FMC 도메인 구성(&N);사용자 액세스 및 역할

문제

이 문서에서는 전역 및 하위 도메인 전체에서 FMC의 여러 사용자에 대해 서로 다른 사용자 권한을 구성하는 방법에 대해 설명합니다.

환경

- Cisco FMC(Secure Firewall Management Center) - 7.6.4(모든 FMC에 적용 가능)
- 전역 도메인 및 하위 도메인을 사용하는 다중 도메인 구축
- 여러 FTD 디바이스가 서로 다른 하위 도메인에 할당됨
- 여러 사용자에게 서로 다른 권한 수준이 필요함

해결

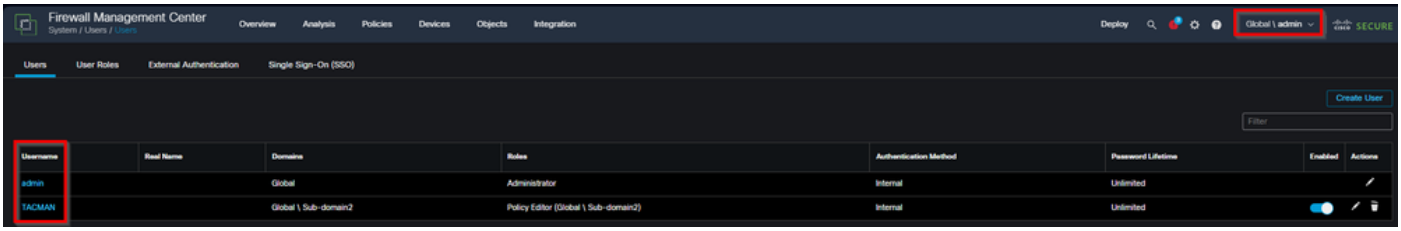
이 문서에서는 도메인 간 액세스를 제한하고 특정 사용자에 대한 전역 도메인 액세스를 제한하는 기능을 사용하여 FMC의 여러 사용자에 대해 서로 다른 사용자 권한을 구성하는 방법을 설명합니다. Cisco FMC는 도메인 간 액세스를 제한하는 기능을 사용하여 여러 도메인에 대한 세분화된 사용자 역할 할당을 지원합니다. 구성에는 특정 도메인의 사용자를 생성하고 액세스 레벨을 제어하기 위한 적절한 역할을 할당하는 작업이 포함됩니다.

사용자 및 도메인 액세스 동작 생성

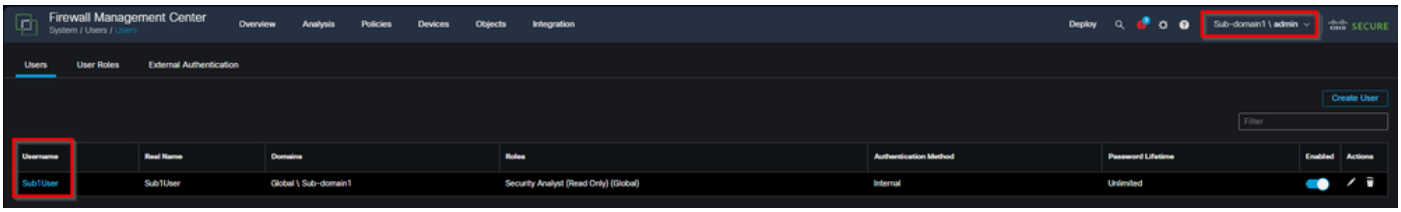
FMC 사용자 관리 시스템은 사용자가 생성되는 위치에 따라 다르게 작동합니다.

하위 도메인에서 생성된 사용자

- 하위 도메인에서 직접 생성된 사용자는 특정 도메인 내에서만 볼 수 있습니다.

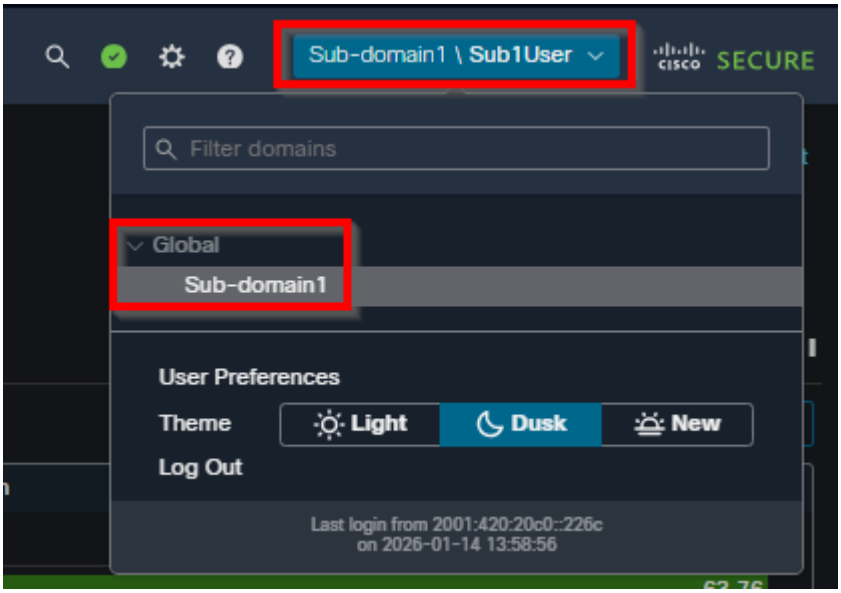


inline_image_0.png



인라인 이미지_1.png

- 이러한 사용자는 도메인 사양 형식(subdomain\username)을 사용하여 로그인해야 합니다.
- 사용자가 생성된 도메인으로 액세스가 자동으로 제한됩니다.

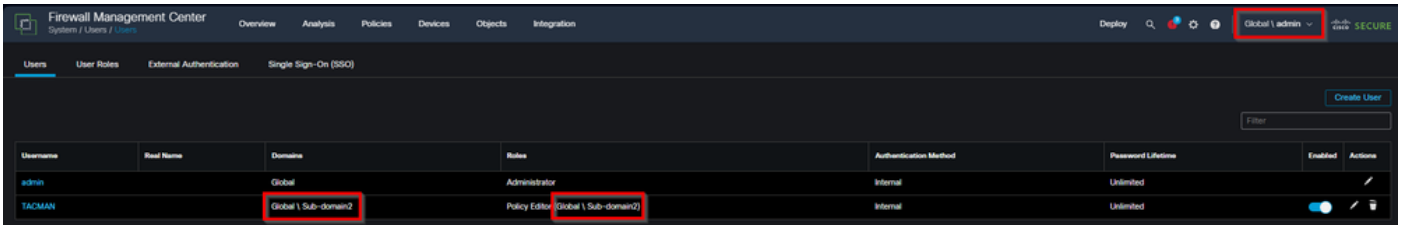


inline_image_2.png

- 하위 도메인에서 생성된 사용자 지정 역할은 해당 도메인에만 적용됩니다.

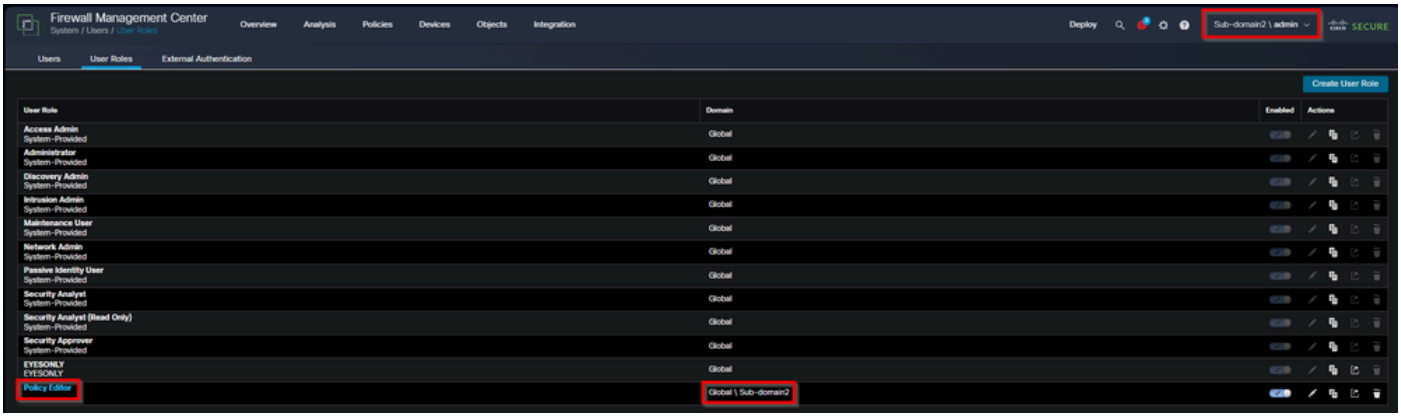
전역 도메인에서 생성된 사용자:

- 전역 도메인에서 생성된 사용자는 자신의 역할이 하위 도메인에만 있더라도 사용자 이름만 사용하여 로그인할 수 있습니다.
- 이러한 사용자는 전역 도메인 사용자 목록에 계속 표시됩니다.



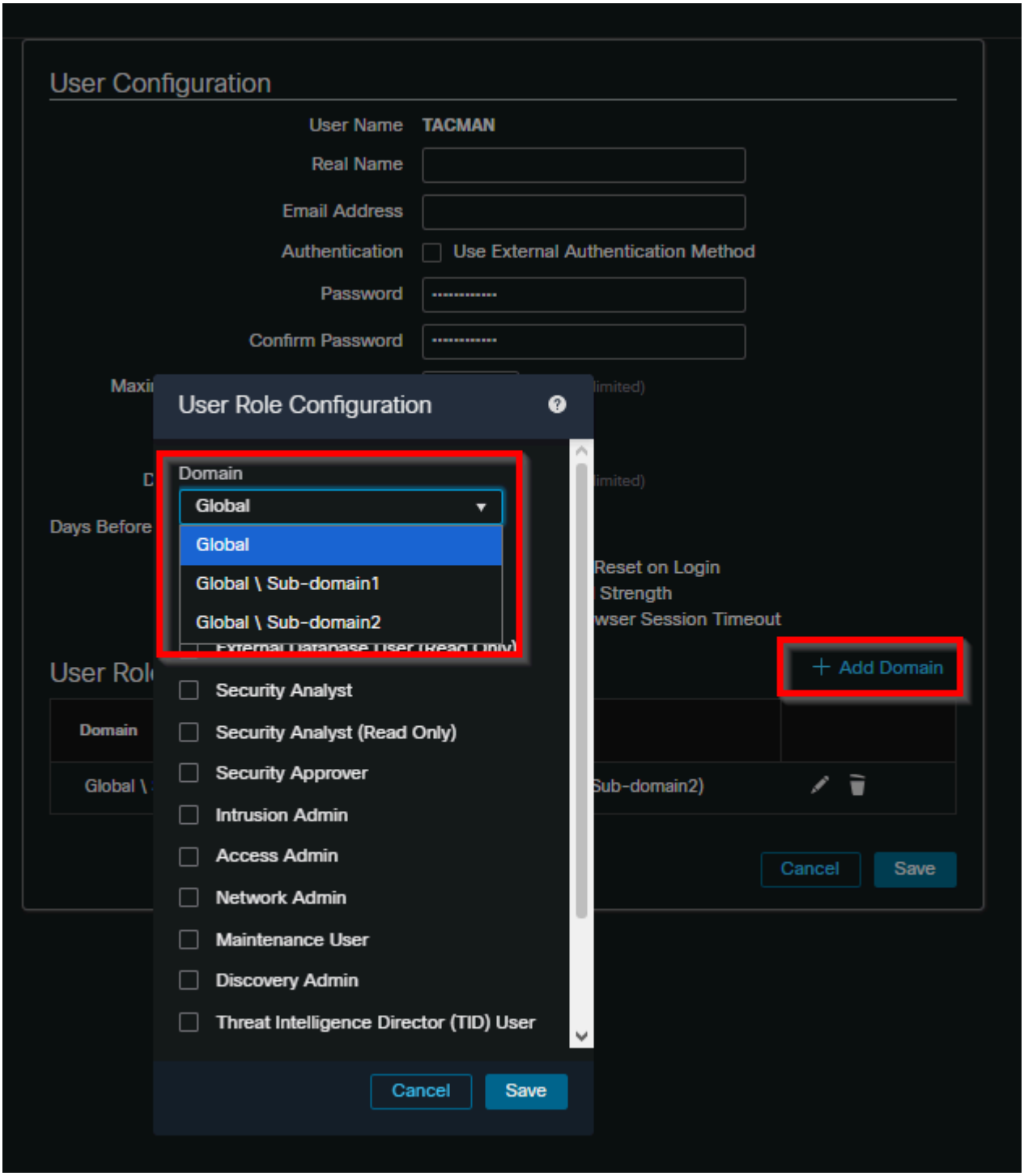
inline_image_3.png

- 모든 하위 도메인에 대해 역할을 할당할 수 있습니다.



inline_image_4.png

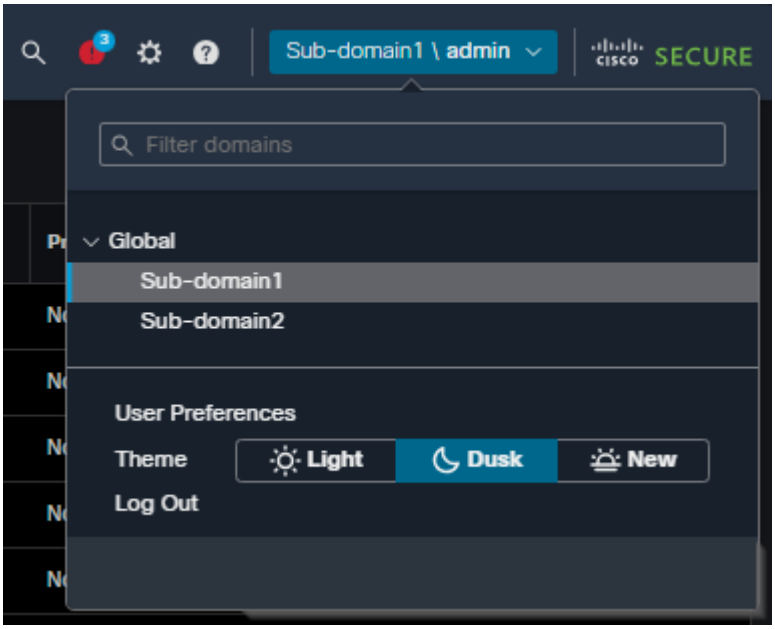
- 역할 할당을 통해 특정 하위 도메인으로 액세스를 제한할 수 있습니다.



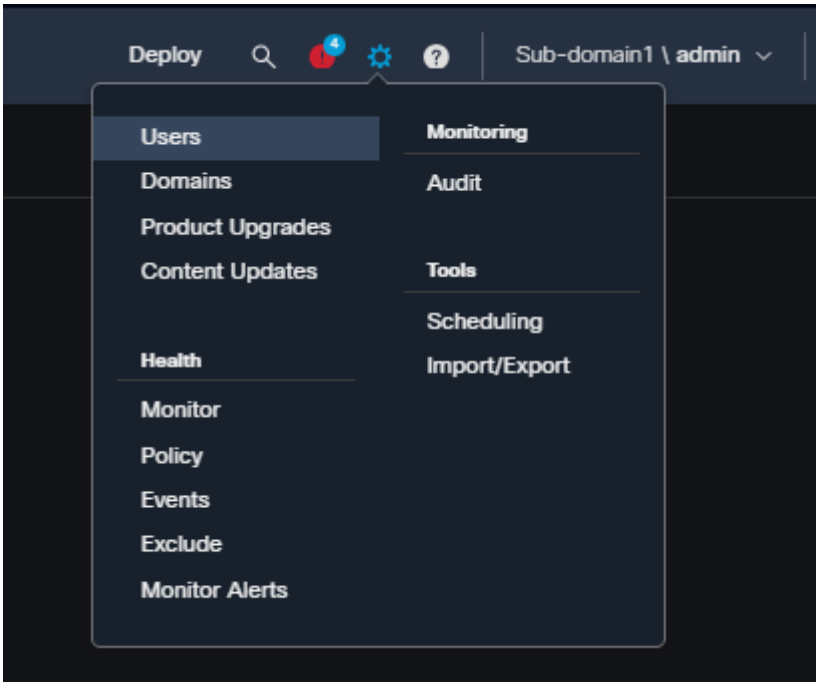
inline_image_5.png

하위 도메인 사용자 제한에 대한 구성 단계

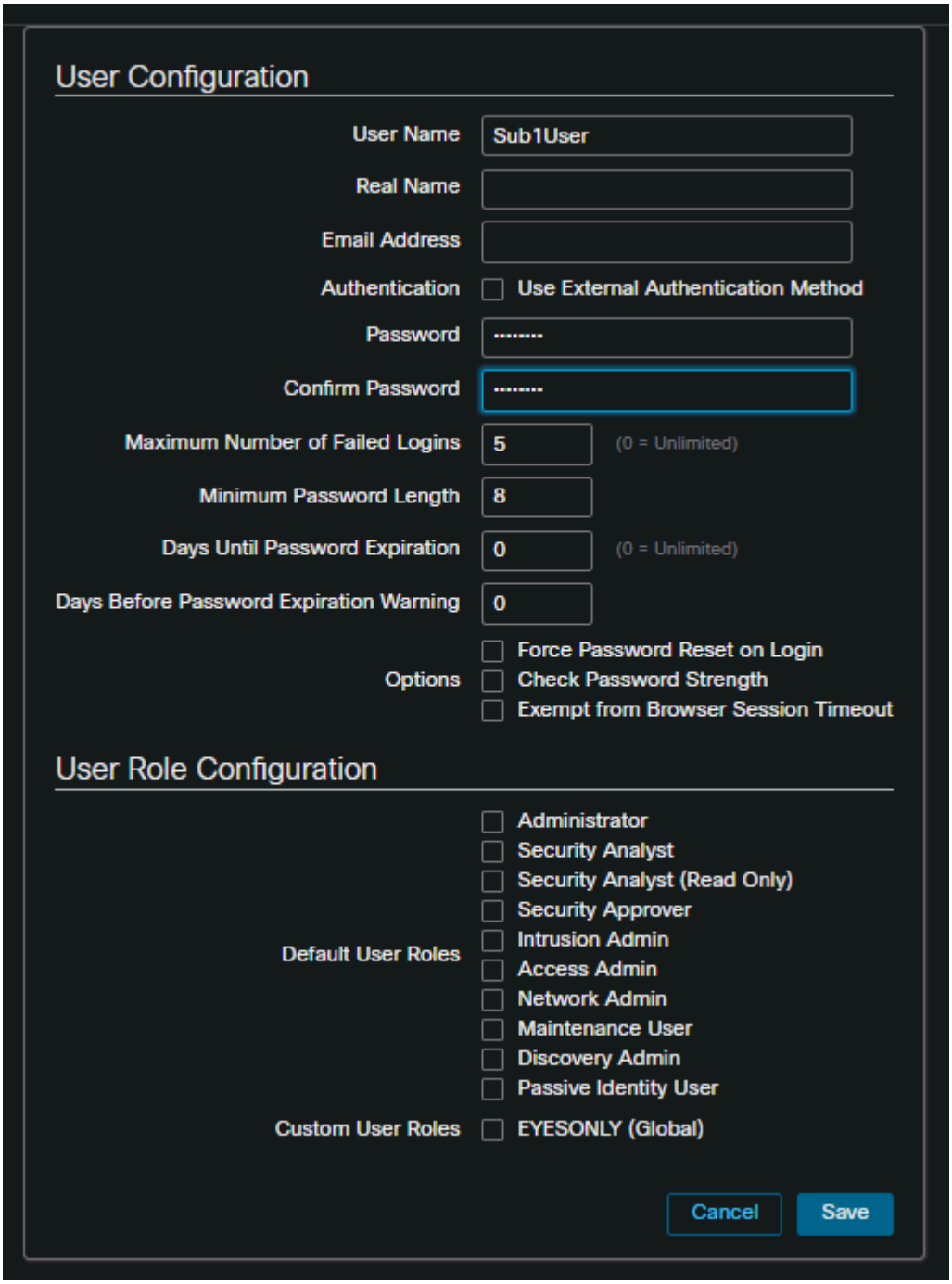
- 액세스를 제한해야 하는 특정 하위 도메인으로 이동하여 System/Users(시스템/사용자) 아래에 사용자 계정을 생성합니다.



inline_image_6.png

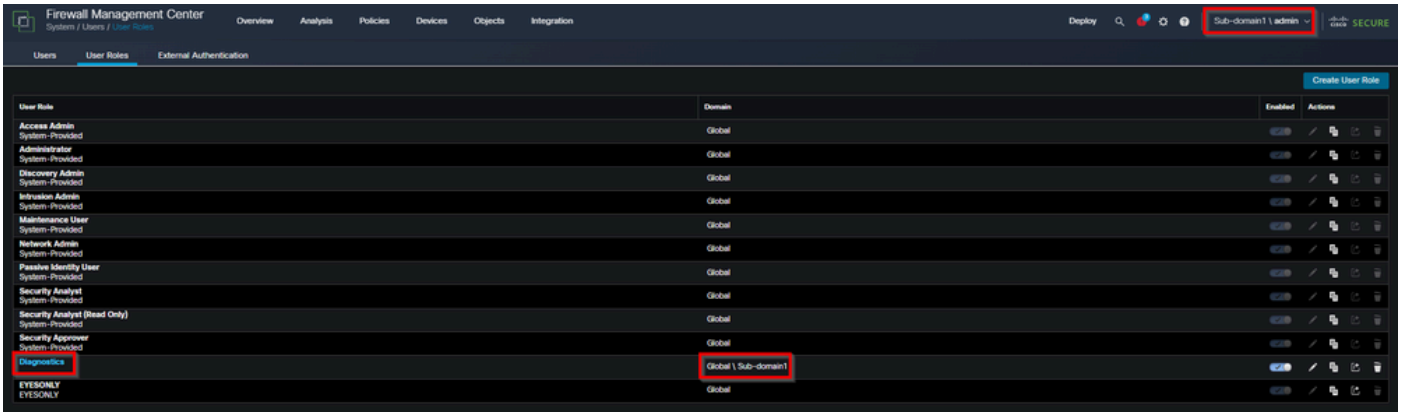


inline_image_7.png



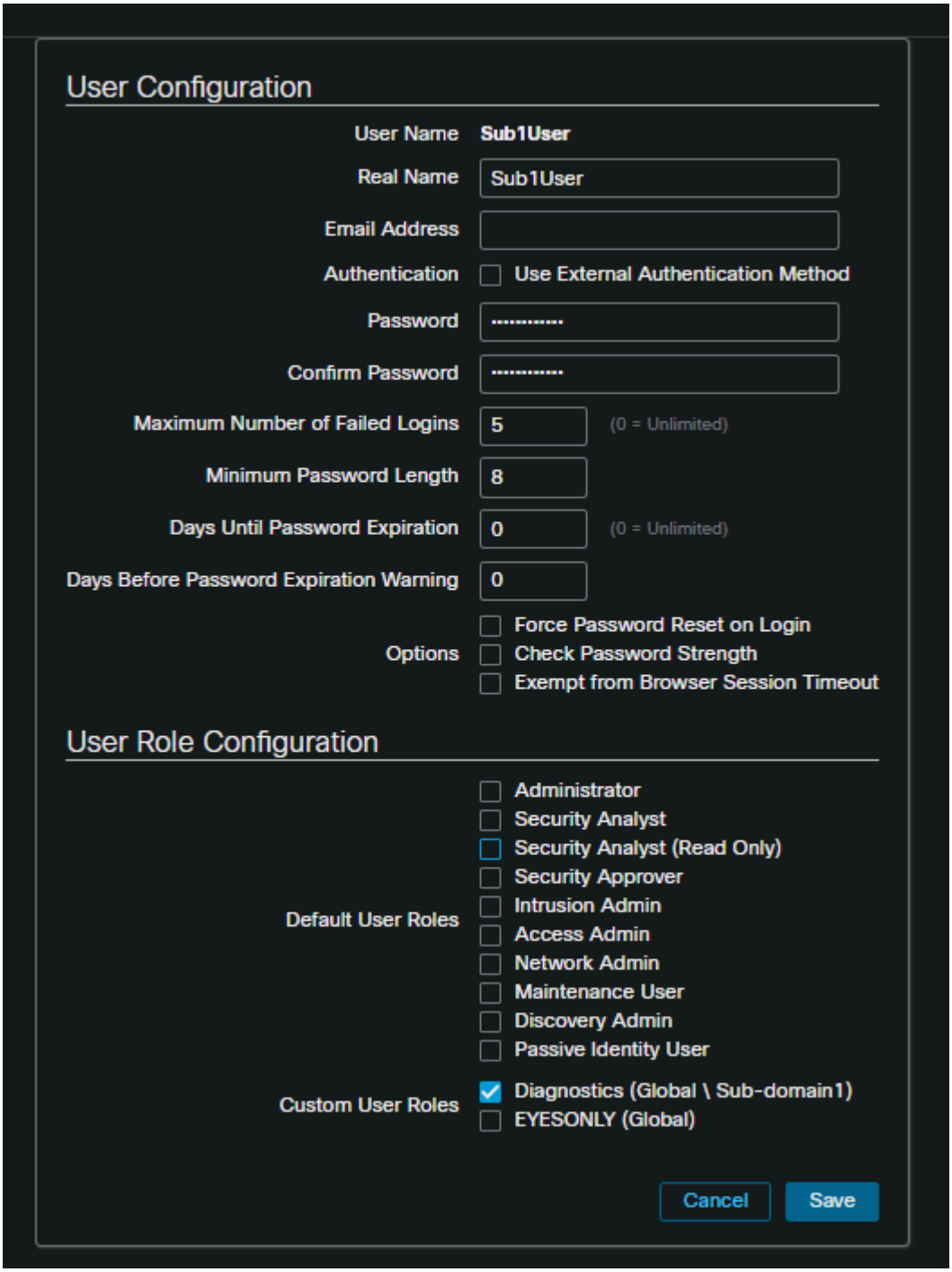
inline_image_8.png

- 시스템/사용자 역할의 하위 도메인 내에 사용자 지정 역할을 만듭니다. 하위 도메인에서 생성된 사용자 지정 사용자 역할은 해당 도메인 내에서만 사용할 수 있으며 다른 도메인에서 액세스할 수 없습니다.



inline_image_9.png

- 사용자에게 사용자 지정 역할을 할당합니다. 사용자는 사용자와 역할이 모두 만들어진 도메인에 대해서만 권한을 상속합니다.



inline_image_10.png

- 하위 도메인 사용자의 사용자 로그인 형식입니다. 하위 도메인에서 생성된 사용자는 다음 로그인 형식을 사용해야 합니다.

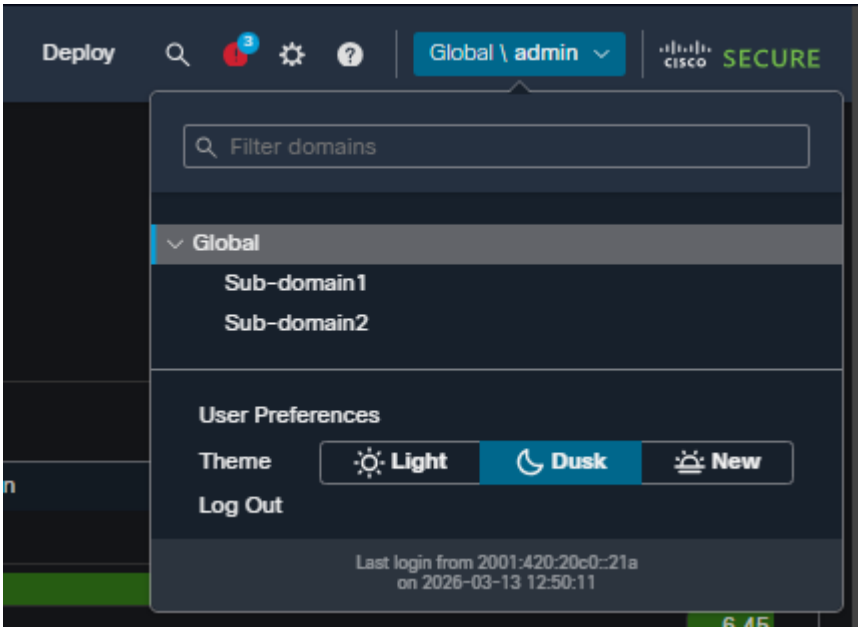
사용자 이름: `Sub-domain\username`

암호: [사용자 암호]

inline_image_11.png

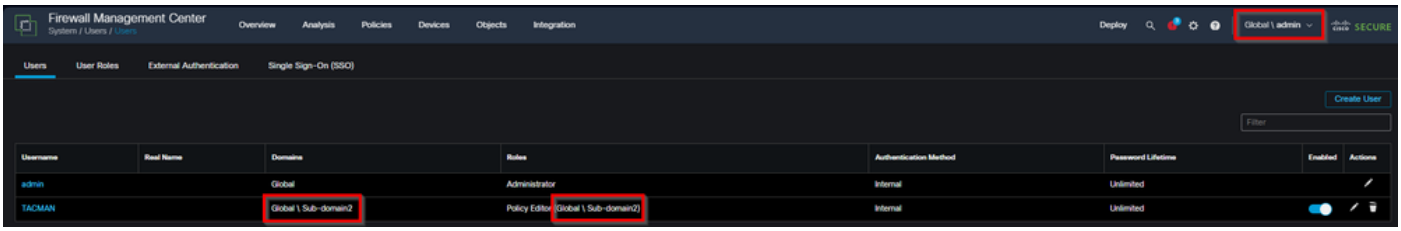
하위 도메인 제한이 있는 전역 도메인 사용자를 위한 구성 단계

- 시스템/사용자 아래의 전역 도메인에서 사용자를 만듭니다. 전역 도메인 액세스 권한이 있는 관리 계정을 사용하여 사용자를 만드십시오.

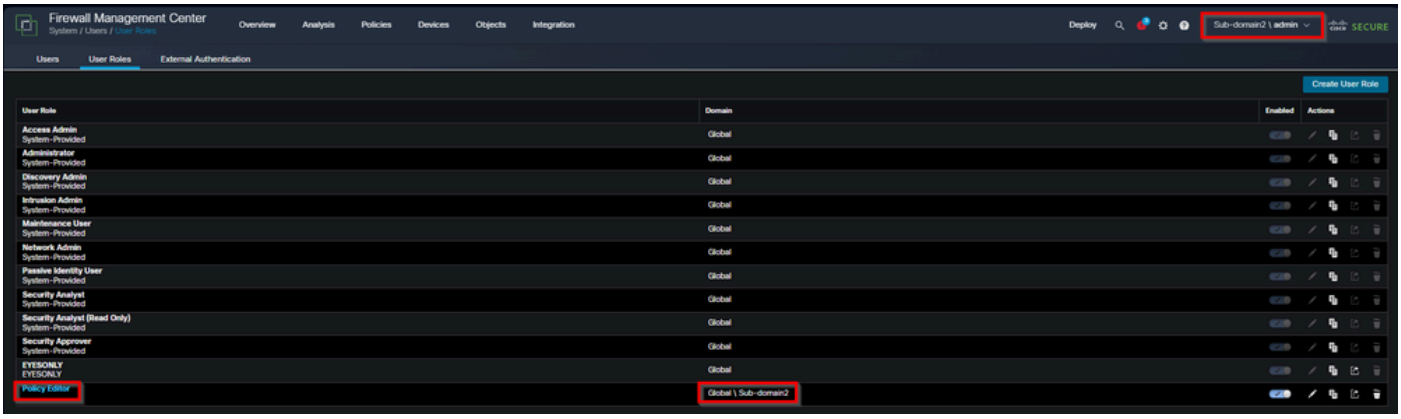


inline_image_12.png

- 시스템/사용자 아래의 특정 하위 도메인에 대해서만 역할을 할당합니다. 사용자 구성에서 전역 도메인 권한을 제공하지 않고 대상 하위 도메인에 대해서만 역할을 할당합니다.



inline_image_3.png



inline_image_14.png

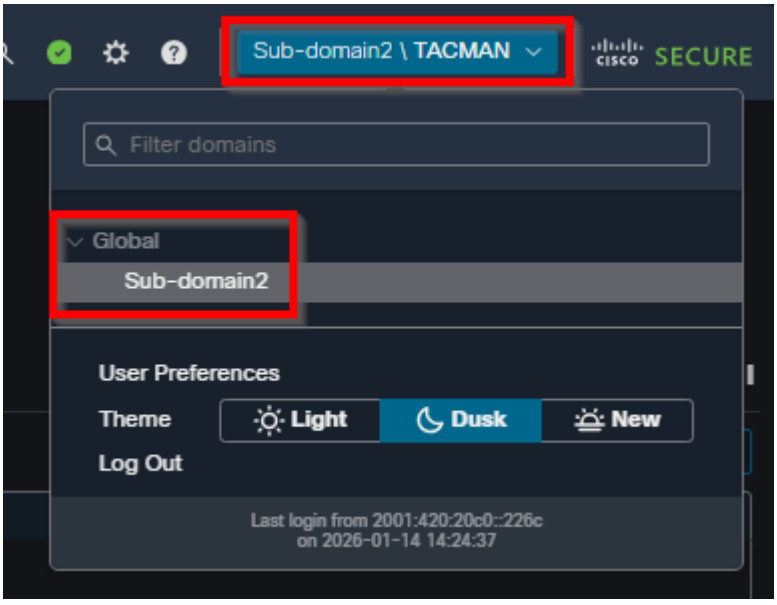
- 이러한 사용자는 도메인 지정 없이 사용자 이름으로만 로그인할 수 있습니다.

사용자 이름: 사용자 이름

암호: [사용자 암호]

inline_image_15.png

- 사용자는 역할이 특별히 할당된 하위 도메인에만 액세스할 수 있으며 전역 도메인 또는 다른 하위 도메인에는 액세스할 수 없습니다.



inline_image_16.png

역할 할당 유연성

사용자는 각 도메인에서 서로 다른 권한을 가질 수 있습니다.

- 하위 도메인 관리자 권한이 있는 전역 도메인의 읽기 전용 권한
- 특정 하위 도메인에서 전체 관리자 권한이 있는 글로벌 도메인 액세스 없음
- 다른 하위 도메인에 대한 액세스 없이 한 하위 도메인의 정책 편집기 권한

외부 사용자 고려 사항

외부 사용자(LDAP 또는 RADIUS 인증):

- 사용자 역할이 그룹 멤버십 또는 사용자 특성을 통해 할당된 경우 최소 액세스 권한을 제거할 수 없습니다.
- 추가 권한은 기본 사용자 역할보다 더 큰 범위를 할당할 수 있습니다.
- 외부 인증 객체는 해당 객체가 생성된 도메인에서만 사용할 수 있습니다.
- 적절한 제한을 위해서는 개별 사용자 권한이 기본 사용자 역할보다 더 큰 범위에서 구성되어야 합니다.

제한 사항 및 고려 사항

- 상위 도메인에서 만든 사용자 지정 사용자 역할은 하위 도메인에서 편집할 수 없습니다.
- 셸 인증은 하위 도메인이 아닌 전역 도메인에서만 사용할 수 있습니다.
- 사용자 환경 설정 및 대시보드 설정은 계정이 액세스할 수 있는 모든 도메인에 적용됩니다.
- 사용자에 대한 권한 수정은 그룹 또는 대량 방법이 아니라 개별적으로 구성됩니다.

원인

보안 경계를 유지하기 위해 도메인 간에 특정 제한 사항을 적용하면서 사용자가 전역 및 하위 도메인에 대한 다양한 액세스 레벨을 필요로 하는 다중 도메인 FMC 구축에서 세분화된 액세스 제어를 구현해야 하기 때문입니다.

관련 콘텐츠

- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 사용자
- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 사용자 지정 사용자 역할 생성
- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 내부 사용자 추가 또는 편집
- Cisco Secure Firewall Management Center 관리 가이드, 7.6: 사용자 및 도메인
- Cisco 기술 지원 및 다운로드

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.