH/rW15kzZ06+
  ZOYOFeyPRCFRGWPXS8AAPDX3cnzlxGazw/1kOLOkCQqowE3DYx0IYI4S6MAEgsEd6CEp
  Hn08mjNE7uvxbOnIw0VpxMb7TYTuWsWdnTQpA090gqxzUrwlSfEKuX2xsU1GUNzbs62X
  GvnNvO4z1PN5gmzN7GYmn3Ya41Ueild3hNt0i6/8Rj
  anyconnect-custom-data perapp perAppPolicy
  pPWyd+j/NM1W2rkLrbiyEXFJ6thJ+s+b4Y3NRbsQvgx00a1pdEbA2pQXuupyHclVSMxW
  qFHxD1sRN09CksUZ3JOttnayFhucFqCoBjFCGj2iGKXvKx/13tMoIsQNh6MQEO+wJchQ9
  IzCKmDcAtXqNbU4hDB5Z2fdJ/skq8+BD00coiVNUHSrhLziKfPSGCF0nmqEO1TcMGZio
```

개체는 다음과 비슷해야 합니다.

Name:

Description:

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Deployment: Type:

```
webvpn
anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
anyconnect-custom-data perapp perAppPolicy
eJyVkfTvgkAQhf8K2adWqBcUNb4hGhG8oKBFg9NsZYVVYJH1quG/d20aH/rW15kzZ06+ZOYOFeyPRCFRGWPXS8AAPDX3cnzlxGazw/1
anyconnect-custom-data perapp perAppPolicy
pFWydj/NM1W2rkLrbiyEXFJ6thJ+s+b4Y3NRbsQvgx00a1pdEbA2pQXuupyHclcVSMxWqFHxD1sRN09CksUZ3JOttnayFhucFqCoBj
```

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

단계 4 사용자 지정 그룹 정책을 사용하는 경우 `deploy-once/append FlexConfig` 개체를 생성하여 그룹 정책에서 동적 스플릿 터널 사용자 지정 특성을 설정합니다.

이름이 `DfltGrpPolicy`인 기본 그룹 정책을 사용하는 경우 `deploy-everytime/append FlexConfig` 개체를 생성하여 그룹 정책에서 동적 스플릿 터널 사용자 지정 특성을 구성합니다. 구축할 때마다 기본 정책에 대한 모든 사용자 지정 변경 사항이 무효화되므로 이 개체를 매번 구축해야 합니다.

사용자 지정 그룹 정책은 기본 그룹 정책과 달리 변경 사항이 무효화되지 않으므로 변경 사항을 한번 구축해야 합니다. 여러 그룹 정책을 사용하는 경우 단일 `FlexConfig` 개체를 사용하여 각 정책에 사용자 지정 특성을 차례로 추가할 수 있습니다. 또는 그룹 정책당 하나의 `FlexConfig` 개체를 생성할 수 있습니다. 결과는 동일하므로 `FlexConfig` 정책 모듈화에 대한 고유의 요구 사항에 따라 선택합니다.

다음 절차는 "sales" 사용자 지정 그룹 정책을 위한 것입니다. 기본 그룹이 아닌 사용자 지정 그룹을 사용하는 것이 좋습니다.

- Objects(개체) > Object Management(개체 관리)**를 선택합니다.
- 목록에서 **FlexConfig > FlexConfig Object(FlexConfig 개체)**를 선택합니다.
- Add FlexConfig Object(FlexConfig 개체 추가)**를 클릭하고, 다음 속성을 구성한 다음 **Save(저장)**를 클릭합니다.

- **Name(이름)** - 개체 이름입니다. 예를 들면 `Add_Per_App_VPN`입니다.
- **Deployment(구축)** - **Once(한 번)**를 선택합니다.
- **Type(유형)** - 기본값인 **Append(추가)**를 그대로 유지합니다.

- **Object body(개체 본문)** - 개체 본문에 사용자 지정 특성을 그룹 정책에 추가하는 데 필요한 명령을 입력합니다. 예를 들어 생성한 특성의 이름이 perAppPolicy이고 그룹 정책의 이름이 "sales"라면 명령은 다음과 같습니다.

```
group-policy sales attributes
anyconnect-custom perapp value perAppPolicy
```

개체는 다음과 비슷해야 합니다.

단계 5 이러한 개체를 구축하는 FlexConfig 정책을 생성합니다.

- Devices(디바이스) > FlexConfig**를 선택합니다.
- New Policy(새 정책)**를 클릭하거나, 기존 FlexConfig 정책을 대상 디바이스에 할당해야 한다면(또는 이미 할당되어 있다면) 해당 정책을 수정합니다.

새 정책을 생성할 때는 정책 이름을 지정하는 대화 상자의 정책에 대상 디바이스를 할당합니다.

- Ctrl 키를 누른 채 목차의 **User Defined(사용자 정의)** 폴더에서 FlexConfig 개체를 선택하고 >을 클릭하여 정책에 추가합니다.

개체는 **Selected Appended FlexConfigs(선택된 추가 FlexConfigs)** 목록에 추가해야 합니다.

- 끌어다 놓기를 사용하여 개체의 순서가 올바른지 확인합니다.

사용자 지정 특성 개체를 생성하는 개체는 그룹 정책에 해당 특성을 할당하는 개체 앞에 있어야 합니다. 그렇지 않으면 아직 존재하지 않는 사용자 지정 특성을 추가하려고 하면 오류가 발생합니다.

사용자 지정 그룹 정책을 구성하는 단일 개체가 있는 경우 목록은 다음과 같이 표시됩니다.

Selected Append FlexConfigs	
#.	Name
1..	Per_App_Allow_All_Policy
2..	Add_Per_App_VPN

- e) **Save(저장)**를 클릭합니다.
- f) 아직 모든 대상 디바이스를 정책에 할당하지 않았다면 **Save(저장)** 아래에 있는 **Policy Assignments(정책 할당)** 링크를 클릭하여 할당합니다.
- g) **Preview Config(구성 미리보기)**를 클릭하고, **Preview(미리보기)** 대화 상자에서 할당된 디바이스 중 하나를 선택합니다.

시스템은 디바이스에 전송될 구성 CLI의 미리보기를 생성합니다. 개체에서 생성된 명령이 올바르게 표시되는지 확인합니다. 미리보기 끝부분에 표시됩니다. 관리 대상 기능에 적용한 다른 변경 사항에서 생성된 명령도 함께 표시됩니다. 이러한 명령의 경우 다음과 유사한 내용이 표시됩니다.

```

###Flex-config Appended CLI ###
webvpn

anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
anyconnect-custom-data perapp perAppPolicy eJyVkfTvgkAQhf8K2adWqBcUNb4hGt
anyconnect-custom-data perapp perAppPolicy pPWyd+j/NM1W2rkLrbiyEXFJ6thJ+s
group-policy sales attributes
anyconnect-custom perapp value perAppPolicy

```

단계 6 변경 사항을 배포합니다.

단계 7 구성을 확인합니다.

- 각 FTD 디바이스에서 명령이 설정되었는지 확인할 수 있습니다. 디바이스에 대한 SSH 세션 또는 FMC의 CLI 툴을 사용합니다(**System(시스템) > Health(상태) > Monitor(모니터)**를 선택한 후 디바이스를 클릭한 다음 **Advanced Troubleshooting(고급 문제 해결)**을 클릭하고 **Threat Defense CLI** 탭 선택). 다음은 설정을 표시하는 명령입니다.
 - **show running-config webvpn**
 - **show running-config anyconnect-custom-data**
 - **show running-config group-policy name**, 여기서 *name*은 sales와 같은 그룹 정책 이름으로 교체됩니다.
- AnyConnect 클라이언트에서 시스템이 올바르게 작동하는지 확인할 수 있습니다. 클라이언트 통계를 열고 다음 항목을 찾습니다.
 - **Tunnel Mode(터널 모드)**는 "Tunnel All Traffic(모든 트래픽 터널링)"이 아닌 "Application Tunnel(애플리케이션 터널)"로 표시되어야 합니다.



VPN Statistics	
CONNECTION INFORMATION	
Time Connected	00:00:53
Status	Connected
Tunneling Mode	Application Tunnel
Tunneling Mode (IPv6)	Application Tunnel

- **Tunneled Apps**(터널링된 앱)에는 MDM에서 터널링을 위해 활성화한 애플리케이션이 나열됩니다.



TUNNELED APPS	
	Teams (com.cisco.wx2.android)
	Cisco Jabber (com.cisco.im)
	Mobile Setup (com.cisco.it.estimate.android.setup)
	Network Setup Assistant (com.cisco.cpm.spw.android.wifisupplicant)
	Outlook (com.microsoft.office.outlook)

다음에 수행할 작업

Per App VPN을 더 이상 사용하지 않으려면 FlexConfig 개체를 생성하여 FTD 디바이스에서 설정을 제거해야 합니다. 또한 MDM을 제거해야 합니다. 지침은 MDM 설명서를 참조하십시오.

FTD 헤드엔드의 경우 사용자 지정 특성을 사용하는 각 그룹 정책에서 사용자 지정 특성을 제거하는 데 필요한 명령이 포함된 `deploy-once/append` FlexConfig 개체를 생성한 다음 해당 특성을 삭제합니다. 예를 들어 두 그룹 정책(DfltGrpPolicy 및 sales)에서 사용자 지정 특성을 사용하고 이 특성의 이름이 perAppPolicy인 경우 명령은 다음과 같습니다.

```
group-policy DfltGrpPolicy attributes
  no anyconnect-custom perapp

group-policy sales attributes
  no anyconnect-custom perapp

no anyconnect-custom-data perapp perAppPolicy

webvpn
  no anyconnect-custom-attr perapp
```

그런 다음 FlexConfig 정책에서 특성을 생성 및 할당하는 개체를 제거하고 이 새 개체를 추가합니다. 설정을 구축하면 앱별 기능이 그룹 정책에서 제거됩니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.