Tenable Identity Exposure 3.x 사용자 및 관리자 가이드

마지막 수정: 2024년 4월 5일

목차

Tenable Identity Exposure 시작 **8**

Tenable Identity Exposure 탐색 10

Tenable Identity Exposure에 로그인 14

작업 영역에 액세스 19

사용자 기본 설정 22

알림 25

대시보드 27

위젯 29

Identity Explorer 33

Trail Flow 35

Trail Flow 표 37

마법사를 사용하여 Trail Flow 검색 39

Trail Flow를 수동으로 검색 41

Trail Flow 쿼리 사용자 지정 43

책갈피 쿼리 47

쿼리 기록 50

일탈 이벤트 표시 52

이벤트 세부 정보 54

특성 변경 사항 58

Trail Flow 사용 사례 61

위험 노출 지표 65

위험 노출 지표 세부 정보 68

일탈 개체 71

일탈 개체 검색 74
일탈 개체 무시 78
원인으로 지목된 특성 80
RSoP 기반 위험 노출 지표 82
Microsoft Entra ID 관련 위험 노출 지표 83
위험 노출 지표의 일탈 수정 84
AdminCount 특성을 일반 사용자에 설정 85
위험한 Kerberos 위임 88
SDProp 일관성 보장 94
공격 지표 98
공격 지표 세부 정보 101
공격 지표 인시던트 103
토폴로지 109
트러스트 관계 111
위험한 트러스트 114
공격 경로 116
공격 관계 121
키 자격 증명 추가 123
멤버 추가 125
작업 허용 127
위임 허용 130
GPO에 속함 133
DCSync 135
작업 허용 권한 부여 138

SID 기록 있음 140
암시적 인수 143
GPO 상속 145
연결된 GPO 147
멤버 관계 149
소유 151
비밀번호 초기화 153
RODC 관리 155
DACL 쓰기 158
쓰기 소유자 160
계층 0 자산 식별 162
공격 경로가 있는 계정 164
공격 경로 노드 유형 166
활동 로그 169
Tenable Identity Exposure 관리자 가이드 171
Active Directory 구성 173
AD 개체 또는 컨테이너에 대한 액세스 174
권한 있는 분석에 대한 액세스 176
Secure Relay 183
네트워크 흐름 184
TLS 요구 사항 185
시작하기 전에 188
허용된 파일 및 프로세스 190
연결 키 192

설치 193
제거 194
자동 업데이트 195
참고 항목 196
Secure Relay 설치(GUI) 197
Secure Relay(Tenable Nessus Agent) 설치 202
설치 후 확인 205
Relay 구성 207
공격 지표 배포 209
공격 지표 설치 213
공격 지표 설치 스크립트 221
기술 변경 사항 및 잠재적 영향 229
공격 시나리오(< v. 3.36) 231
Microsoft Sysmon 설치 236
공격 지표 제거 241
공격 지표 문제 해결 242
바이러스 백신 탐지 243
고급 감사 정책 구성 우선 순위 245
이벤트 로그 수신기 유효성 검사 247
Tenable Identity Exposure 로그 파일 249
DFS 복제 문제 완화 256
인증 258
Tenable One을 사용한 인증 259
Tenable Identity Exposure 계정을 사용한 인증 260

LDAP를 사용하여 인증 264
SAML을 사용한 인증 267
사용자 계정 270
사용자 만들기 271
사용자 편집 273
사용자 비활성화 274
사용자 삭제 275
보안 프로필 276
지표 사용자 지정 278
지표의 사용자 지정 미세 조정 280
사용자 역할 282
역할 관리 283
역할에 대한 권한 설정 284
사용자 인터페이스 엔터티에 대한 권한 설정(예) 289
포리스트 292
포리스트 관리 293
서비스 계정 보호 294
도메인 296
도메인에서 데이터 강제로 새로 고침 300
허니팟 계정 301
Kerberos 인증 304
알림 312
SMTP 서버 구성 313
이메일 알림 315

Syslog 알림 319
Syslog 및 이메일 알림 세부 정보 323
상태 검사 328
보고 센터 334
Microsoft Entra ID 지원 337
Tenable Cloud 데이터 수집 346
권한 있는 분석 347
활동 로그 348
Tenable Identity Exposure 공개 API 351
데이터 관리 353
배포 리전 354
Tenable Identity Exposure 라이선싱 356
라이선스 관리 359
Tenable Identity Exposure 문제 해결 363
Tenable Identity Exposure 진단 도구 364
Tenable Identity Exposure와 SYSVOL 강화 간섭 366

Tenable Identity Exposure 시작

마지막 업데이트: 2024-04-30

Tenable Identity Exposure(이전의 Tenable.ad)를 사용하면 위협을 예상하고 침해를 탐지하며 인시던트와 공격에 대응하여 인프라의 보안을 확보할 수 있습니다. 직관적인 대시보드를 사용해 실시간으로 Active Directory를 모니터링하므로, 한눈에 가장 중대한 취약성을 파악하고 그에 대한 권장 수정 과정을 알아볼 수 있습니다. Tenable Identity Exposure의 공격 지표와 위험 노출 지표를 사용하면 Active Directory에 영향을 미치는 기본적인 문제점을 탐색하고 위험한 트러스트 관계를 식별하며 공격의 심층적인 세부 정보를 분석할 수 있습니다.

> 공격 지표와 위험 노출 지표 기능은 구매한 라이선스의 종류에 따라 이용할 수 있습니다.

시작하려면 Tenable Identity Exposure 시작하기를 참조하십시오.

> **참고:** Tenable Identity Exposure을(를) 단독으로 구입하거나 Tenable One 패키지의 일부분으로 구입할 수 있습니다. 자세한 내용은 Tenable One을 참조하십시오.

> **팁:** *Tenable Identity Exposure 사용자 가이드*는 영어, 일본어, 독일어, 한국어, 중국어 간체 및 중국어 번체로 제공됩니다. *Tenable Identity Exposure* 사용자 인터페이스는 영어, 일본어, 독일어, 프랑스어, 한국어, 중국어 간체 및 중국어 번체로 제공됩니다. 사용자 인터페이스 언어를 변경하려면 사용자 기본 설정을 참조하십시오.

Tenable Identity Exposure에 관한 자세한 정보는 다음 고객 교육 자료를 참조하십시오.

- Tenable Identity Exposure 자체 도움말 가이드
- Tenable Identity Exposure 개요(Tenable University)

Tenable One 위험 노출 관리 플랫폼

Tenable One은 조직이 최신 공격 표면에 대한 가시성을 확보하고 가능한 공격을 방지하기 위한 노력을 집중하며 최적의 비즈니스 성과를 지원하기 위해 사이버 위험을 정확하게 커뮤니케이션할 수 있도록 지원하는 위험 노출 관리 플랫폼입니다.

이 플랫폼은 IT 자산, 클라우드 리소스, 컨테이너, 웹 앱 및 ID 시스템을 아우르는 가장 폭넓은 취약성 범위를 결합하고 Tenable Research에서 제공하는 취약성 범위의 속도와 폭을 기반으로 종합적인 분석을 더해 작업의 우선 순위를 지정하고 사이버 위험을 커뮤니케이션합니다. Tenable One은 조직에 다음과 같은 이점을 제공합니다.

- 최신 공격 표면 전체에 걸친 종합적 가시성 확보
- 위협을 예측하고 공격을 방지하기 위한 노력의 우선 순위를 지정
- 더 나은 결정을 내리기 위해 사이버 위험을 커뮤니케이션

Tenable Identity Exposure을(를) 독립 실행형 제품으로 사용하거나 Tenable One 위험 노출 관리 플랫폼의 일부분으로 구입할 수 있습니다.

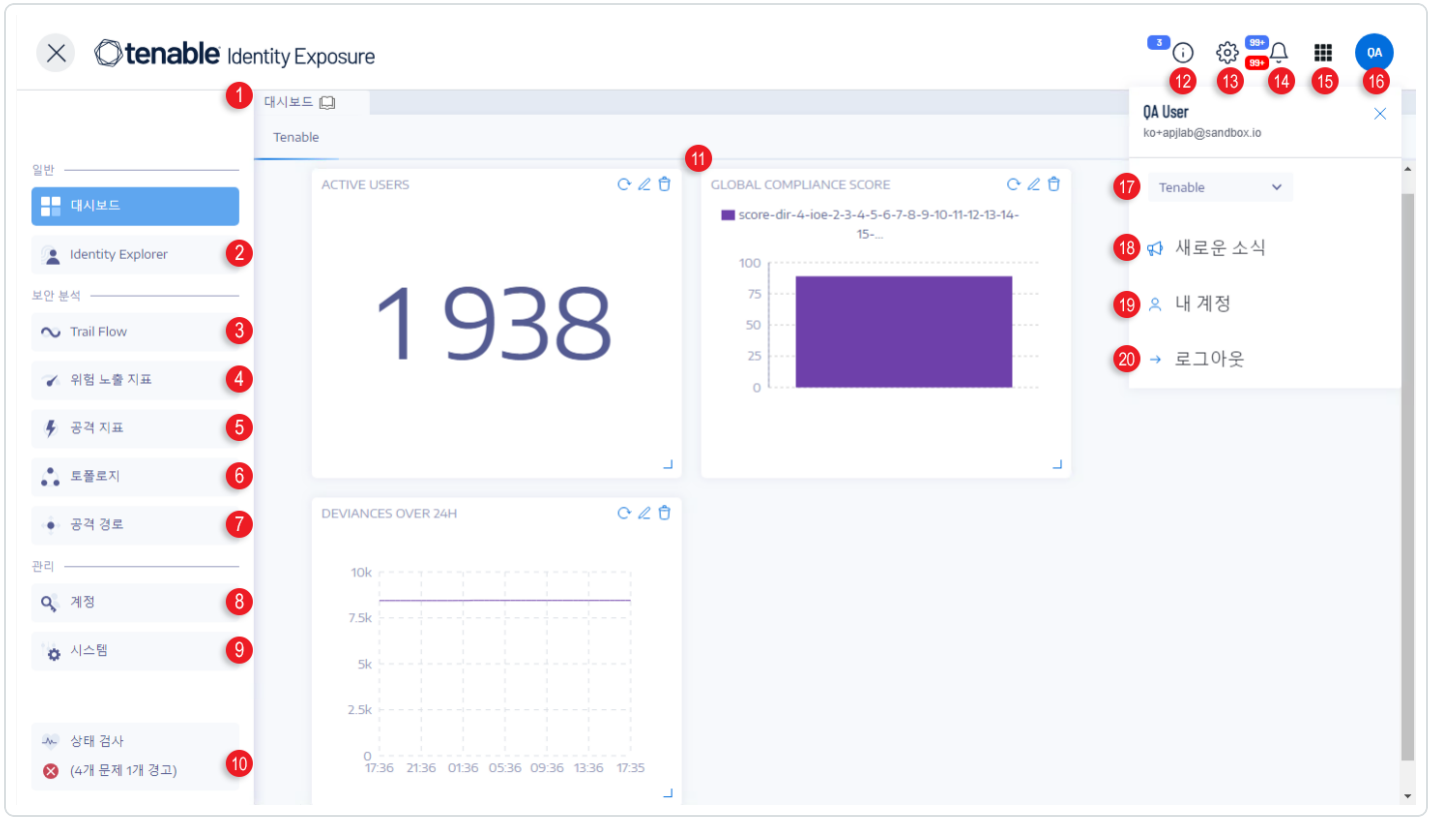
> **팁:** Tenable One 제품을 시작하는 방법에 관한 자세한 정보는 Tenable One 배포 가이드를 참조하십시오.

Tenable Identity Exposure 탐색

Tenable Identity Exposure에 로그인한 후에 이 예시에서 볼 수 있는 것처럼 홈페이지가 열립니다.

사이드바 탐색 모음을 펼치거나 접는 방법:

- 펼치기: 창 왼쪽 상단에 있는 ☰ 메뉴를 클릭합니다.
- 접기: 창 왼쪽 상단에 있는 **X**를 클릭합니다.



#	정의	용도
1	대시보드	대시보드를 사용하면 Active Directory 인프라의 보안을 효율적이고도 시각적인 방식으로 관리하고 모니터링할 수 있습니다.
2	Identity Explorer	Tenable Identity Exposure의 Identity Explorer 보기는 Active Directory와 Microsoft Entra ID 전체의 ID를 통합

		합니다. 이 보기에는 나열된 각 자산의 ID 위험 점수(베타)와 침해된 ID의 잠재적 범위가 표시됩니다.
3	Trail Flow	Trail Flow에 Active Directory에 영향을 미치는 이벤트의 실시간 모니터링 및 분석이 표시됩니다.
4	위험 노출 지표	Tenable Identity Exposure는 위험 노출 지표(IoE)를 사용하여 Active Directory의 보안 성숙도를 측정하고 모니터링 및 분석 대상인 이벤트 흐름에 심각도 수준(위험, 높음, 중간 또는 낮음)을 할당합니다.
5	공격 지표	Tenable Identity Exposure는 공격 지표를 통해 공격을 실시간으로 탐지할 수 있습니다.
6	Topology	토폴로지 페이지에서는 Active Directory에 대한 대화형 그래프 시각화를 제공합니다. 여기에는 포리스트 및 도메인과 그 사이에 존재하는 트러스트 관계가 표시됩니다.
7	공격 경로	공격 경로 페이지에는 Active Directory 관계가 그래픽으로 표시됩니다. • Blast Radius: 침해되었을 가능성이 있는 자산으로부터 AD 내 내부 확산 이동 정도를 평가합니다. • Attack Path: 특정 진입 지점에서 자산에 도달하기 위한 권한 상승 기술을 예상합니다.

		• 자산 노출: 자산 노출 시각화를 사용하여 자산의 취약성을 측정하고 모든 상승 경로를 차단합니다.
8, 9	관리 **필수 사용자 역할**: 적절한 권한이 있는 조직 사용자.	이 섹션을 사용하여 다음과 같은 항목을 구성할 수 있습니다. • 계정: 사용자 계정, 역할 및 보안 프로필. • 시스템: 포리스트 및 도메인, 애플리케이션 서비스, 알림 및 인증. 자세한 내용은 Tenable Identity Exposure 관리자 가이드를 참조하십시오.
10	상태 검사	상태 검사를 사용하면 도메인과 서비스 계정의 구성을 실시간으로 하나의 통합된 보기에서 파악할 수 있으며 여기에서 드릴다운하여 더 자세한 정보를 알아볼 수 있습니다.
11	위젯	위젯은 대시보드에서 사용자 지정 가능한 데이터 세트입니다. 여기에는 막대형 차트, 꺾은선형 차트 및 카운터 등이 포함될 수 있습니다.
12	제품 업데이트	최신 제품 기능에 관한 정보입니다.
13	설정	시스템 구성, 포리스트 및 도메인 관리, 라이선스, 사용자 및 역할 관리, 프로필, 활동 로그에 대한 액세스합니다.
14	알림(벨)	벨 아이콘과 배지 수를 보면 사용자의 확인을 대기 중인 공격 알림 및/또는

		노출 알림 수를 알 수 있습니다.
15	애플리케이션 전환기	Tenable 작업 영역에서 애플리케이션 간에 전환하려면 이 아이콘을 클릭합니다.
16, 19	사용자 프로필 아이콘(사용자 기본 설정)	이 아이콘을 클릭하여 보안 프로필, 릴리스 정보, 활동 로그, 기본 설정의 하위 메뉴에 액세스하거나 로그아웃합니다.
17	보안 프로필	보안 프로필을 사용하면 다양한 유형의 사용자가 다양한 보고 관점에서 보안 분석을 검토할 수 있습니다.
18	새로운 소식	클릭하여 Tenable Identity Exposure의 최신 버전에 대한 릴리스 정보를 확인합니다.
20	로그아웃	클릭하여 Tenable Identity Exposure에서 로그아웃합니다.

Tenable Identity Exposure에 로그인

클라이언트 URL을 통해 Tenable Identity Exposure의 웹 애플리케이션에 액세스합니다.

Tenable Identity Exposure에 로그인하려면 다음 옵션 중 하나를 선택합니다.

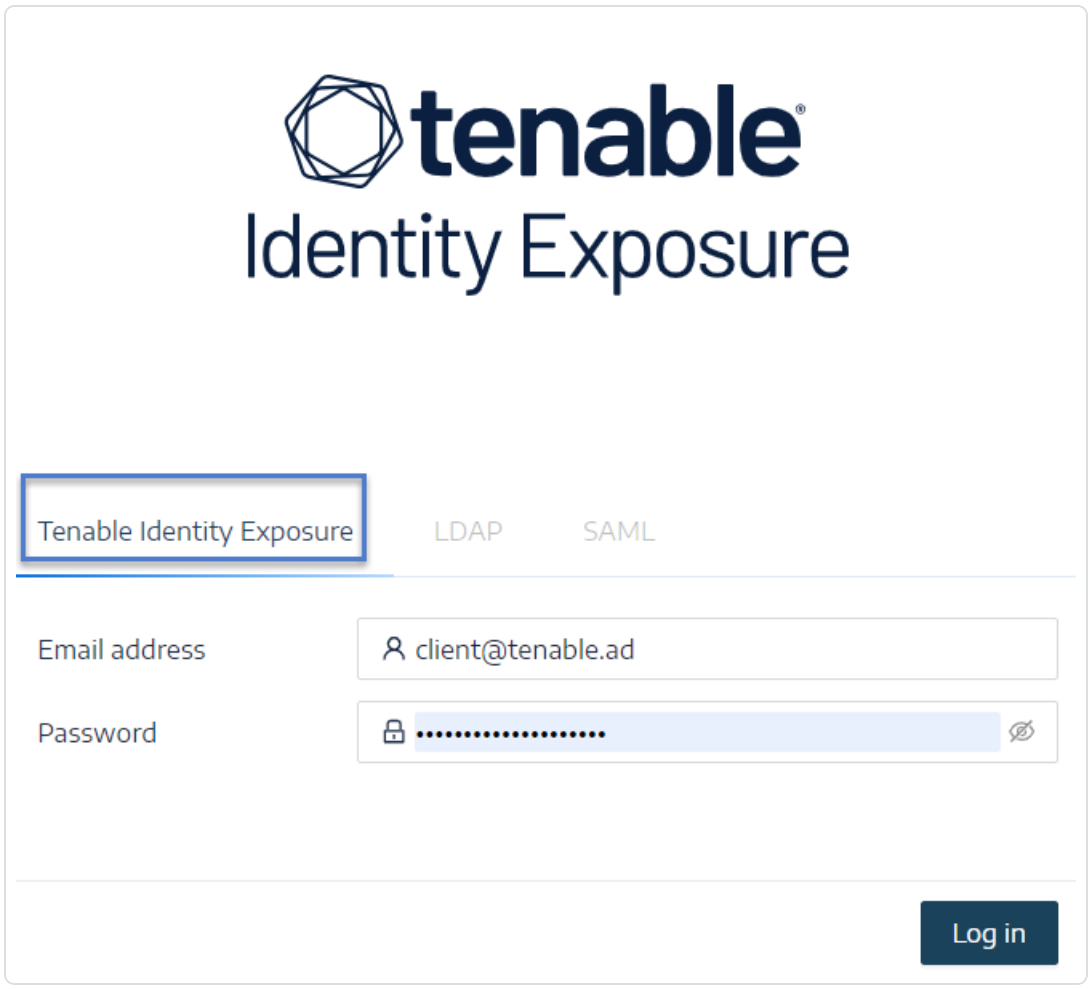
- ◦ Tenable Identity Exposure 계정 사용
  ◦ LDAP 계정 사용
  ◦ SAML 사용

Tenable Identity Exposure 계정 사용

Tenable Identity Exposure 계정을 사용하여 로그인하는 방법:

1. 브라우저에서 주소 표시줄에 클라이언트 URL(예: client.tenable.ad)을 입력합니다.

   로그인 창이 표시됩니다.



2. **Tenable Identity Exposure** 탭을 클릭합니다.
3. 이메일 주소를 입력합니다.
4. 비밀번호를 입력합니다.
5. **로그인**을 클릭합니다.

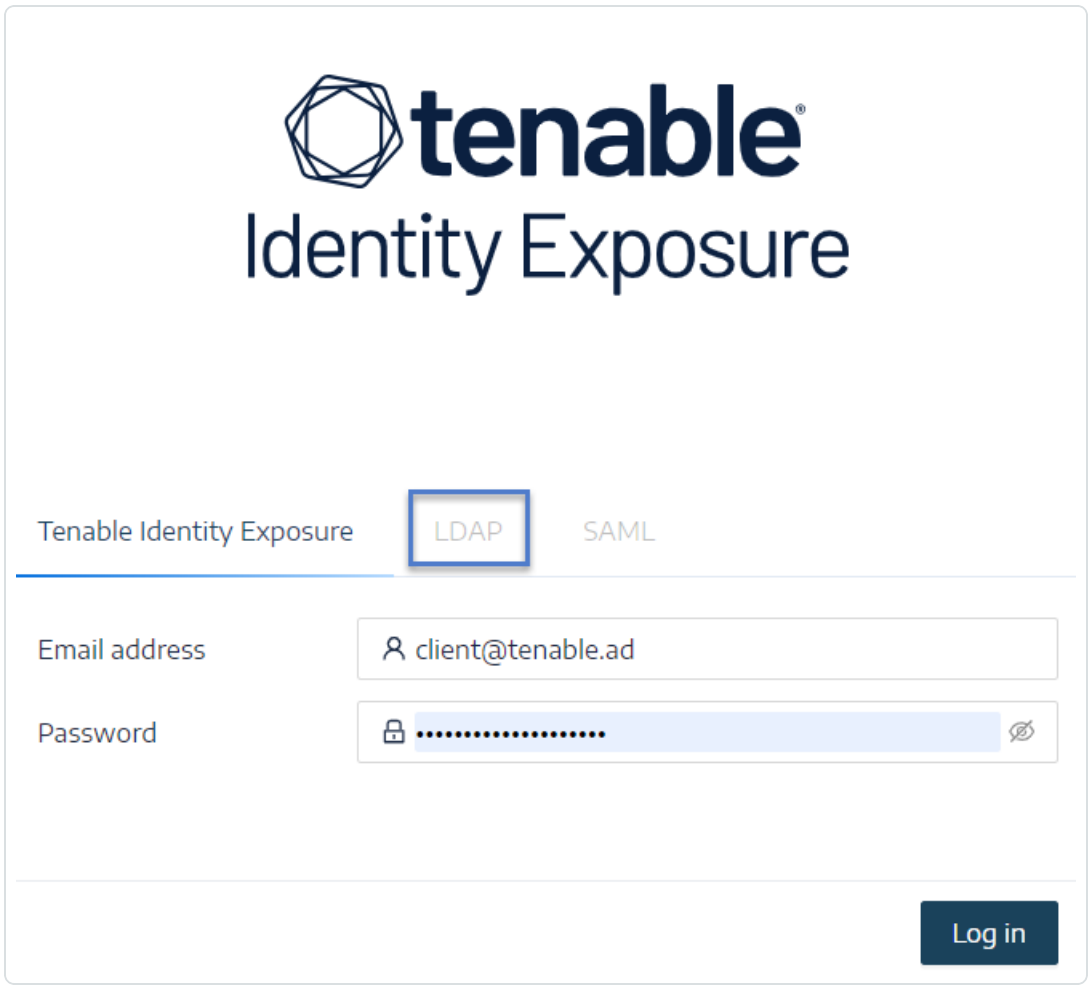
   Tenable Identity Exposure 페이지가 열립니다.

LDAP 계정 사용

LDAP를 사용하여 로그인하는 방법:

1. 브라우저에서 주소 표시줄에 클라이언트 URL(예: client.tenable.ad)을 입력합니다.

   로그인 창이 표시됩니다.



2. **LDAP** 탭을 클릭합니다.
3. LDAP 계정 이름을 입력합니다.
4. LDAP 비밀번호를 입력합니다.
5. **로그인**을 클릭합니다.

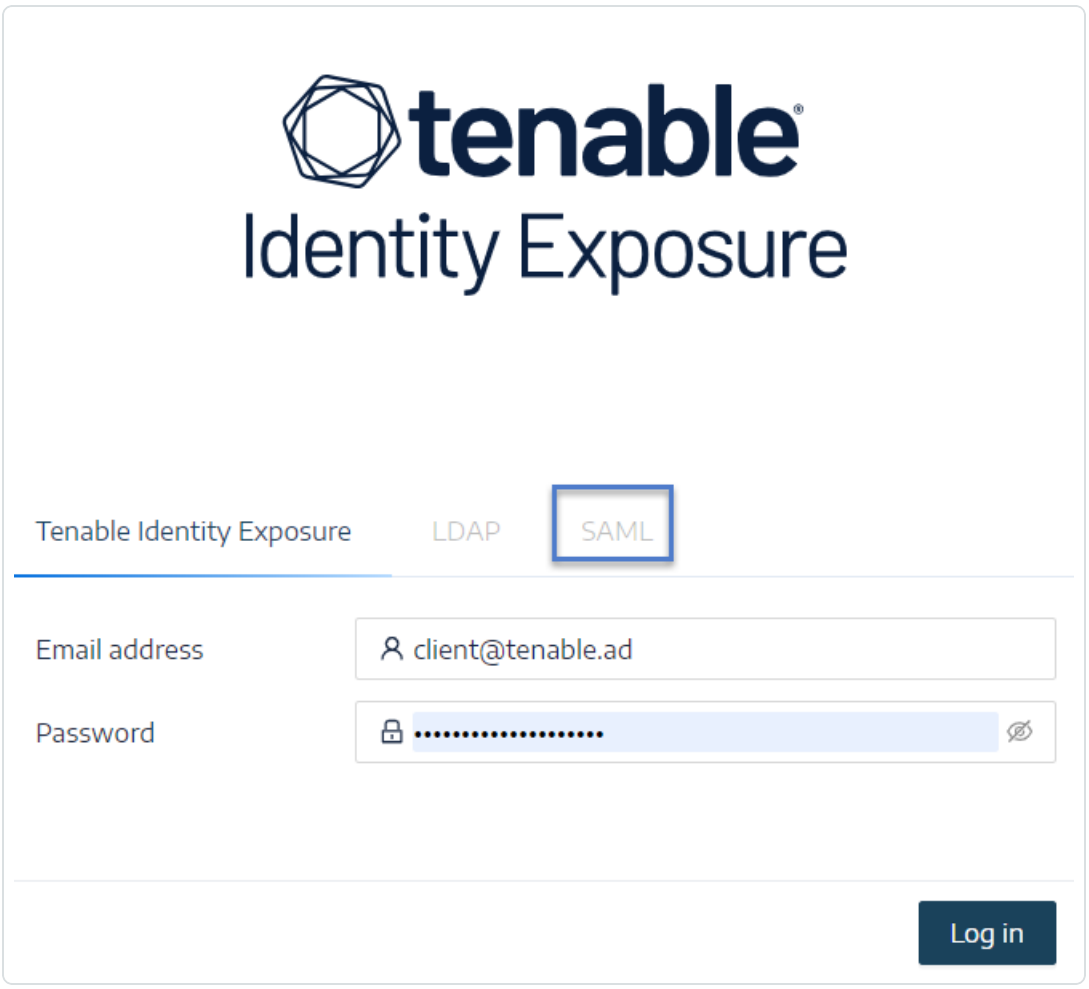
   Tenable Identity Exposure 페이지가 열립니다.

SAML 사용

SAML을 사용하여 로그인하는 방법:

1. 브라우저에서 주소 표시줄에 클라이언트 URL(예: client.tenable.ad)을 입력합니다.

   로그인 창이 표시됩니다.



2. **SAML** 탭을 클릭합니다.
3. ID 공급자(IDP)에 대한 링크를 클릭합니다.

   Tenable Identity Exposure에서 인증을 위해 SAML 서버로 리디렉션합니다.
4. IDP에 회사 자격 증명을 입력합니다.

   로그인한 사용자 자격으로 Tenable Identity Exposure에 리디렉션됩니다.

주의: 로그인에 여러 번 실패하면 Tenable Identity Exposure에서 계정을 잠급니다. 관리자에게 문의하십시오.

Tenable Identity Exposure에서 로그아웃하는 방법:

1. Tenable Identity Exposure에서 사용자 아이콘을 클릭합니다.

   하위 메뉴가 표시됩니다.

2. **로그아웃**을 클릭합니다.

   Tenable Identity Exposure가 로그인 페이지로 되돌아갑니다.

작업 영역에 액세스

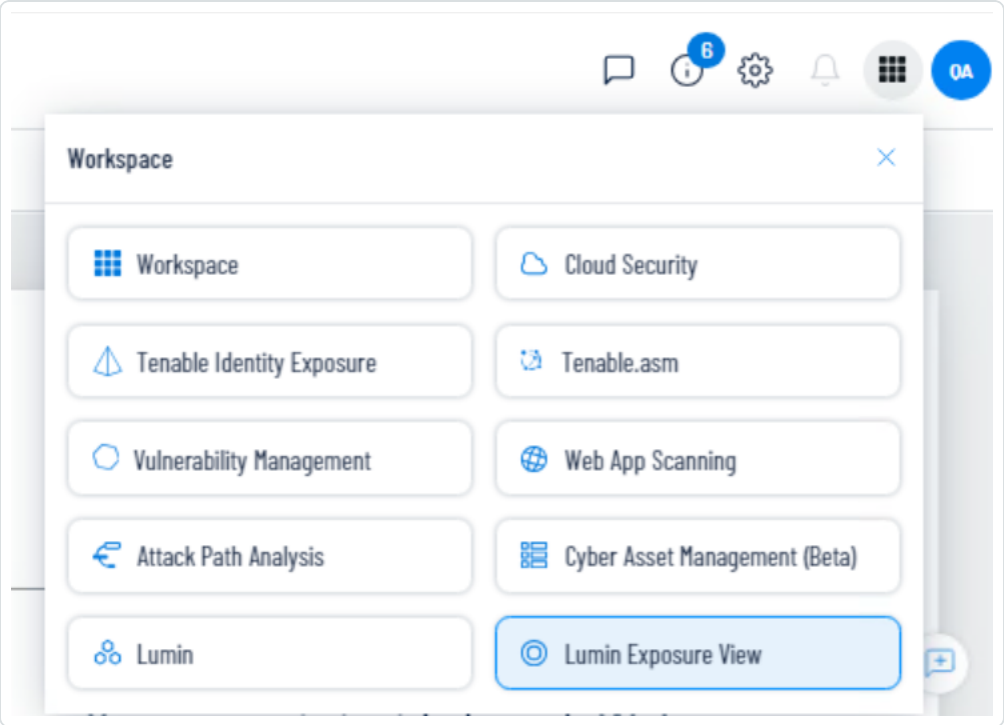
Tenable에 로그인하면 기본적으로 **작업 영역** 페이지가 표시됩니다. **작업 영역** 페이지에서 Tenable 애플리케이션을 전환하거나 나중에 **작업 영역** 페이지를 건너뛰도록 기본 애플리케이션을 설정할 수 있습니다. 상단 탐색 모음에 있는 **작업 영역** 메뉴에서 애플리케이션을 전환할 수도 있습니다.

작업 영역 메뉴 열기

작업 영역 메뉴를 여는 방법:

1. 원하는 Tenable 애플리케이션의 오른쪽 상단 모서리에서 ▦ 버튼을 클릭합니다.

   작업 영역 메뉴가 표시됩니다.



2. 애플리케이션 타일을 클릭하여 엽니다.

작업 영역 페이지 보기

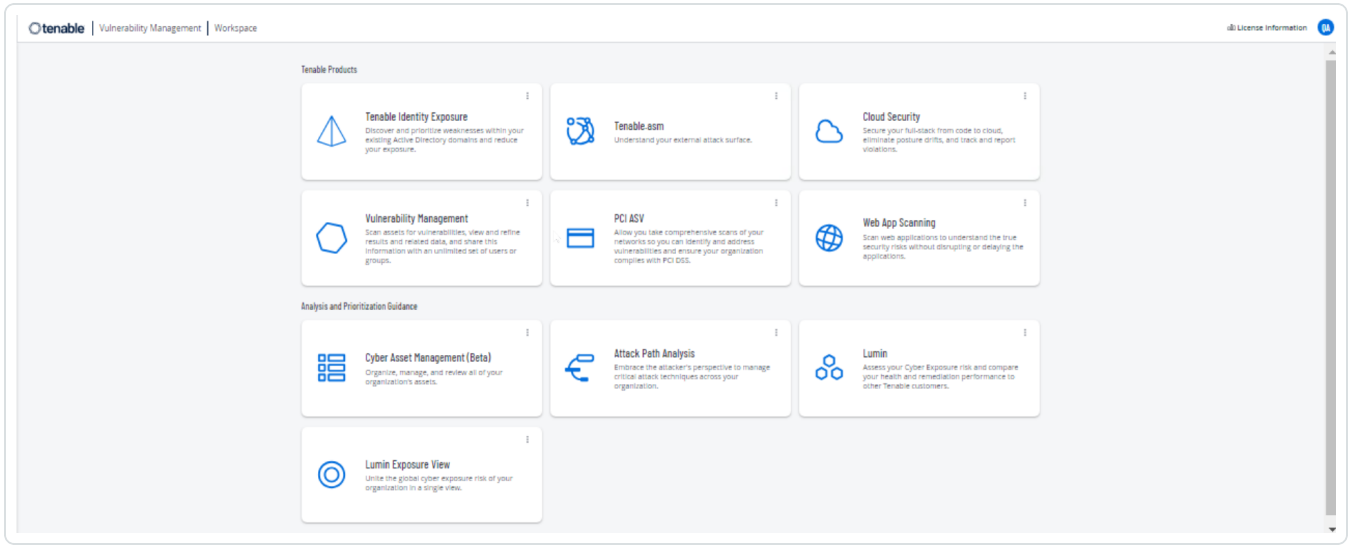
작업 영역 페이지를 보는 방법:

1. 원하는 Tenable 애플리케이션의 오른쪽 상단 모서리에서 ⠿ 버튼을 클릭합니다.

   작업 영역 메뉴가 표시됩니다.

2. **작업 영역** 메뉴에서 **작업 영역**을 클릭합니다.

   작업 영역 페이지가 표시됩니다.



기본 애플리케이션 설정

Tenable에 로그인하면 기본적으로 **작업 영역** 페이지가 표시됩니다. 그러나 나중에 **작업 영역** 페이지를 건너뛰도록 기본 애플리케이션을 설정할 수 있습니다.

> 기본적으로 **관리자**, **스캔 관리자**, **스캔 작업자**, **표준** 및 **기본** 역할이 부여된 사용자는 기본 애플리케이션을 설정할 수 있습니다. 다른 역할을 보유하고 있는 경우, 관리자에게 연락하여 **내 계정** 아래의 **관리** 권한을 요청하십시오. 자세한 내용은 사용자 지정 역할을 참조하십시오.

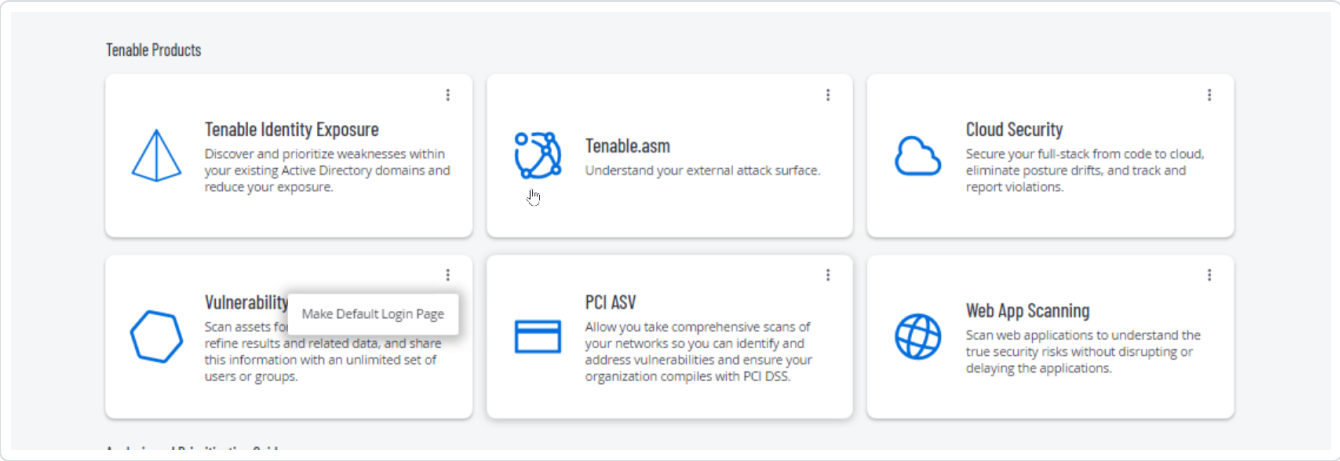
기본 로그인 애플리케이션을 설정하는 방법:

1. Tenable에 로그인합니다.

   작업 영역 페이지가 표시됩니다.

2. 선택할 애플리케이션의 오른쪽 상단 모서리에서 ⋮ 버튼을 클릭합니다.

   메뉴가 표시됩니다.



3. 메뉴에서 **기본 로그인 페이지로 설정**을 클릭합니다.

   이제 로그인하면 이 애플리케이션이 표시됩니다.

기본 애플리케이션 제거

기본 로그인 애플리케이션을 제거하는 방법:

1. Tenable에 로그인합니다.

   작업 영역 페이지가 표시됩니다.

2. 제거할 애플리케이션의 오른쪽 상단 모서리에서 ⋮ 버튼을 클릭합니다.

   메뉴가 표시됩니다.

3. **기본 로그인 페이지 제거**를 클릭합니다.

   이제 로그인하면 **작업 영역** 페이지가 표시됩니다.

사용자 기본 설정

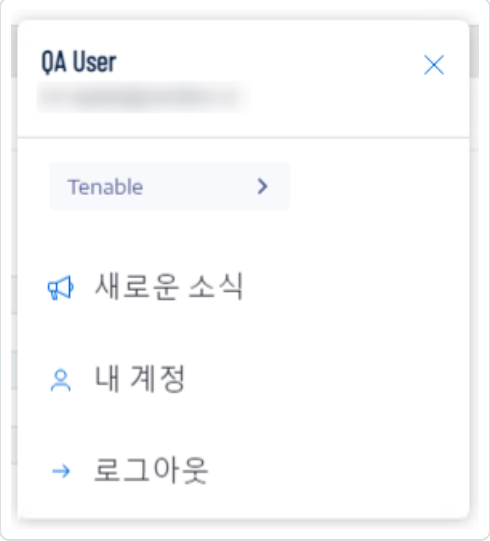
사용자 기본 설정은 Tenable Identity Exposure에서 설정할 수 있습니다.

- 언어를 선택하는 방법:
- 프로필을 선택하는 방법:
- 비밀번호를 변경하는 방법:
- 프로필을 선택하는 방법:

기본 설정을 설정하는 방법:

1. Tenable Identity Exposure에서 오른쪽 상단에 있는 사용자 프로필 아이콘을 클릭합니다.

   하위 메뉴가 표시됩니다.

2. **내 계정**을 선택합니다.

   기본 설정 페이지가 표시됩니다.

언어를 선택하는 방법:

a. **언어**에서 드롭다운 목록의 화살표를 클릭하여 기본 설정 언어를 선택합니다.

b. **저장**을 클릭합니다.

메시지가 표시되어 Tenable Identity Exposure에서 기본 설정을 업데이트했다고 확인합니다. 사용자 인터페이스에 선택한 언어가 표시됩니다.

프로필을 선택하는 방법:

한 보안 프로필에서 다른 보안 프로필로 전환하면 Tenable Identity Exposure에서 대시보드, 위젯 및 Trail Flow에 지표 구성과 데이터 표시를 표시하는 방식이 달라집니다.

a. **기본 설정** 아래에서 **프로필**을 클릭합니다.

b. **기본 설정 프로필**에서 드롭다운 화살표를 클릭하여 Tenable Identity Exposure에 연결된 후에 표시할 기본 프로필을 선택합니다.

c. **저장**을 클릭합니다.

메시지가 표시되어 Tenable Identity Exposure에서 기본 설정을 업데이트했다고 확인합니다.

자세한 내용은 보안 프로필을 참조하십시오.

비밀번호를 변경하는 방법:

> **참고**:Tenable One 라이선스가 있는 경우 비밀번호 정보를 사용할 수 없으며 이 경우 Tenable Vulnerability Management에서 모든 인증 설정을 관리합니다. 자세한 정보는 Tenable Vulnerability Management 사용자 가이드의 액세스 제어를 참조하십시오.

a. **기본 설정** 아래에서 **자격 증명**을 클릭합니다.

b. 다음과 같은 정보를 입력합니다.

- 이전 비밀번호.
- 새 비밀번호.

c. **새 비밀번호 확인** 입력란에 새 비밀번호를 다시 입력합니다.

d. **저장**을 클릭합니다.

메시지가 표시되어 Tenable Identity Exposure에서 비밀번호가 변경되었음을 확인합니다.

> **참고**: Tenable Identity Exposure에서 LDAP나 SAML과 같은 외부 공급자를 통해 연결된 계정의 비밀번호를 변경할 수는 없습니다.

API 키를 관리하는 방법:

a. **기본 설정** 아래에서 **API 키**를 클릭합니다.

   액세스 토큰이 **현재 API 키** 입력란에 표시됩니다.

b. 다음과 같은 작업을 수행할 수 있습니다.

c. 아이콘을 클릭하여 필요에 따라 사용할 수 있도록 API 키를 클립보드에 복사합니다.

d. **API 키 새로 고침**을 클릭하여 새 액세스 토큰을 만듭니다.

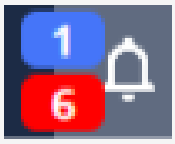
   메시지가 표시되어 확인을 요청합니다.

   > **참고**: API 키를 새로 고치면 Tenable Identity Exposure에서 현재 토큰을 비활성화합니다.

자세한 내용은 공개 API 사용을 참조하십시오.

알림

Tenable Identity Exposure 홈페이지의 오른쪽 상단에 벨 아이콘과 배지 수가 표시되어 사용자의 확인을 기다리는 공격 알림 및/또는 노출 알림을 알려줍니다. 새 알림이 수신되면 Tenable Identity Exposure에서 알림 배지 수를 높입니다.

	**파란색**	노출 알림
	빨간색	공격 알림

알림을 표시하는 방법:

1. Tenable Identity Exposure에서 벨 아이콘을 클릭합니다.

   알림 창이 열립니다.

2. 다음 중 한 가지 작업을 수행합니다.
   - **노출 알림** 탭을 클릭하여 노출 알림을 표시합니다.
   - **공격 알림** 탭을 클릭하여 공격 알림을 표시합니다.

     연결된 알림 목록이 표시됩니다.

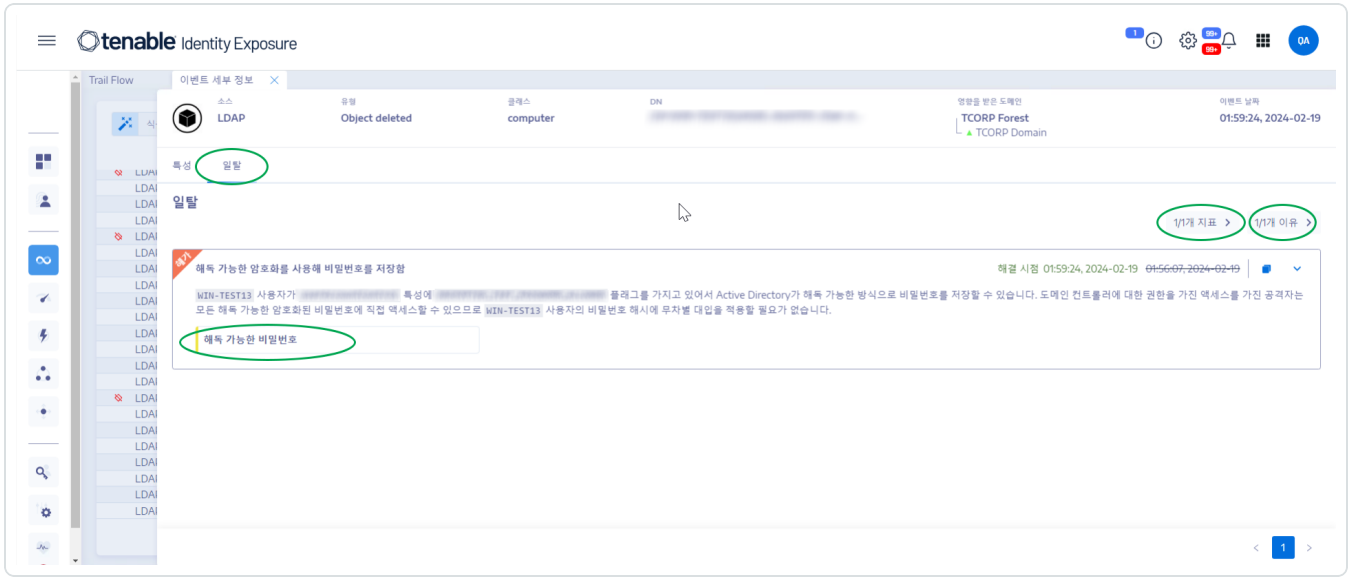
알림과 연결된 이벤트를 보는 방법:

1. 목록에서 알림을 선택하고 **작업**> **일탈 보기**를 클릭합니다.

   다음 정보를 포함한 이벤트 세부 정보 창이 열립니다.
   - 소스(이벤트 수집기)
   - 개체 유형
   - 파일
   - 경로
   - 영향을 받은 도메인
   - 날짜
   - 이벤트 시점의 값과 현재 값을 포함한 특성 목록

2. **일탈** 탭을 클릭합니다.

   해당 이벤트와 연결된 일탈 목록을 포함한 **일탈** 창이 열립니다.



3. **n/n 지표**를 클릭하여 알림을 트리거한 위험 노출 지표 창을 표시합니다.
4. **n/n 이유**를 클릭하여 알림 이유를 표시합니다.
5. 화살표를 클릭하여 해당 알림의 정보를 펼치거나 접습니다.
6. 지표 이름을 클릭하여 지표 세부 정보 페이지를 표시합니다.

알림을 보관하는 방법:

알림을 확인한 후에 보관할 수 있습니다.

1. **알림** 창의 알림 목록에서 보관하려는 알림의 확인란을 선택합니다.
   - 선택 사항으로 창 아래의 **n/n개 개체 선택됨** 확인란을 클릭하여 모든 알림을 일괄 선택할 수도 있습니다.
2. 창 아래에서 **작업 선택** > **보관**을 클릭합니다.
3. **확인**을 클릭합니다.

대시보드

대시보드를 사용하면 Active Directory 보안에 영향을 미치는 데이터와 추세를 시각화할 수 있습니다. 위젯으로 사용자 지정하여 요구 사항에 따라 차트와 카운터를 표시할 수 있습니다.

Tenable Identity Exposure에서 조직에 관련된 우선 순위 문제에 집중하기 위해 사용할 수 있는 대시보드 템플릿을 제공합니다. 예를 들어 다음과 같은 템플릿이 있습니다.

- **AD 규정 준수 및 상위 위험** – 규정 준수 점수, 변화 및 위험 중요도 규정 준수
- **AD Risk 360** – 위험 노출 지표 심각도 기준 일탈 변화 및 문제
- **비밀번호 관리 위험** – 비밀번호 관련 문제
- **사용자 모니터링** – AD 사용자 변화, 사용자 범주 수
- **기본 관리자 모니터링** – 관리 계정 메트릭

템플릿을 사용하여 새 대시보드를 만드는 방법:

1. Tenable Identity Exposure에서  또는 **대시보드**를 클릭합니다. (이 페이지는 기본적으로 Tenable Identity Exposure에서도 열립니다.)
2. 다음 중 하나를 수행할 수 있습니다.
   - 창이 비어 있는 경우: **대시보드 추가**를 클릭합니다.
   - 창에 이미 하나 이상의 대시보드가 포함되어 있는 경우: 오른쪽 상단의  > **새 대시보드 추가**를 클릭합니다.

     대시보드 템플릿 구성 창이 열립니다.
3. 추가할 대시보드를 선택합니다.
4. **대시보드 추가**를 클릭합니다.
5. 메시지가 표시되어 Tenable Identity Exposure에서 대시보드와 위젯을 만들었다고 확인합니다. **대시보드** 창의 탭 아래에 새 대시보드가 표시됩니다.

사용자 지정 대시보드를 추가하는 방법:

1. Tenable Identity Exposure에서  또는 **대시보드**를 클릭합니다. (이 페이지는 기본적으로 Tenable Identity Exposure에서도 열립니다.)
2. 오른쪽 상단에서  > **새 대시보드 추가**를 클릭합니다.

   대시보드 템플릿 구성 창이 열립니다.
3. 하단에서 **사용자 지정 대시보드** 템플릿을 선택합니다.
4. 대시보드 이름을 입력합니다.
5. **대시보드 추가**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 대시보드를 만들었다고 확인합니다. **대시보드** 창의 탭 아래에 새 대시보드가 표시됩니다.
6. 대시보드에 위젯을 추가하는 방법은 위젯을 참조하십시오.

대시보드의 이름을 바꾸는 방법:

1. **대시보드** 창에서 이름을 바꾸려는 대시보드의 탭을 선택합니다.
2. 오른쪽 상단에서 > **이름 편집**을 클릭합니다.

   대시보드 구성 창이 열립니다.
3. **이름** 입력란에 대시보드의 다른 이름을 입력합니다.
4. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 대시보드를 업데이트했다고 확인합니다.

대시보드를 삭제하는 방법:

1. **대시보드** 창에서 삭제하려는 대시보드의 탭을 선택합니다.
2. 오른쪽 상단에서 > **대시보드 삭제**를 클릭합니다.

   대시보드 삭제 창이 열려 삭제 확인을 요청합니다.
3. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 대시보드를 삭제했다고 확인합니다.

위젯

대시보드의 위젯을 사용하면 Active Directory를 막대형 차트, 꺾은선형 차트 및 카운터 형식으로 표시할 수 있습니다. 위젯을 사용자 지정하여 특정 정보를 표시하고 끌어서 대시보드에서의 위치를 변경할 수 있습니다.

새로 만든 대시보드 또는 기존 대시보드에 위젯을 추가할 수 있습니다.

대시보드에 위젯을 추가하는 방법:

1. Tenable Identity Exposure에서  또는 **대시보드**를 클릭합니다. (이 페이지는 기본적으로 Tenable Identity Exposure에서도 열립니다.)
2. 대시보드 창에서 대시보드 탭을 선택합니다.
3. 다음 중 하나를 수행할 수 있습니다.
   - 대시보드가 비어 있는 경우: **위젯 추가**를 클릭합니다.
   - 대시보드에 이미 위젯이 포함되어 있는 경우: 오른쪽 상단에서  > **현재 대시보드에 위젯 추가**를 클릭합니다.

     위젯 추가 창이 열립니다.
4. 타일을 클릭하여 다음 중 하나를 선택합니다.
   - 막대형 차트
   - 꺾은선형 차트
   - 카운터
5. **위젯 이름** 입력란에 해당 위젯의 이름 입력
6. **위젯 구성** 아래의 **데이터 유형** 입력란에서 드롭다운 목록의 화살표를 클릭하여 다음 중 한 가지를 선택합니다.
   - 사용자 수: 도메인의 활성 사용자 수입니다.
   - 일탈 수: 탐지된 일탈 또는 보안 침해의 수입니다.

- 규정 준수 점수: Tenable Identity Exposure에서 탐지된 일탈의 수와 그 심각도 수준을 계산한 점수(0~100점)입니다.
- 기간(꺾은선형 차트의 경우): 드롭다운 목록의 화살표를 클릭하여 표시할 기간을 선택합니다.

7. **데이터 세트 구성** 아래에서:

데이터 세트 구성	
상태(사용자 수)	활성, 비활성 또는 모두를 선택합니다.
지표	a. **지표**를 클릭하여 하나 이상의 지표를 선택합니다. **위험 노출 지표** 창이 시작됩니다. b. 목록에서 하나의 또는 여러 지표를 선택합니다. 원하는 경우 다음과 같이 할 수도 있습니다. ■ 검색 상자에 지표 이름을 입력합니다. ■ 모든 지표를 선택합니다. ■ 특정 심각도 수준(위험, 높음, 중간 또는 낮음)의 모든 지표를 선택합니다. c. **선택 항목 필터링**을 클릭합니다.
도메인	a. **도메인**을 클릭하여 하나 이상의 도메인을 선택합니다. **포리스트 및 도메인** 창이 열립니다. b. 목록에서 도메인을 선택합니다. 원하는 경우 다음과 같이 할 수도 있습니다. ■ 검색 상자에 도메인 이름을 입력합니다. ■ 모든 도메인을 선택합니다. c. **선택 항목 필터링**을 클릭합니다.

8. **데이터 세트의 이름** 입력란에 데이터 세트의 이름을 입력합니다.
9. 위젯의 도메인을 선택합니다.

원하는 경우 검색 상자에 도메인 이름을 입력할 수 있습니다.

10. **선택 항목 필터링**을 클릭합니다.
11. 원하는 경우 **새 데이터 세트 추가**를 클릭하여 위젯의 다른 옵션을 포함한 다른 데이터 세트를 추가할 수 있습니다.
12. **추가**를 클릭합니다.

    메시지가 표시되어 Tenable Identity Exposure에 위젯이 추가되었음을 확인합니다.

위젯을 수정하는 방법:

1. Tenable Identity Exposure에서 **대시보드**를 클릭합니다.
2. 수정하려는 위젯을 포함하는 대시보드를 선택합니다.
3. 위젯을 선택합니다.
4. 위젯의 오른쪽 상단에 있는 ✎ 아이콘을 클릭합니다.

   위젯 수정 창이 열립니다.
5. 필요에 따라 수정합니다.
6. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 위젯을 업데이트했음을 확인합니다.

위젯을 새로 고치는 방법:

1. 위젯을 선택합니다.
2. 위젯의 오른쪽 상단에 있는 ↻ 아이콘을 클릭합니다.

   위젯이 새로 고쳐집니다.

위젯을 삭제하는 방법:

1. Tenable Identity Exposure에서 **대시보드**를 클릭합니다.
2. 삭제하려는 위젯을 포함하는 대시보드를 선택합니다.
3. 위젯을 선택합니다.

4. 🗑 아이콘을 클릭합니다.

   위젯 제거 창이 열립니다. 메시지가 표시되어 삭제할 것인지 확인을 요청합니다.

5. **확인**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 위젯을 대시보드에서 삭제했음을 확인합니다.

참고 항목

- 대시보드

Identity Explorer

권한: Microsoft Entra ID의 구성 및 데이터 시각화에 액세스하려면 사용자 역할에 적절한 권한이 있어야 합니다. 자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

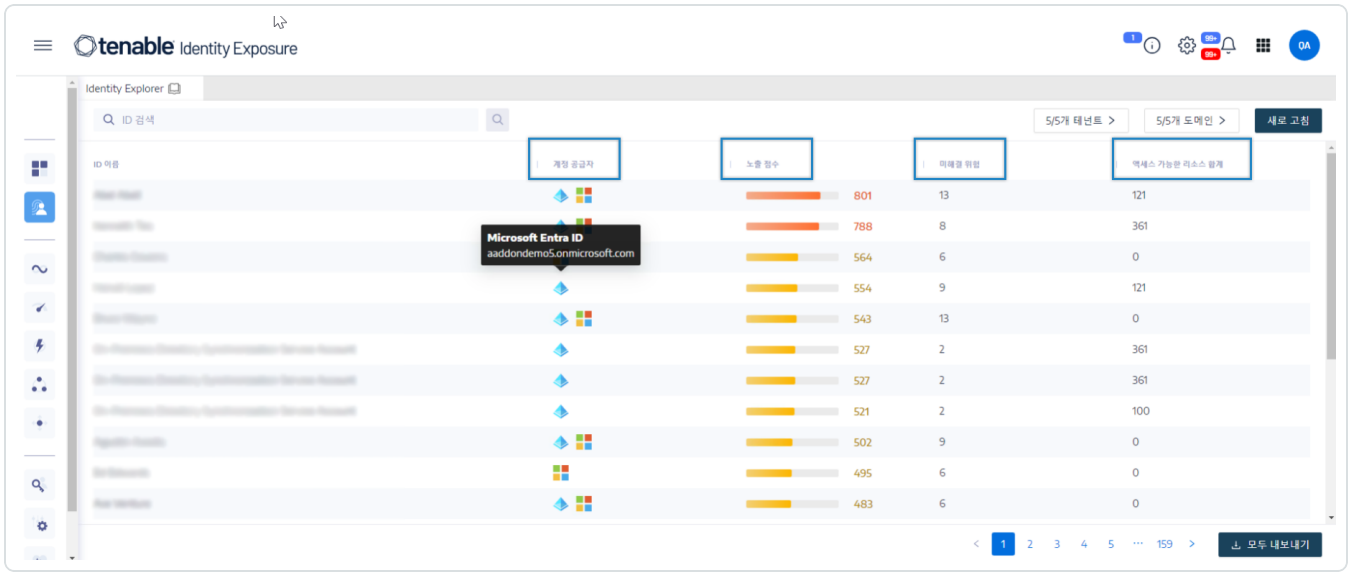
Tenable Identity Exposure의 Identity Explorer 보기는 Active Directory와 Microsoft Entra ID 모두의 ID를 통합합니다. 이 보기에는 나열된 각 자산의 ID 위험 점수(베타)와 침해된 ID의 잠재적 범위가 표시됩니다.

Identity Explorer에 액세스하는 방법:

참고: Identity Explorer는 Microsoft Entra ID 기능을 사용하는 경우에만 표시됩니다. 자세한 내용은 Microsoft Entra ID 지원을 참조하십시오.

- Tenable Identity Exposure에서 왼쪽 탐색 모음의 Identity Explorer 아이콘 을 클릭합니다.

  Identity Explorer 창이 열립니다.



Identity Explorer 창에는 액세스할 수 있는 리소스 전체에 대하여 다음과 같은 정보가 표시됩니다.

- **ID 이름** – ID 공급자에 속한 사용자 계정의 이름입니다.
- **계정 공급자** – ID 공급자입니다.

- **위험 노출 점수** – Tenable Identity Exposure에서는 자산 또는 ID의 중요도와 각 ID 공급자에 대한 취약성을 평가하여 이 지표를 계산하고 집계하여 주어진 ID에 대한 전체 노출 점수를 제공합니다.

  > **참고**: Tenable Identity Exposure에서는 사용자에게 Tenable One 라이선스가 있는 경우에만 위험 노출 점수를 표시합니다.

- **미해결 위험** - Microsoft Entra ID 위험 노출 지표가 자산을 스캔하여 탐지한 조사 결과의 수입니다. 자세한 내용은 Microsoft Entra ID 관련 위험 노출 지표을 참조하십시오.
- **액세스 가능한 리소스 합계** - 이 자산이 액세스(읽기, 쓰기 등)할 수 있는 모든 유형의 리소스 수입니다.

ID를 검색하는 방법:

1. **Identity Explorer** 창의 **검색** 상자에 사용자나 계정의 이름을 입력합니다.
2. 아이콘을 클릭합니다.

   Tenable Identity Exposure에서 일치하는 결과를 표시합니다.

ID를 내보내는 방법:

1. **Identity Explorer** 창 하단에서 **모두 내보내기**를 클릭합니다.

   ID 내보내기 창이 열립니다.
2. **모두 내보내기**를 클릭합니다.

   Tenable Identity Exposure에서 파일을 로컬 컴퓨터에 다운로드합니다.

Trail Flow

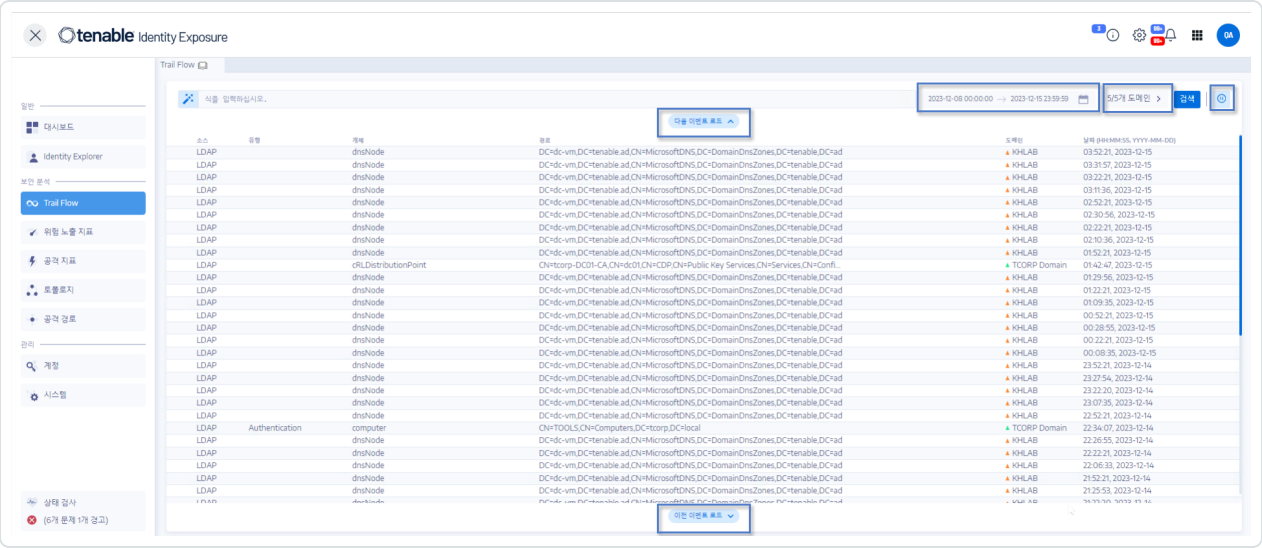
Tenable Identity Exposure의 Trail Flow에는 AD 인프라에 영향을 미치는 이벤트에 대한 실시간 모니터링 및 분석이 표시됩니다. 이것을 사용하면 중대한 취약성과 수정하기 위해 권장되는 과정을 확인할 수 있습니다.

Trail Flow 페이지를 사용하면 시간을 거슬러 되돌아가 이전 이벤트를 로드하거나 특정 이벤트를 검색할 수 있습니다. 또한 페이지 상단에 검색 상자를 사용하여 위협을 검색하고 악성 패턴을 탐지할 수도 있습니다.

Trail Flow에 액세스하는 방법:

- Tenable Identity Exposure에서 왼쪽의 탐색 모음에 있는 **Trail Flow**를 클릭합니다.

  이벤트 목록을 포함한 Trail Flow 페이지가 열립니다. 자세한 내용은 Trail Flow 표을 참조하십시오.



시간 범위를 선택하는 방법:

1. **Trail Flow** 페이지 상단에서 캘린더 상자를 클릭합니다.
2. 시작 날짜와 종료 날짜를 선택합니다.
3. **검색**을 클릭합니다.

   Tenable Identity Exposure에서 선택한 시간 범위로 Trail Flow 표를 업데이트합니다.

도메인을 선택하는 방법:

1. **Trail Flow** 페이지 상단에 **n/n 도메인 >**을 클릭합니다.

   포리스트 및 도메인 창이 열립니다.

2. 포리스트와 도메인을 선택합니다.

3. **선택 항목 필터링**을 클릭합니다.

   Tenable Identity Exposure에서 선택한 포리스트와 도메인의 정보로 Trail Flow 표를 업데이트 합니다.

이벤트를 확인하는 방법:

- Trail Flow 표에서 탐색하려는 이벤트를 포함한 줄을 클릭합니다.

  이벤트 세부 정보 창이 열립니다. 자세한 내용은 이벤트 세부 정보을 참조하십시오.

Trail Flow를 일시 정지하고 다시 시작하는 방법:

- 다음 중 한 가지 작업을 수행합니다.
  - ⏸ 아이콘을 클릭하여 Trail Flow를 일시 정지합니다.

    Tail Flow를 일시 정지하면 최신 이벤트를 자동으로 수직 스크롤링하는 작업이 멈추지만, 분석은 배경에서 계속 실행되어 이벤트에 대한 검색을 실행할 수 있습니다.
  - ▶ 아이콘을 클릭하여 Trail Flow를 다시 시작합니다.

다음 또는 이전 이벤트를 로드하는 방법:

- Trail Flow 페이지에서 다음 중 한 가지 작업을 수행합니다.
  - 다음 이벤트 로드 클릭
  - 이전 이벤트 로드 클릭

Trail Flow 표

Tenable Identity Exposure에서 Active Directory에 이벤트를 발생하는 대로 계속해서 Trail Flow 표의 목록에 추가합니다. 여기에는 다음과 같은 정보가 포함됩니다.

정보	설명
소스	AD 인프라에 보안 관련 변경 사항이 발생한 곳을 나타냅니다. 가능한 소스는 두 가지입니다. • AD 인프라와 통신에 사용되는 LDAP(Lightweight Directory Access Protocol)입니다. • 파일, 프린터 등을 공유하는 데 사용되는 SMB(Server Message Block) 프로토콜입니다. **Tenable Identity Exposure**에서 네트워크를 통과하는 LDAP와 SMB 트래픽을 철저히 분석하여 이상과 잠재적 위협을 탐지합니다. **참고**: Active Directory(AD)를 사용하면 관리자가 사용자와 컴퓨터 계정에 배포된 설정을 제어하는 그룹 정책을 만들 수 있습니다. GPO(Group Policy Object)에 이러한 제어 설정을 저장합니다. Sysvol 폴더는 GPO 파일을 도메인 컨트롤러에 저장합니다. AD 보안을 위해 GPO 내용을 모니터링하는 것이 중요합니다. 각각의 도메인 멤버가 높은 수준의 권한을 가지고 적용하거나 실행할 수 있기 때문입니다.
유형	다음과 같은 이벤트의 특징적인 요소를 보여줍니다. • ACL 변경됨 • SPN 변경됨 • 멤버 제거됨 • 새 멤버 • 새 트러스트 관계 • 알 수 없는 파일 유형 추가됨 • 새 개체 • 개체 제거됨

	• 비밀번호 변경됨 • UAC 변경됨 • 새 GPO 연결됨 • GPO 링크 제거됨 • 소유자 변경 • 파일 이름 바꿈 • SPN 만듦 • 인증 초기화 실패 • 인증 실패
개체	AD 개체와 연결된 클래스 또는 파일 확장자를 나타냅니다. 디렉터리 개체(사용자, 컴퓨터 등) 또는 특정 파일 이름 확장자(ini, XML, csv)를 포함한 파일을 검색할 수 있습니다.
경로	AD에 이 개채의 고유한 위치를 식별하는 AD 개체까지 전체 경로를 나타냅니다.
디렉터리	AD 인프라 변경이 발생한 디렉터리를 나타냅니다.
날짜	이벤트 시간을 나타냅니다.

마법사를 사용하여 Trail Flow 검색

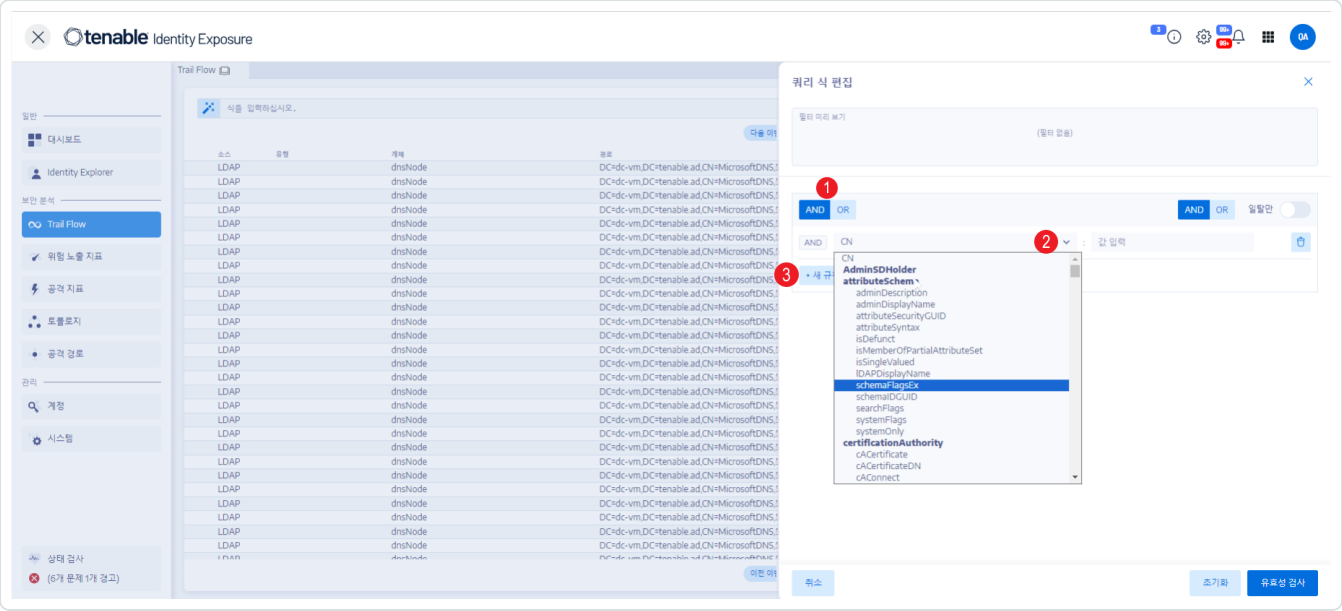
검색 마법사를 사용하면 쿼리 식을 만들고 조합할 수 있습니다.

- 검색 상자에서 식을 자주 사용하는 경우, 책갈피 목록에 추가하여 나중에 사용할 수 있습니다.
- 검색 상자에 식을 입력하면 사용자가 다시 사용할 수 있도록 Tenable Identity Exposure에서 이 식을 기록 창에 저장합니다.

마법사를 사용하여 검색하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 아이콘을 클릭합니다.

   쿼리 식 편집 창이 시작됩니다. 자세한 내용은 Trail Flow 쿼리 사용자 지정을 참조하십시오.



3. 패널에서 쿼리 식을 정의하려면 **AND** 또는 **OR** 연산자 버튼(1)을 클릭하여 첫 번째 조건에 적용합니다.
4. 드롭다운 메뉴에서 특성을 하나 선택한 다음 그 값(2)을 입력합니다.
5. 다음 중 작업을 수행합니다.

- 특성을 추가하려면 **+ 새 규칙 추가**(3)를 클릭합니다.
- 또 다른 조건을 추가하려면 **새 조건 추가+AND** 또는 **+OR** 연산자를 클릭합니다. 드롭다운 메뉴에서 특성을 선택하고 그 값을 입력합니다.
- 검색을 일탈 개체로 제한하려면 **일탈만** 토글을 허용으로 클릭합니다. **+AND** 또는 **+OR** 연산자를 선택하여 해당 조건을 쿼리에 추가합니다.
- 조건 또는 규칙을 삭제하려면 🗑 아이콘을 클릭합니다.

6. **유효성 검사**를 클릭하여 검색을 실행하거나 **초기화**하여 쿼리 식을 수정합니다.

참고 항목

- Trail Flow를 수동으로 검색
- 마법사를 사용하여 Trail Flow 검색
- Trail Flow 쿼리 사용자 지정
- 책갈피 쿼리
- 쿼리 기록

Trail Flow를 수동으로 검색

특정 문자열 또는 패턴과 일치하는 이벤트를 필터링하려면 검색 상자에 식을 입력하여 부울 연산자 *, **AND** 및 **OR**를 사용하여 결과를 상세 검색할 수 있습니다. **OR** 문을 괄호로 감싸면 검색 우선 순위를 수정할 수 있습니다. 검색으로 Active Directory 특성에서 특정 값을 찾습니다.

Trail Flow를 수동으로 검색하는 방법:

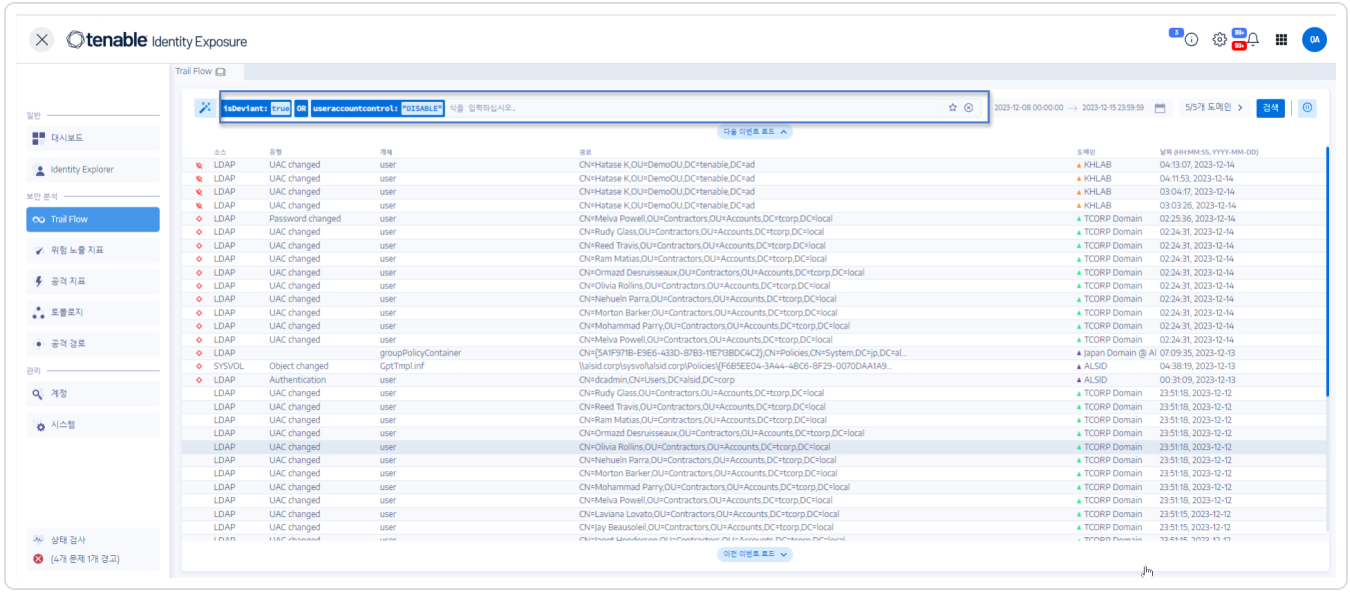
1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자에 쿼리 식을 입력합니다.
3. 검색 결과를 다음과 같이 필터링할 수 있습니다.
    - **캘린더** 상자를 클릭하여 시작 날짜와 종료 날짜를 선택합니다.
    - **n/n 도메인**을 클릭하여 포리스트와 도메인을 선택합니다.
4. **검색**을 클릭합니다.

    Tenable Identity Exposure에서 검색 기준과 일치하는 결과로 목록을 업데이트합니다.

예:

다음 예에서 검색한 대상은 다음과 같습니다.

- 모니터링되는 AD 인프라를 위험하게 할 수 있는 비활성화된 사용자 계정.
- 의심스러운 활동 및 비정상적 계정 사용.



문법 및 구문

수동 쿼리 식은 다음과 같은 문법과 구문을 사용합니다.

- 문법: `EXPRESSION [OPERATOR EXPRESSION]*`
- 구문: `__KEY__ __SELECTOR__ __VALUE__`

  여기에서:

  - `__KEY__`는 검색할 AD 개체 특성을 가리킵니다(예: `CN`, `userAccountControl`, `members` 등).
  - `__SELECTOR__`는 연산자(`:`, >, <, >=, <=)를 가리킵니다.
  - `__VALUE__`는 검색할 값을 가리킵니다.

    특정 콘텐츠를 찾는 데 이외의 키를 사용할 수 있습니다.
  - `isDeviant`는 일탈을 만든 이벤트를 찾습니다.

AND 및 **OR** 연산자를 사용하면 여러 개의 Trail Flow 쿼리 식을 조합할 수 있습니다.

예:

- 공통 이름 속성으로 `alice` 문자열을 포함하는 모든 객체를 찾기: `cn:"alice"`
- 공통 이름 특성에 문자열 `alice`를 포함하고 특정 일탈을 만든 모든 개체 찾기: `isDeviant:"true" and cn:"alice"`
- 이름이 Default Domain Policy인 GPO 찾기: `objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- SID에 S-1-5-21을 포함하는 모든 비활성화된 계정 찾기: `userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`
- Sysvol에서 모든 `script.ini` 파일 찾기: `globalpath:"sysvol" and types:"SCRIPTSini"`

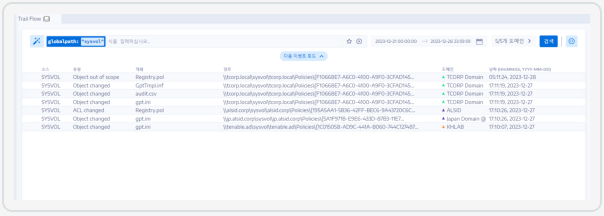
  > **참고**: 여기서 `types`는 열 머리글이 아니라 개체 속성을 나타냅니다.

Trail Flow 쿼리 사용자 지정

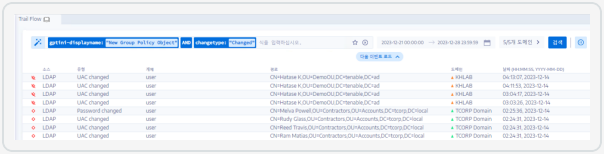
Trail Flow를 사용하면 위험 노출 지표 및 공격 지표의 기본 모니터링 이상으로 Tenable Identity Exposure 기능을 확장할 수 있습니다. 사용자 지정 쿼리를 만들어서 데이터를 빠르게 검색하고 쿼리를 Tenable Identity Exposure에서 SIEM(Security Information and Event Management)에 보낼 수 있는 사용자 지정 알림으로 사용할 수도 있습니다.

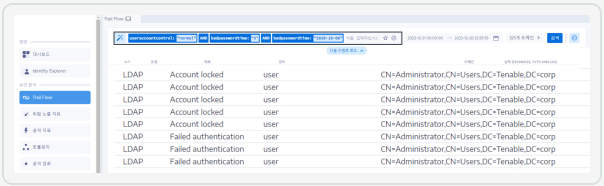
다음 예는 Tenable Identity Exposure의 실용적인 사용자 지정 쿼리를 보여줍니다.

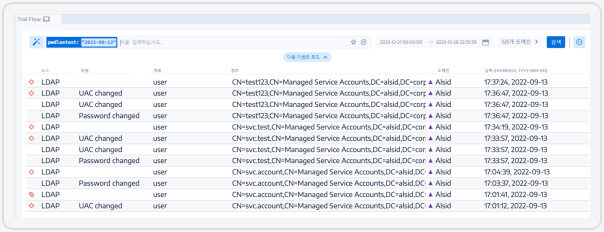
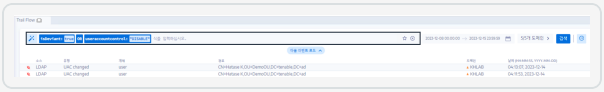
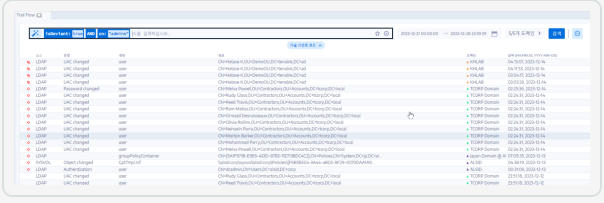
사용 사례	설명

GPO 시작 및 종료 바이너리 및 전역 SYSVOL 경로 모니터링	부팅 시작 경로 및/또는 전역 SYSVOL 복제 경로에서 스크립트를 모니터링합니다. 공격자는 종종 이러한 스크립트를 사용하여 네이티브 AD 서비스를 악용하여 환경 전체에서 랜섬웨어를 빠르게 확산시킵니다.
	• **시작 경로 쿼리의 스크립트:**
	`globalpath: "sysvol" AND types: "Scriptsini"`
	참고: 여기에서 types는 열 헤더가 아닌 개체 특성을 가리킵니다.
	• **SYSVOL 모니터링 쿼리**:
	`globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")`
	 

GPO 구성 수정	GPO 구성에 대한 수정 사항을 모니터링합니다. 공격자는 종종 이 방법을 사용하여 지속성 및/또는 계정 탈취를

	돕기 위해 보안 설정을 다운그레이드합니다. • **GPO 모니터링 쿼리:** `gptini-displayname:"New Group Policy Object" AND changetype:"Changed"` 

인증 및 비밀번호 초기화 실패	여러 번의 인증 시도 실패로 인해 잠금이 발생하는지 모니터링합니다. 비밀번호 무차별 대입 시도에 대한 조기 경고 플래그 역할을 할 수 있습니다.
	
	참고: 잠금 정책 및 날짜/시간 변수를 설정해야 합니다. 자세한 내용은 Tenable Identity Exposure 계정을 사용한 인증을 참조하십시오.
	
	• **인증 실패 쿼리:**
	
	`useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>" AND badpasswordtime:"<DATE_TIME_STAMP>"`
	
	 
	
	• **비밀번호 초기화 쿼리:**
	
	`pwdlastset:" <DATE_TIME_STAMP"`

	
개체 권한 추가, 제거 또는 변경	ACL 권한 및 관련 개체 권한 집합에 대한 무단 수정을 모니터링합니다. 공격자는 이 방법을 악용하여 권한을 상승시킵니다. **참고**: 날짜/시간 변수를 제공해야 합니다. • **개체 권한 쿼리:** `ntsecuritydescriptor:0 AND whenchanged:"DATE_TIME_STAMP"` 
일탈을 초래하는 관리자 변경	기본 제공 관리 그룹과 사용자 지정 그룹은 위험을 초래할 수 있는 일탈 또는 구성 변경을 면밀히 모니터링해야 하는 중요한 그룹입니다. 이 쿼리를 사용하면 관리자 그룹 내 보안 설정에 악영향을 미쳤을 수 있는 최근 변경 사항을 신속하게 검토할 수 있습니다. • **관리자 변경 사항 쿼리:** `isDeviant:true AND cn:"admins"` 

참고 항목

- Trail Flow를 수동으로 검색
- 마법사를 사용하여 Trail Flow 검색
- 책갈피 쿼리
- 쿼리 기록
- Trail Flow 사용 사례

책갈피 쿼리

쿼리 식을 자주 사용하는 경우, 사용자 지정 책갈피 목록에 추가하여 다시 사용할 수 있습니다.

쿼리 식을 책갈피에 추가하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자 옆에 있는 🪄 아이콘을 클릭합니다.

   쿼리 식 편집 창이 시작됩니다.
3. 검색 상자에 쿼리 식을 입력합니다.
4. 검색 상자 오른쪽에 있는 ☆ 아이콘을 클릭합니다.

   책갈피에 추가 상자가 표시됩니다.
5. **폴더 선택** 상자에서 드롭다운 화살표를 클릭하여 목록에서 폴더를 선택합니다.
6. (선택 사항) **새 폴더 만들기** 토글이 **예**가 되도록 클릭합니다. **폴더 이름** 상자에 해당 책갈피 폴더의 이름을 입력합니다.
7. **책갈피 이름** 상자에 책갈피 이름을 입력합니다.
8. **추가**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 목록에 책갈피를 추가했다고 확인합니다.

책갈피에 추가한 쿼리 식을 사용하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자 안쪽을 클릭합니다.

   검색 상자 아래로 **기록**과 **책갈피** 탭이 표시됩니다.
3. **책갈피** 탭을 클릭합니다.

   책갈피 목록이 표시됩니다.
4. 책갈피를 클릭하여 선택합니다.

   Tenable Identity Exposure에서 쿼리 식을 로드하여 검색을 실행합니다.

책갈피를 관리하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자 안쪽을 클릭합니다.

   검색 상자 아래로 **기록**과 **책갈피** 탭이 표시됩니다.
3. **책갈피** 탭을 클릭합니다.

   책갈피 목록이 표시됩니다.
4. **책갈피 관리**를 클릭합니다.

   책갈피 창이 열립니다.
5. 다음 중 작업을 수행합니다.
   - 책갈피 검색:
     a. 검색 상자에 책갈피 이름을 입력합니다.
     b. 드롭다운 목록에서 폴더를 선택합니다.
   - 책갈피 또는 책갈피 폴더 이름 편집:
     a. 책갈피 또는 책갈피 폴더의 ✎ 아이콘을 클릭합니다.
     b. **책갈피 이름** 또는 **폴더 이름** 상자에 책갈피 또는 책갈피 폴더의 새 이름을 입력합니다.
     c. **편집**을 클릭합니다.

        메시지가 표시되어 Tenable Identity Exposure에서 책갈피 또는 책갈피 폴더 이름을 업데이트했다고 확인합니다.
   - 책갈피 폴더의 책갈피 삭제:
     - 책갈피 또는 책갈피 폴더의 🗑 아이콘을 클릭합니다.

참고 항목

- Trail Flow를 수동으로 검색
- 마법사를 사용하여 Trail Flow 검색
- Trail Flow 쿼리 사용자 지정

- 쿼리 기록
- Trail Flow 사용 사례

쿼리 기록

검색 상자에 식을 입력하면 사용자가 다시 사용할 수 있도록 Tenable Identity Exposure에서 이 식을 기록 창에 저장합니다.

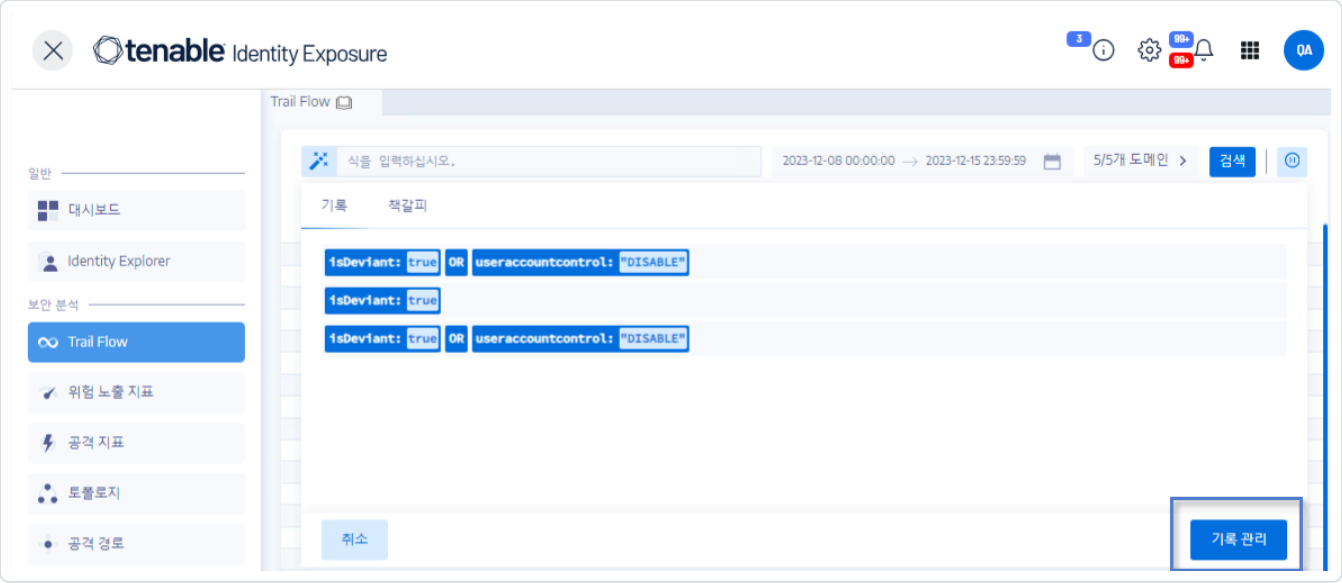
기록에서 쿼리 식을 사용하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자 안쪽을 클릭합니다.

   검색 상자 아래로 **기록**과 **책갈피** 탭이 표시됩니다.
3. **기록** 탭을 클릭합니다.

   쿼리 식 목록이 표시됩니다.
4. 클릭하여 사용할 쿼리 식을 선택합니다.

   Tenable Identity Exposure에서 쿼리 식을 로드하여 검색을 실행합니다.



쿼리 식 기록을 관리하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자 안쪽을 클릭합니다.

   검색 상자 아래로 **기록**과 **책갈피** 탭이 표시됩니다.

3. **기록** 탭을 클릭합니다.

   쿼리 식 목록이 표시됩니다.

4. **기록 관리**를 클릭합니다.

   기록 창이 열립니다.

5. 다음 중 작업을 수행합니다.

- 쿼리 식 검색:
  a. 검색 상자에 쿼리 식을 입력합니다.
  b. 캘린더 상자를 클릭하여 시작 날짜와 종료 날짜를 선택합니다.
  c. **검색**을 클릭합니다.
- 기록에서 쿼리 식을 삭제:
  - 🗑 아이콘을 클릭합니다.
- 기록에서 모든 쿼리 식을 지우기:
  a. **선택 항목 지우기**를 클릭합니다.

     메시지가 표시되어 삭제할 것인지 확인을 요청합니다.

  b. **확인**을 클릭합니다.

참고 항목

- Trail Flow를 수동으로 검색
- 마법사를 사용하여 Trail Flow 검색
- Trail Flow 쿼리 사용자 지정
- 책갈피 쿼리
- Trail Flow 사용 사례

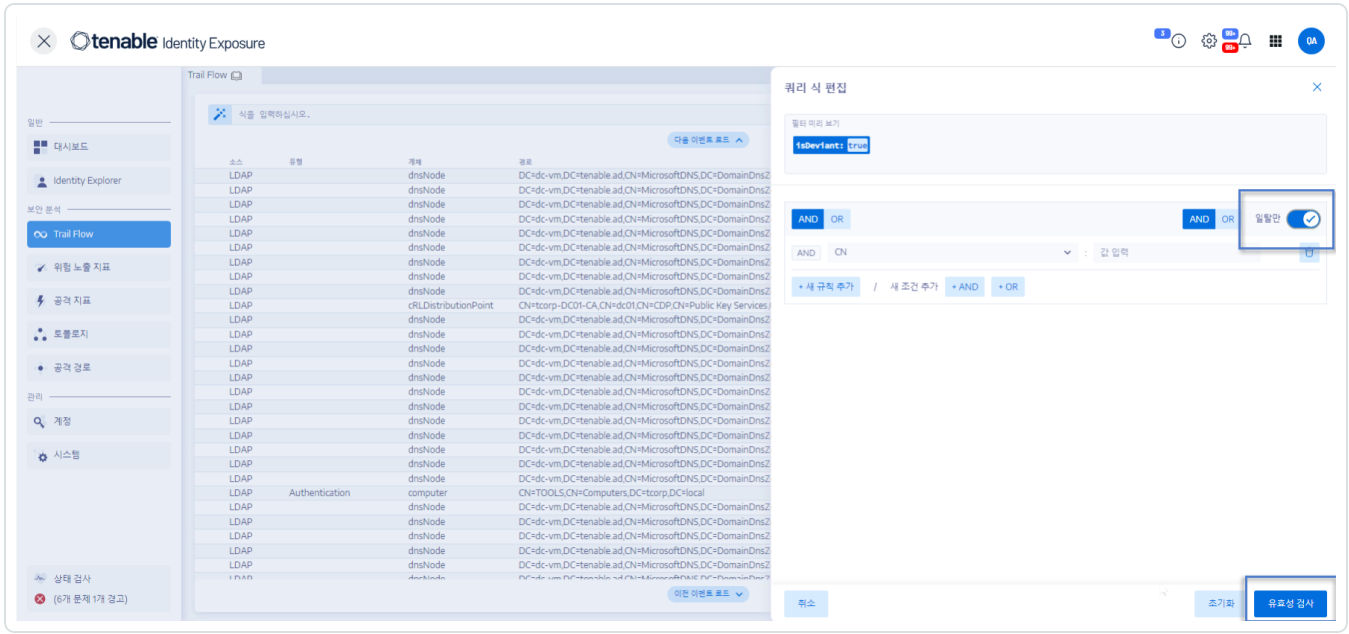
일탈 이벤트 표시

Trail Flow 표의 일탈 이벤트에만 초점을 맞출 수 있습니다.

일탈 이벤트만 표시하는 방법:

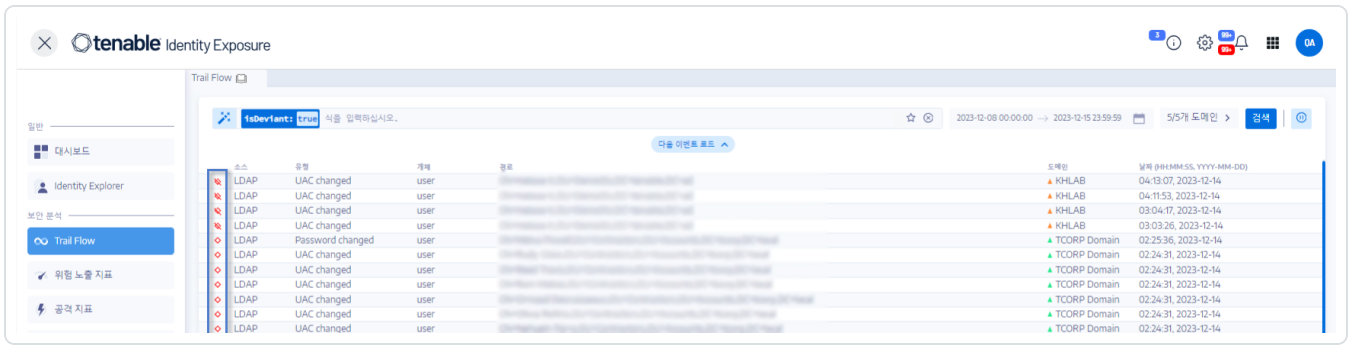
1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. 검색 상자 옆에 있는 아이콘을 클릭합니다.

   쿼리 식 편집 창이 시작됩니다.



3. **일탈만** 토글을 허용으로 클릭합니다.
4. **유효성 검사**를 클릭합니다.

   Tenable Identity Exposure에서 Trail Flow 표를 소스 옆에 빨간색 다이아몬드가 있는 이벤트 목록으로 업데이트합니다.



여기에서:

- Trail Flow가 Tenable Identity Exposure 보안 프로필에서 일탈을 탐지했습니다.
- Trail Flow가 다른 보안 프로필에서 일탈을 탐지했습니다.
- 변경 사항으로 일탈을 해결되었음을 나타냅니다.

이벤트 세부 정보

Tenable Identity Exposure의 Trail Flow는 Active Directory(AD)에 영향을 미치는 각각의 이벤트에 관한 상세한 정보를 제공합니다. 특정 이벤트의 세부 정보를 이용하면 기술적 정보를 검토하고 위험 노출 지표(IoE)의 심각도 수준에 따라 필요한 수정 조치를 취할 수 있습니다.

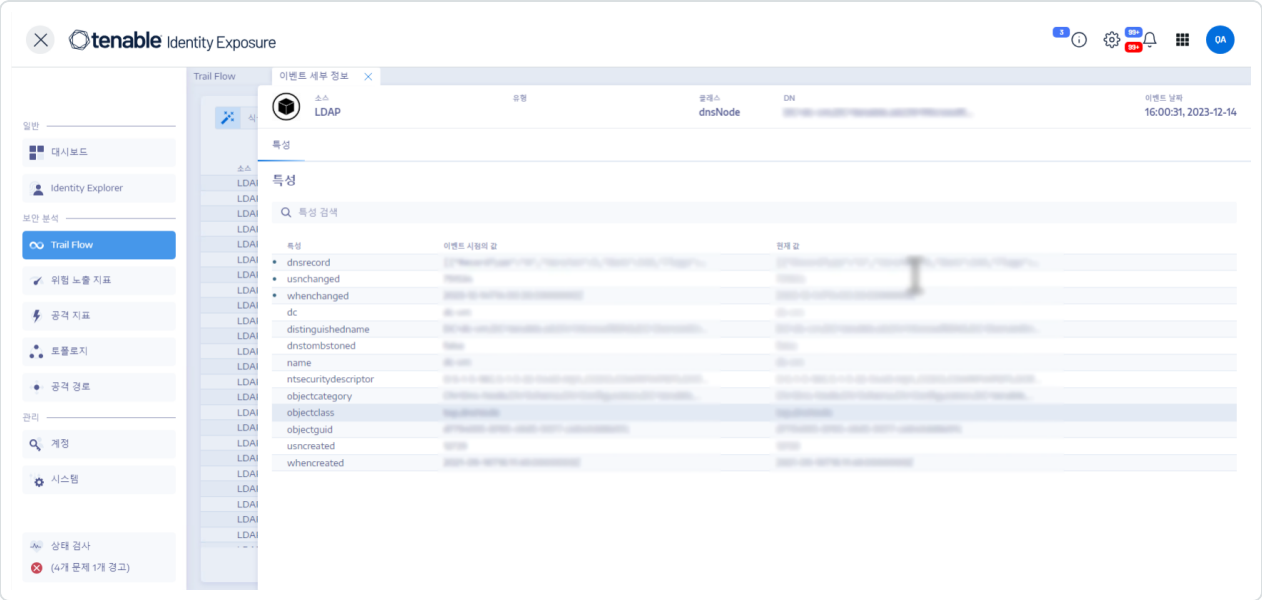
이벤트 세부 정보를 보는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. Trail Flow 표에서 항목을 클릭하여 선택합니다.

   이벤트 세부 정보 창이 열립니다.

IoE, 이벤트 및 일탈 개체

- **위험 노출 지표**(IoE)는 AD에 영향을 미치는 위협을 설명합니다. Tenable Identity Exposure의 IoE는 실시간으로 이벤트를 수신하여 보안 수준을 평가합니다. IoE에는 여러 개의 기술 취약성이 포함될 수 있습니다. IoE는 탐지된 취약성, 연결된 일탈 개체 및 수정 조치를 위한 권장 사항에 관한 정보를 제공합니다.
- **이벤트**는 AD에 표시되는 보안과 관련한 변경 사항을 나타냅니다. 비밀번호 변경, 사용자 만들기, 새로운 또는 수정된 GPO, 또는 새로 위임된 권한 등일 수 있습니다. 한 이벤트로 인해 IoE의 규정 준수 상태가 준수에서 미준수로 바뀔 수 있습니다.
- **일탈 개체**는 기술적 요소이며, 그 자체로 또는 다른 일탈 개체와 연결되어 IoE의 공격 벡터가 작동할 수 있게 합니다.



특성 표

특성 표에는 다음과 같은 열이 포함됩니다.

열	설명
특성	Trail Flow 표에서 선택한 이벤트와 연결된 AD 개체의 특성을 나타냅니다. 특성은 개체의 특징을 설명합니다. 여러 개의 특성이 AD 개체 하나를 설명할 수 있습니다.
이벤트 시점의 값	이벤트가 발생한 시점의 특성을 나타냅니다.
현재 값	사용자가 조회하는 시점에 AD에서 특성의 값을 나타냅니다.

팁: 이벤트가 발생하기 전의 특성 값을 표시하려면 왼쪽에 있는 파란색 점을 가리킵니다(있는 경우).

특성을 검색하는 방법:

- **이벤트 세부 정보** 창에서 검색 상자에 문자열을 입력합니다.

  Tenable Identity Exposure에서 검색 문자열과 일치하는 특성으로 목록의 범위를 좁힙니다.

자세한 내용은 특성 변경 사항을 참조하십시오.

일탈

Trail Flow의 이벤트에 일탈이 포함된 경우, 이벤트 세부 정보 창에도 이것이 표시되어 문제의 출처로 드릴다운할 수 있습니다.

일탈을 표시하는 방법:

1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. Trail Flow 표에서 항목을 클릭하여 선택합니다.

   이벤트 세부 정보 창이 열립니다.
3. **일탈** 탭을 선택합니다.

   Tenable Identity Exposure에서 일탈과 이들을 트리거한 IoE 목록을 표시합니다.

IoE 세부 정보로 드릴다운하는 방법:

1. **일탈** 탭에서 일탈 이유 아래에 있는 IoE 타일을 클릭합니다.

   지표 세부 정보 창이 열리고 일탈 개체 목록 및 다음과 같은 정보가 포함됩니다.

   - IoE의 이름
   - IoE 심각도(위험, 높음, 중간, 낮음)
   - IoE 상태
   - 최신 탐지의 타임스탬프
2. 다음 탭 중 하나를 클릭합니다.
   - **정보** - IoE의 내부 및 외부 리소스를 포함합니다.
   - **취약성 세부 정보** - AD에서 탐지된 약점의 설명을 제공합니다.

- **일탈 개체** - 기술적 세부 정보와 개체를 필터링할 검색 상자를 포함합니다.
- **권장 사항** - 문제를 해결하는 방법에 관한 팁을 포함합니다.

특성 변경 사항

특성의 값이 변경되면 Trail Flow의 해당 **특성** 열 앞에 파란색 점이 표시됩니다.

특성 변경을 표시하는 방법:

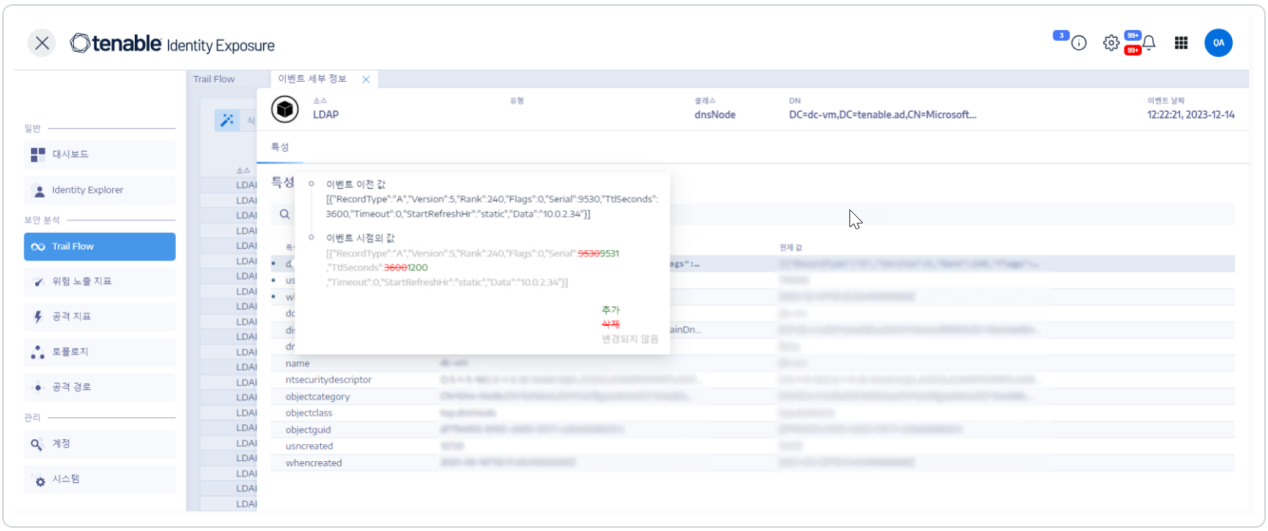
1. Tenable Identity Exposure에서 왼쪽의 탐색 모음에 있는 **Trail Flow**를 클릭합니다.

   이벤트 목록을 포함하는 **Trail Flow** 페이지가 열립니다.

2. 이벤트 줄 앞에 있는 파란색 점을 가리키면 변경 사항이 표시됩니다.

   이벤트 시점의 값 레이블 색은 특성에 적용된 변경 사항에 따라 다릅니다.

   - 녹색 - **추가**
   - 빨간색 - **삭제**
   - 회색 - **변경되지 않음**



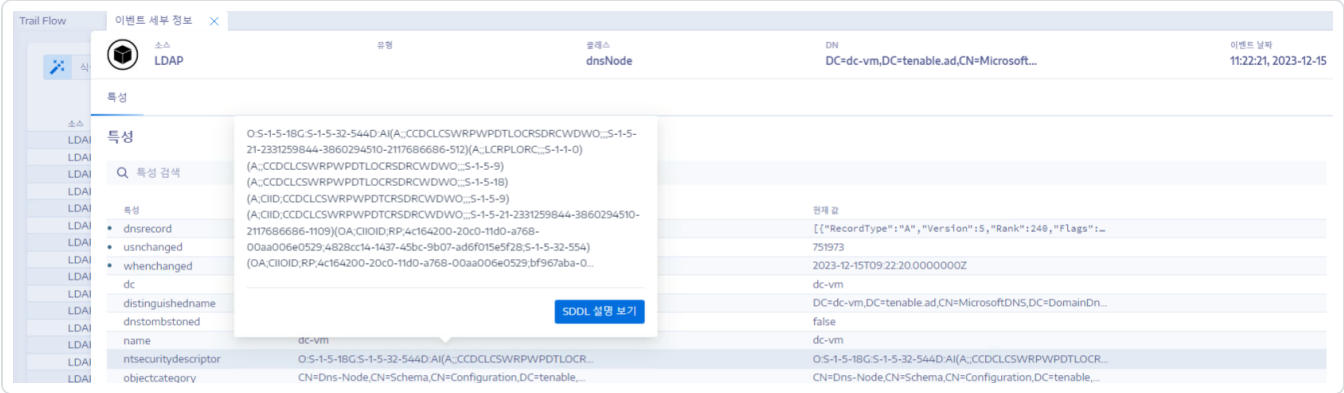
"ntsecuritydescriptor" 특성

보안 설명자는 AD 개체에 관한 보안 정보(예: 소유권 및 권한 등)를 포함하는 데이터 구조입니다. 자세한 내용은 Microsoft의 온라인 설명서를 참조하십시오.

개체 보안 설명자의 세부 정보를 표시하는 방법:

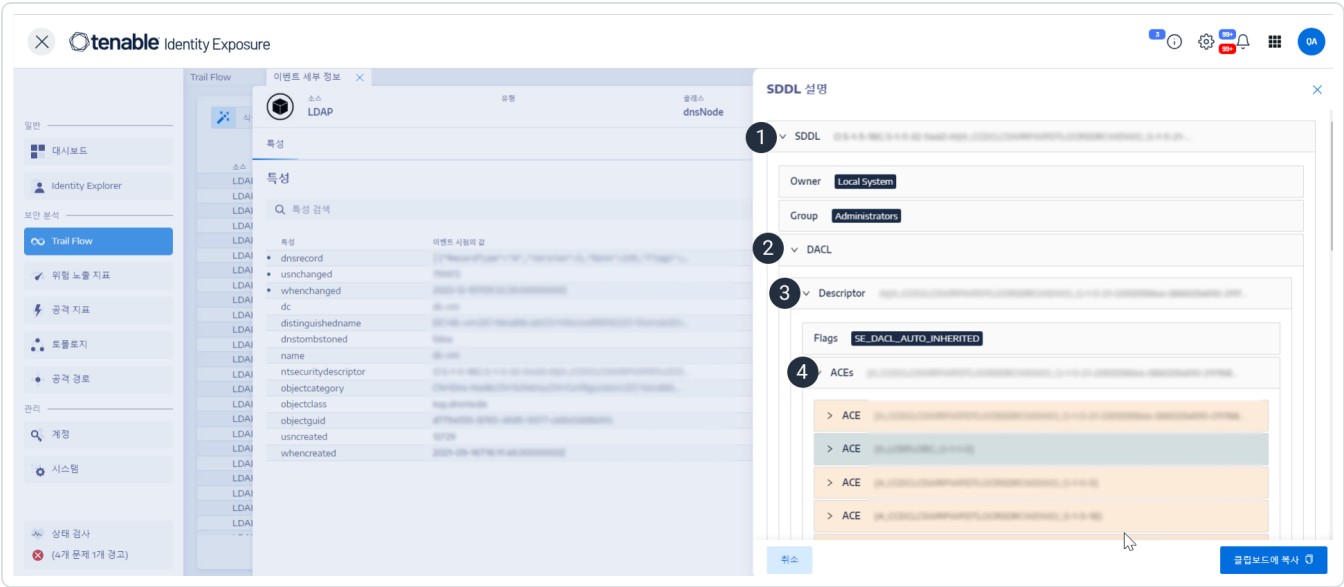
1. Tenable Identity Exposure에서 **Trail Flow**를 클릭하여 Trail Flow 페이지를 엽니다.
2. Trail Flow 표에서 항목을 클릭하여 선택합니다.

   이벤트 세부 정보 창이 열립니다.
3. `ntsecuritydescriptor` 특성 항목(이벤트 시점의 값 또는 현재 값 열)**을 가리킵니다.



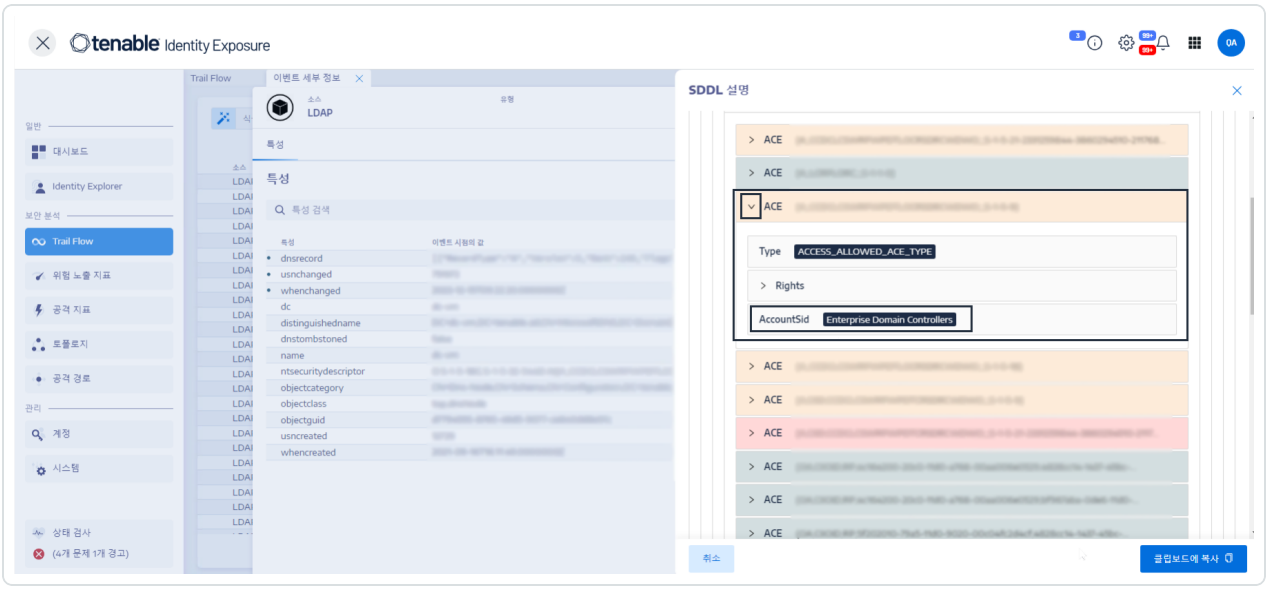
4. **SDDL 설명 보기**를 클릭합니다.

   SDDL 설명 창이 열립니다.
5. SDDL (1), DACL (2) 및 설명자 (3) 왼쪽의 화살표를 클릭하면 설명이 펼쳐집니다.



6. 색으로 강조 표시된 액세스 제어 항목(ACE)(4)으로 이동하여 해당 개체의 액세스 권한을 표시합니다. 색상 코드는 다음을 나타냅니다.

- **빨간색** - 사용자에게 위험한 권한이 할당되어 있으며 개체에 대한 액세스 권한이 있으면 안 됩니다.
- **주황색** - 권한 있는 사용자에게 위험한 권한이 할당되어 있지만 이들에게는 보통 이런 유형의 권한이 있습니다(예: 도메인 관리자).
- **녹색** - 위험한 권한이 없습니다.



7. SDDL 설명을 복사하려면 **클립보드에 복사**를 클릭합니다.

Trail Flow 사용 사례

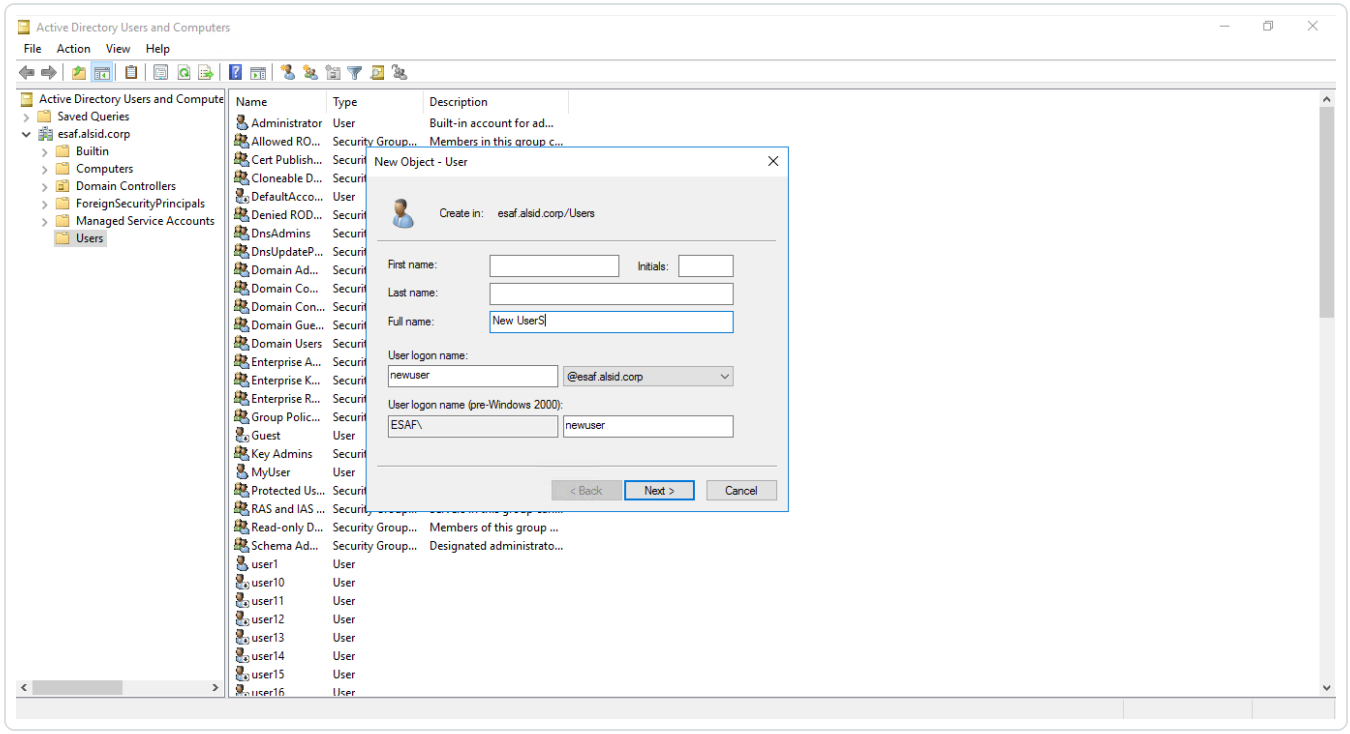
Trail Flow 동작을 이해하기 위해 두 가지 예를 들어 사용자가 Active Directory(AD) 인터페이스에서 수행하는 작업이 Trail Flow 페이지에 어떻게 반영되는지 나타내었습니다.

각각의 예는 관리자 쪽의 데이터(AD 인터페이스)와 최종 사용자 데이터(Tenable Identity Exposure)를 비교합니다. AD에서 작업을 수행하기 위해 애플리케이션, API 또는 서비스를 사용해도 Trail Flow에서의 결과는 똑같습니다.

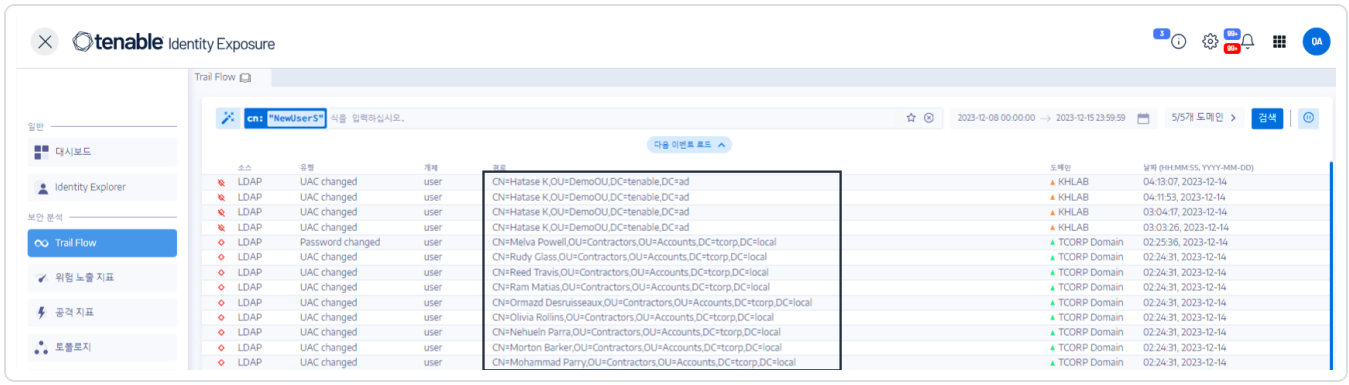
참고: 이러한 예는 전체적인 것이 아니며 가능한 모든 상황을 다룰 수는 없습니다.

새 AD 사용자 계정을 만들면 Trail Flow에는 무슨 일이 일어납니까?

- 관리자 쪽에서 새 사용자 계정에 대한 다양한 정보를 입력합니다.

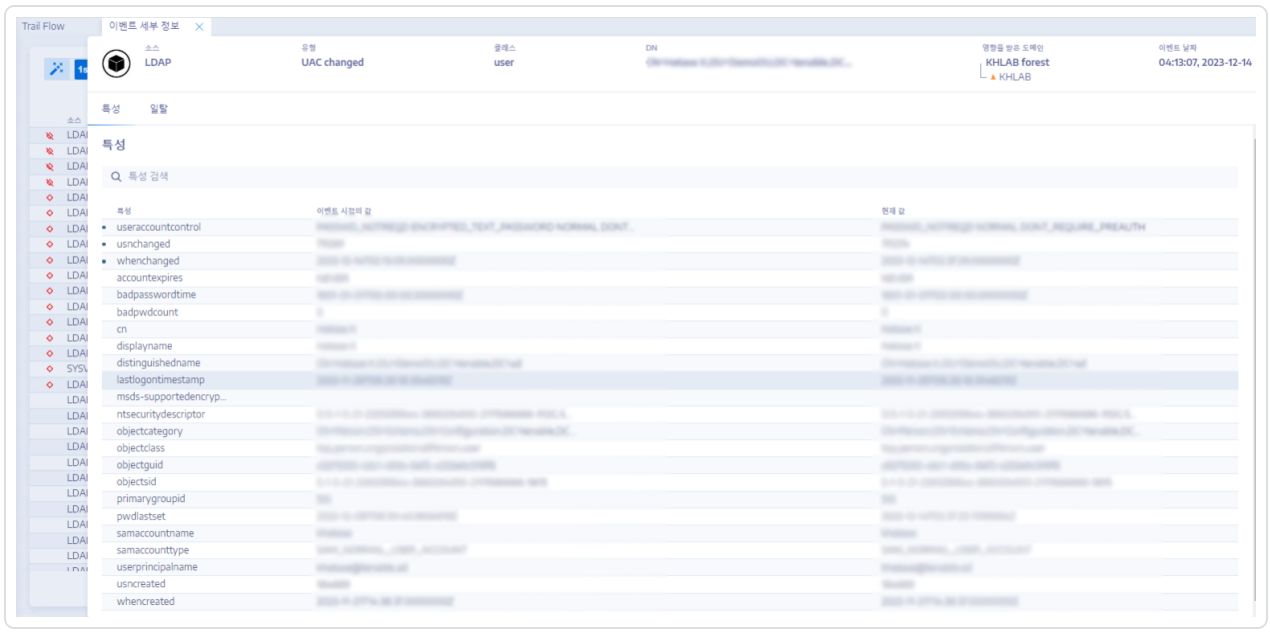


- 최종 사용자 쪽에서 Tenable Identity Exposure에서 **Trail Flow** 페이지를 업데이트합니다. *새 개체*를 나타내는 **유형** 열을 참조하십시오.



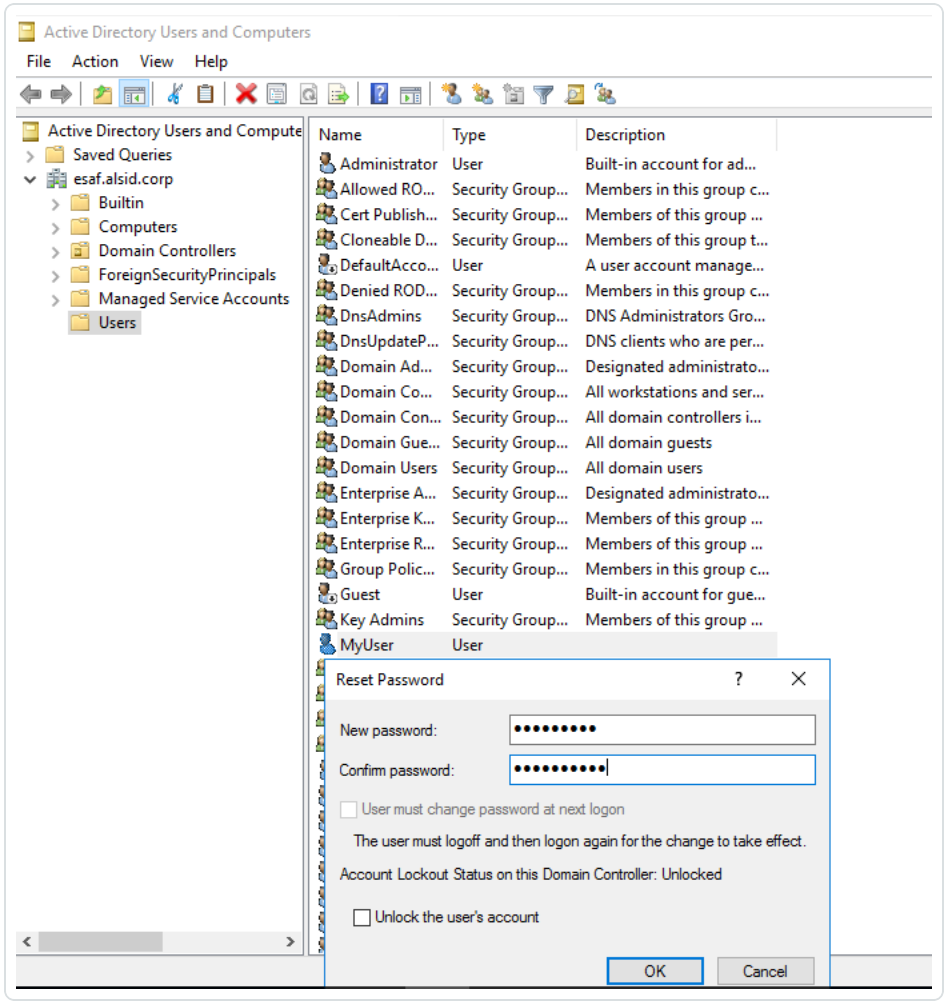
- **이벤트 세부 정보** 페이지에도 이 변경 사항이 반영됩니다. 특성 이름 왼쪽에 파란색 점이 있으면 업데이트가 발생했음을 나타냅니다.

  특성에 대한 자세한 내용은 이벤트 세부 정보 보기를 참조하십시오.

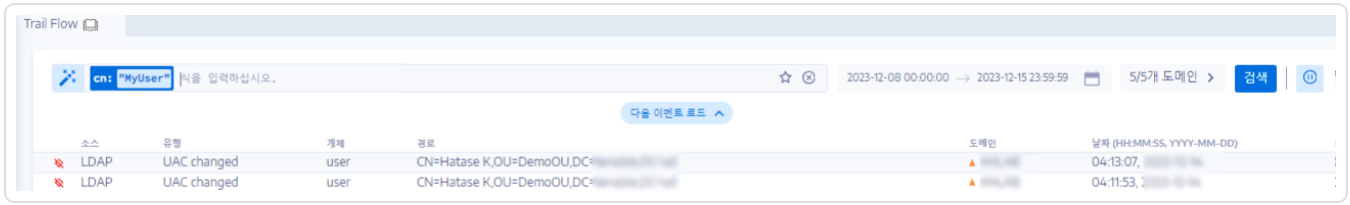


AD 사용자의 비밀번호를 변경하면 Trail Flow에는 무엇이 발생합니까?

- 관리자 쪽에서 사용자의 비밀번호를 초기화하기 위한 다양한 정보를 입력합니다.

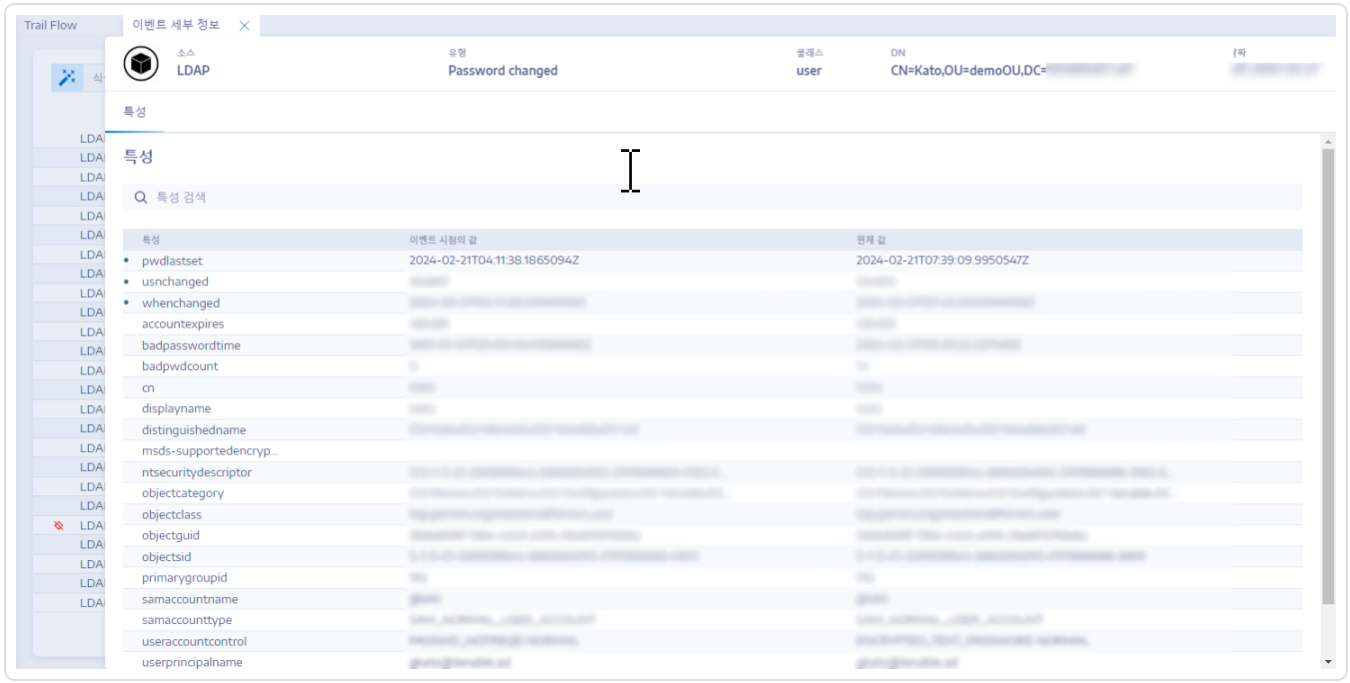


- 최종 사용자 쪽에서 Tenable Identity Exposure에서 **Trail Flow** 페이지를 업데이트합니다. **유형** 열에 "비밀번호 변경"이 표시됩니다.



- **이벤트 세부 정보** 페이지에도 whenchanged 특성 왼쪽에 파란색 점으로 이 변경 사항이 반영됩니다.

특성에 대한 자세한 내용은 이벤트 세부 정보을(를) 참조하십시오.



참고 항목

- Trail Flow를 수동으로 검색
- 마법사를 사용하여 Trail Flow 검색
- Trail Flow 쿼리 사용자 지정
- 책갈피 쿼리
- 쿼리 기록

위험 노출 지표

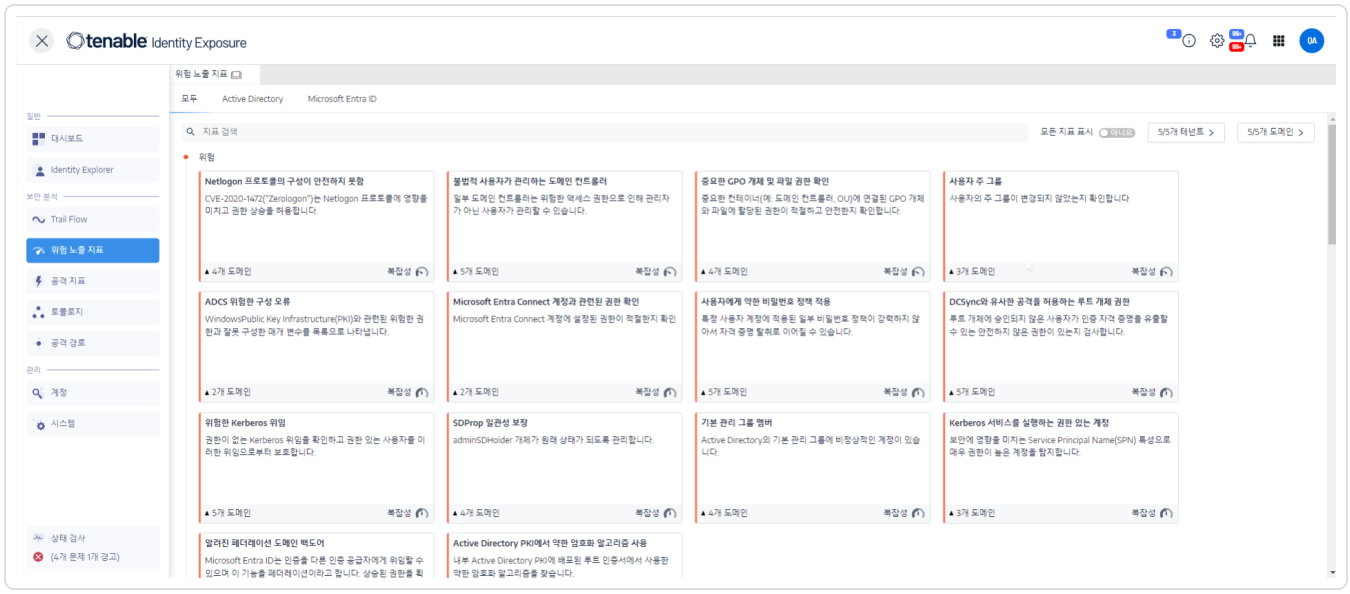
Tenable Identity Exposure에서는 위험 노출 지표(IoE)를 통해 AD 인프라의 보안 성숙도를 측정하고 모니터링 및 분석하는 이벤트 흐름에 심각도 수준을 할당합니다. Tenable Identity Exposure는 보안 저하를 탐지하면 알림을 트리거합니다.

IoE를 표시하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭합니다.

   위험 노출 지표 창이 시작됩니다. 기본적으로 Tenable Identity Exposure에서는 일탈을 포함한 IoE만 표시합니다.

2. (선택 사항) 모든 IoE를 표시하려면 **모든 지표 표시** 토글을 클릭하여 **예**로 설정합니다.



IoE를 검색하는 방법:

1. **위험 노출 지표** 페이지 위의 검색 상자에 문자열을 입력합니다. IoE와 관련된 용어가 될 수 있습니다(예: 비밀번호, 사용자, 로그온 등).

2. Enter 키를 누릅니다.

   IoE 페이지가 검색어와 관련된 지표로 업데이트됩니다.

특정 포리스트 또는 도메인에 대하여 IoE를 필터링하는 방법:

1. **n/n 도메인**을 클릭합니다.

   포리스트 및 도메인 창이 열립니다.

2. 포리스트 또는 도메인을 선택합니다.
3. **선택 항목 필터링**을 클릭합니다.

심각도 수준

심각도 수준을 이용하면 탐지된 취약성의 심각도를 평가하고 수정 작업의 우선 순위를 정할 수 있습니다.

위험 노출 지표 창에 IoE가 다음과 같이 표시됩니다.

- 색상 코드를 사용하여 심각도 기준별로 표시합니다.
- 세로 방향으로 - 가장 심각한 것에서 가장 덜 심각한 것 순서대로(최고 우선 순위가 빨간색 및 최저 우선 순위가 파란색).
- 가로 방향으로 - 가장 복잡한 것에서 가장 덜 복잡한 것 순서대로. Tenable Identity Exposure에서 복잡도 지표를 동적으로 계산하여 일탈 IoE를 수정하는 작업의 난이도 수준을 나타냅니다.

심각도	설명
위험 - 빨간색	특정 권한이 없는 사용자에 의한 Active Directory의 공격과 침해를 예방하는 방법을 보여줍니다.
높음 - 주황색	자격 증명 도용 또는 보안 우회로 이어지는 악용 이후 기술이나 위험하려면 체이닝이 필요한 악용 기술을 다룹니다.
중간 - 노란색	Active Directory 인프라에 약간의 위험이 있음을 나타냅니다.
낮음 - 파란색	보안 관행이 양호함을 표시합니다. 특정 비즈니스 컨텍스트에 따라 AD 보안에 영향을 미치지 않을 수도 있는 영향이 낮은 일탈을 허용할 수도 있습니다. 이러한 일탈은 관리자가 비활성 계정을 활성화하는 것과 같이 오류를 발생시키는 경우에만 AD에 영향을 미칩니다.

참고 항목

- 위험 노출 지표 세부 정보
- 일탈 개체
- 일탈 개체 검색
- 일탈 개체 무시
- 원인으로 지목된 특성

위험 노출 지표 세부 정보

특정 위험 노출 지표의 세부 정보를 보면 탐지된 취약성, 관련된 일탈 개체에 관한 기술적 정보와 수정을 위한 권장 사항을 검토할 수 있습니다.

위험 노출 지표 세부 정보를 표시하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭합니다.

   위험 노출 지표 창이 시작됩니다. 기본적으로 Tenable Identity Exposure에서는 일탈을 포함한 IoE만 표시합니다.

2. (선택 사항) 모든 IoE를 표시하려면 **모든 지표 표시** 토글을 클릭하여 **예**로 설정합니다.

3. 페이지에서 **위험 노출 지표** 타일을 클릭합니다.

   지표 세부 정보 창이 열립니다.

   상단에 **지표 세부 정보** 창은 Trail Flow 표에 이미 제공된 정보를 요약합니다.

   - IoE의 **이름**.
   - **심각도** 수준(위험, 높음, 중간 또는 낮음).
   - 규정 준수 **상태**는 Tenable Identity Exposure에서 실행한 마지막 분석 결과를 기반으로 합니다.
   - **최신 탐지**는 Tenable Identity Exposure에서 분석을 실행한 마지막 시간.

4. IoE에 대한 더 자세한 정보는 다음 탭을 클릭하십시오.

탭	설명
정보	다음과 같은 IoE에 대한 내부 및 외부 리소스를 포함합니다. • 종합 요약 - 적절한 결정을 내리는 데 도움이 되는 문제에 대한 개요. • 문서 - IoE에 대한 외부 리소스에 링크. • 공격자에게 알려진 도구 - 해킹 도구 이름. • 영향을 받는 도메인의 트리 구조.
취약성 세부 정보	AD에서 탐지된 약점에 대한 설명 및 수정 조치를 취하지 않는 경우 Active Directory(AD)에 미치는 위험을 설명합니다.
일탈 개체	일탈 개체는 AD의 약점 또는 잠재적인 위험한 동작을 공개합니다. 일탈 개체에 필터를 적용하여 중대한 문제를 정확하게 찾을 수 있습니다. IoE 상태가 규정 준수가 아니고 일탈 개체를 포함하는 경우, 수정 조치를 취하여 Tenable Identity Exposure에서 탐지한 보안 결함을 수정할 수 있습니다. 자세한 내용은 일탈 개체을 참조하십시오.
권장 사항	보안 요구 사항에 따라 규정 준수를 복원하고 AD 보안을 개선하는 방법에 관한 팁: • 종합 요약에서는 Tenable Identity Exposure에서 제안한 해법 개요를 확인할 수 있습니다. • 세부 정보 하위 섹션에는 해당 작업 계획을 구현하는 방법에 관한 조언을 제공하며 관리자가 AD 인프라에 필요한 변경을 시작하도록 지원합니다. • 문서 하위 섹션에서는 제안된 해법 또는 위협에 관한 외부 리소스로 이동하는 링크를 제공합니다.

참고 항목

- 위험 노출 지표
- 일탈 개체
- 일탈 개체 검색
- 일탈 개체 무시
- 원인으로 지목된 특성

일탈 개체

Tenable Identity Exposure의 위험 노출 지표(IoE)는 Active Directory(AD)의 약점 또는 잠재적으로 위험한 동작을 드러낼 수 있는 일탈 개체에 플래그를 지정할 수 있습니다. 이와 같은 일탈 개체에 집중하면 중요한 문제를 정확하게 찾아내어 수정하는 데 도움이 됩니다. 다음 작업을 수행할 수 있습니다.

- 일탈 개체를 검색합니다.
- 일정한 기간 동안 일탈 개체를 무시합니다.
- 일탈 개체를 검색할 포리스트와 도메인을 선택합니다.
- IoE에 영향을 미치는 원인으로 지목된 특성에 대한 설명을 가져옵니다.
- 모든 일탈 개체를 표시하는 보고서를 다운로드합니다.

일탈 개체를 표시하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭합니다.

   위험 노출 지표 페이지가 시작됩니다. 기본적으로 Tenable Identity Exposure에서는 일탈을 포함한 IoE만 표시합니다.

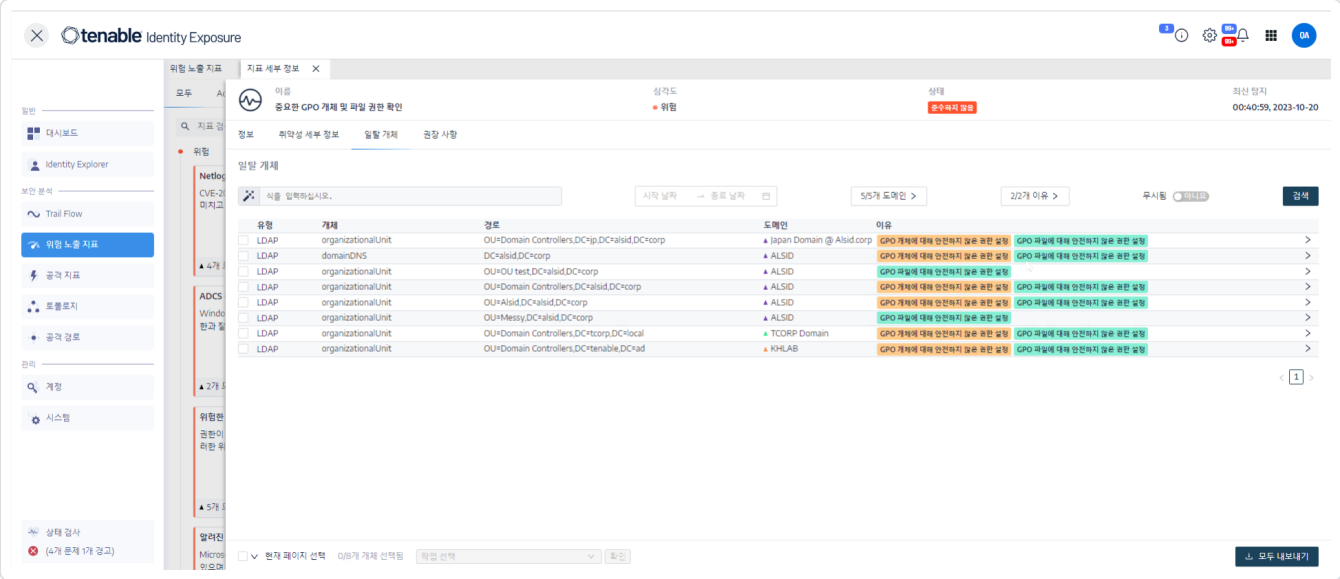
2. 페이지에서 **위험 노출 지표** 타일을 클릭합니다.

   지표 세부 정보 창이 열립니다.

3. **일탈 개체** 탭을 클릭합니다.

   IoE와 연결된 일탈 개체 목록이 표시됩니다.



일탈 개체 표에는 다음과 같은 정보가 포함됩니다.

- **유형** - AD에서 발생한 각종 보안 관련 변경 사항의 출처를 나타냅니다(LDAP 또는 SMB 프로토콜).
- **개체** - AD 개체와 연결된 클래스 또는 파일 확장자를 나타냅니다.
- **경로** - AD 개체로 이동하는 전체 경로를 나타내어 AD에서 이 개체의 고유한 위치를 식별할 수 있습니다.
- **도메인** - AD의 변경 사항의 출처가 되는 도메인을 나타냅니다.
- **이유** - 일탈 개체에 영향을 미치는 원인으로 지목된 특성을 나열합니다.

일탈 개체 보고서를 내보내는 방법:

1. **일탈 개체** 페이지의 아래에서 **모두 내보내기**를 클릭합니다.

   일탈 개체 내보내기 창이 표시됩니다.

2. **내보내기 형식** 상자에서 드롭다운 화살표를 클릭하여 형식을 선택합니다.
3. **모두 내보내기**를 클릭합니다.

   Tenable Identity Exposure에서 일탈 개체 보고서를 사용자 컴퓨터에 다운로드합니다.

참고 항목

- 위험 노출 지표
- 위험 노출 지표 세부 정보
- 일탈 개체 검색
- 일탈 개체 무시
- 원인으로 지목된 특성

일탈 개체 검색

일탈 개체를 수동으로 검색하거나 마법사를 사용해 검색할 수 있습니다.

마법사 검색

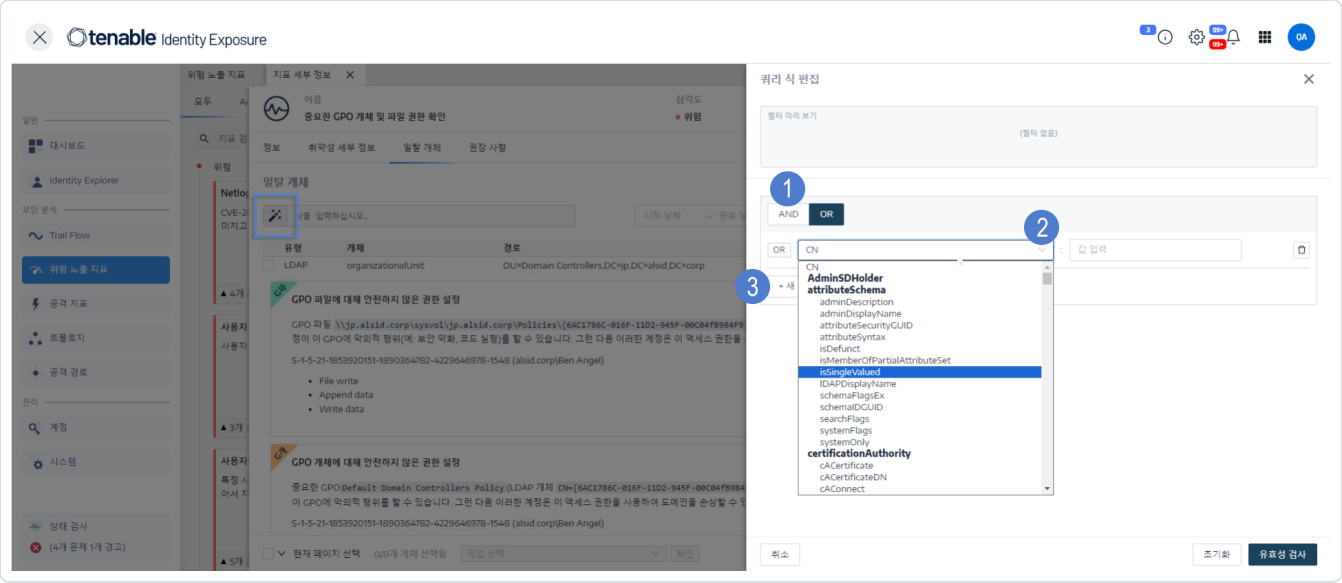
검색 마법사를 사용하면 쿼리 식을 만들 수 있습니다.

- 검색 상자에서 식을 자주 사용하는 경우, 책갈피 목록에 추가하여 나중에 사용할 수 있습니다.
- 검색 상자에 식을 입력하면 다시 사용할 수 있도록 Tenable Identity Exposure에서 이 식을 기록 창에 저장합니다.

마법사를 사용해 일탈 개체를 검색하는 방법:

1. 일탈 개체의 목록을 표시합니다.
2. 아이콘을 클릭합니다.

   쿼리 식 편집 창이 시작됩니다.



3. 패널에서 쿼리 식을 정의하려면 **AND** 또는 **OR** 연산자 버튼(1)을 클릭하여 첫 번째 조건에 적용합니다.
4. 드롭다운 메뉴에서 특성을 하나 선택한 다음 그 값(2)을 입력합니다.
5. 다음 중 작업을 수행합니다.

- 특성을 추가하려면 **+ 새 규칙 추가**(3)를 클릭합니다.
- 또 다른 조건을 추가하려면 **새 조건 추가+AND** 또는 **+OR** 연산자를 클릭합니다. 드롭다운 메뉴에서 특성을 선택하고 그 값을 입력합니다.
- 검색을 일탈 개체로 제한하려면 **일탈만** 토글을 허용으로 클릭합니다. **+AND** 또는 **+OR** 연산자를 선택하여 해당 조건을 쿼리에 추가합니다.
- 조건 또는 규칙을 삭제하려면 🗑 아이콘을 클릭합니다.

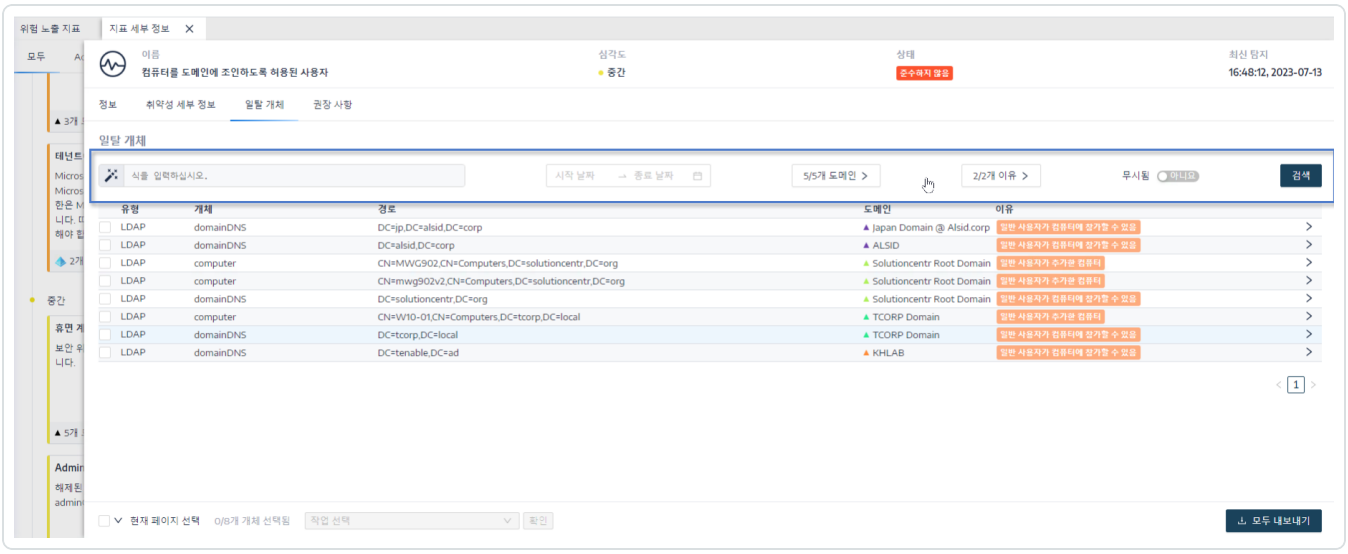
6. **유효성 검사**를 클릭하여 검색을 실행하거나 **초기화**하여 쿼리 식을 수정합니다.

수동 검색

특정 문자열 또는 패턴과 일치하는 일탈 개체를 필터링하려면 검색 상자에 식을 입력하여 부울 연산자 *, **AND** 및 **OR**를 사용해 결과를 상세 검색하면 됩니다. **OR** 문을 괄호로 감싸면 검색 우선 순위를 수정할 수 있습니다. 검색으로 Active Directory 특성에서 특정 값을 찾습니다. Trail Flow를 수동으로 검색하는 방법:

수동으로 일탈 개체를 검색하는 방법:

1. 일탈 개체의 목록을 표시합니다.



2. 검색 상자에 쿼리 식을 입력합니다.
3. 검색 결과를 다음과 같이 필터링할 수 있습니다.

- **캘린더** 상자를 클릭하여 시작 날짜와 종료 날짜를 선택합니다.
- **n/n 도메인**을 클릭하여 포리스트와 도메인을 선택합니다.

4. **검색**을 클릭합니다.

   Tenable Identity Exposure에서 검색 기준과 일치하는 결과로 목록을 업데이트합니다.

문법 및 구문

수동 쿼리 식은 다음과 같은 문법과 구문을 사용합니다.

- 문법: `EXPRESSION [OPERATOR EXPRESSION]*`
- 구문: `__KEY__ __SELECTOR__ __VALUE__`

  여기에서:

  - `__KEY__`는 검색할 AD 개체 특성을 가리킵니다(예: `CN`, `userAccountControl`, `members` 등).
  - `__SELECTOR__`는 연산자(`:`, >, <, >=, <=)를 가리킵니다.
  - `__VALUE__`는 검색할 값을 가리킵니다.

    특정 콘텐츠를 찾는 데 이외의 키를 사용할 수 있습니다.
  - `isDeviant`는 일탈을 만든 이벤트를 찾습니다.

AND 및 **OR** 연산자를 사용하면 여러 개의 Trail Flow 쿼리 식을 조합할 수 있습니다.

예:

- 공통 이름 속성으로 `alice` 문자열을 포함하는 모든 객체를 찾기: `cn:"alice"`
- 공통 이름 특성에 문자열 `alice`를 포함하고 특정 일탈을 만든 모든 개체 찾기: `isDeviant:"true" and cn:"alice"`
- 이름이 Default Domain Policy인 GPO 찾기: `objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- SID에 S-1-5-21을 포함하는 모든 비활성화된 계정 찾기: `userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`

- Sysvol에서 모든 `script.ini` 파일 찾기: `globalpath:"sysvol" and types:"SCRIPTSini"`

  > **참고**: 여기서 `types`는 열 머리글이 아니라 개체 속성을 나타냅니다.

참고 항목

- 위험 노출 지표
- 위험 노출 지표 세부 정보
- 일탈 개체
- 일탈 개체 무시
- 원인으로 지목된 특성

일탈 개체 무시

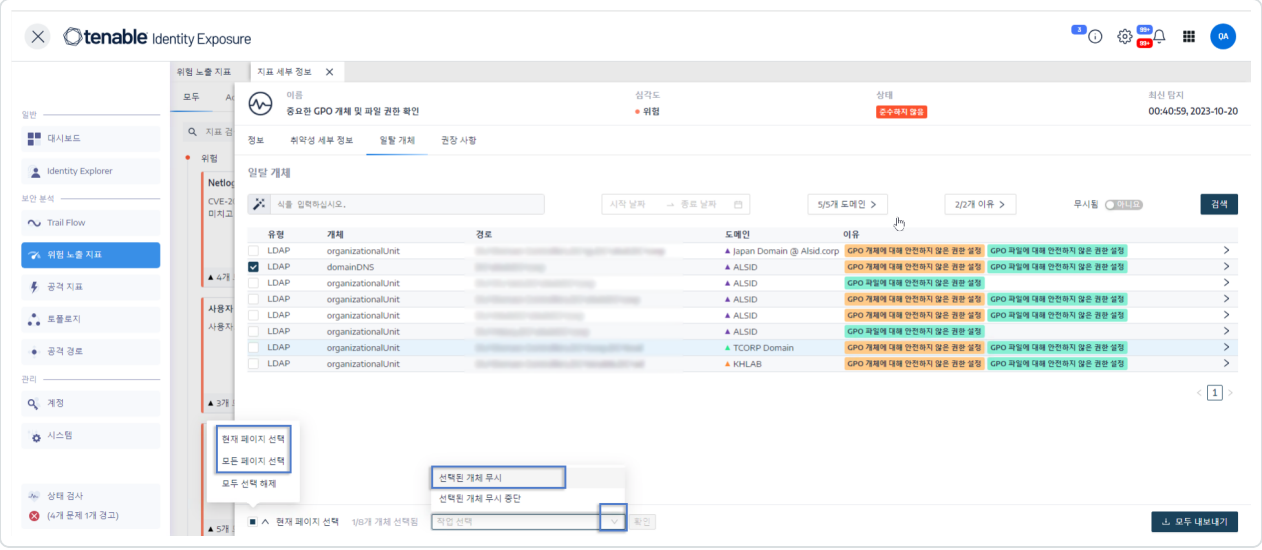
조사 또는 보고 목적으로 화면이 복잡해지는 것을 방지하려면, Tenable Identity Exposure에서 선택한 기간 동안 몇몇 일탈 개체를 무시하도록 적용하여 일부 개체를 필터링할 수 있습니다. 일탈 개체는 하나 또는 여러 개 무시하기로 선택할 수 있습니다. 사용자 지정 필터를 바로 적용하거나 필터를 활성화할 기간을 지정할 수 있습니다.

참고: 개체를 무시해도 Tenable Identity Exposure에서 해결되는 것은 아닙니다.

일탈 개체를 무시하는 방법:

1. Tenable Identity Exposure에서 일탈 개체 목록을 표시합니다.
2. 무시할 일탈 개체 앞에 있는 확인란을 선택합니다.
3. 선택 사항으로, 무시할 일탈 개체를 필터링할 수도 있습니다.
    - **캘린더** 상자를 클릭하여 시작 날짜와 종료 날짜를 선택합니다.
    - **n/n 도메인**을 클릭하여 포리스트와 도메인을 선택합니다.

팁: 더 빨리 선택하려면 **모든 페이지 선택** 또는 페이지 아래에 있는 **현재 페이지 선택** 상자에 체크 표시하면 됩니다.



4. 페이지 아래의 드롭다운 목록에서 **선택한 개체 무시**를 선택합니다.
5. **확인**을 클릭합니다.

선택한 개체 무시 창이 표시됩니다.

6. **무시할 기한** 상자를 클릭하여 캘린더를 표시하고 Tenable Identity Exposure에서 해당 일탈 개체를 무시할 기한 날짜를 선택합니다.
7. **확인**을 클릭합니다.

   Tenable Identity Exposure에서 확인 메시지를 표시하고 남은 일탈 개체 목록을 업데이트합니다.

무시한 일탈 개체를 표시하는 방법:

1. **무시** 토글을 클릭하여 **예**로 설정합니다.
2. 페이지 아래에 있는 **모든 페이지 선택**을 클릭합니다.
3. 드롭다운 목록에서 **선택된 개체 무시 중단**을 선택합니다.
4. **확인**을 클릭합니다.

   확인 페이지가 표시됩니다.
5. **확인**을 클릭하여 변경 사항을 확인합니다.

   Tenable Identity Exposure에서 무시된 일탈 개체를 표시합니다.

참고 항목

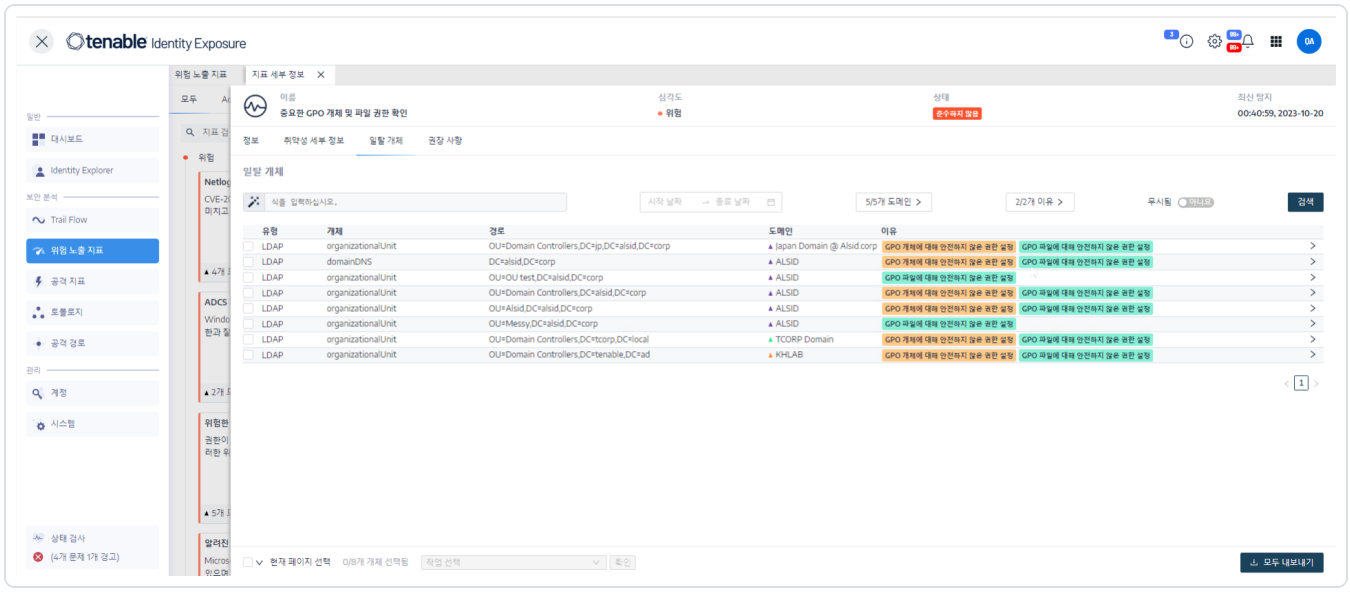
- 위험 노출 지표
- 위험 노출 지표 세부 정보
- 일탈 개체
- 일탈 개체 검색
- 원인으로 지목된 특성

원인으로 지목된 특성

Tenable Identity Exposure는 위험 노출 지표(IoE)의 일탈 개체를 트리거한 원인으로 지목된 특성을 표시하고 그 이유를 제시하여 일탈을 이해하고 수정하는 데 도움이 됩니다.

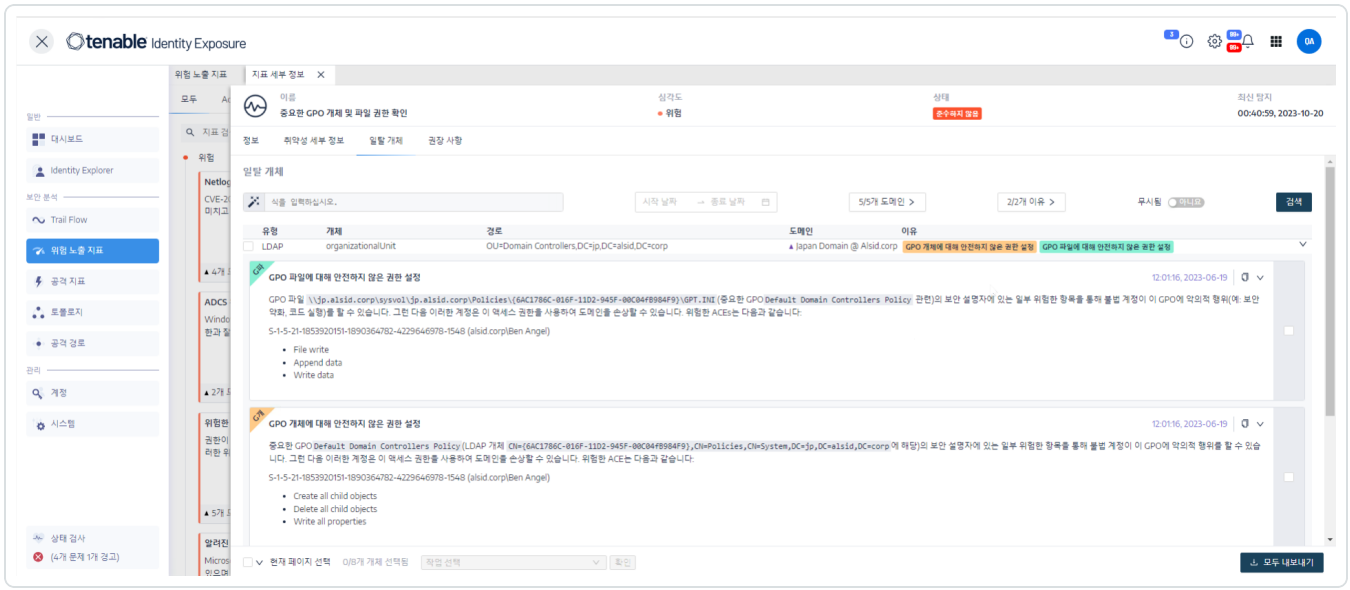
원인으로 지목된 특성을 확인하는 방법:

1. 일탈 개체의 목록을 표시합니다.



2. 일탈 개체 목록에서 한 항목을 클릭합니다.

   Tenable Identity Exposure에서 해당 일탈 개체의 원인으로 지목된 특성 목록을 표시합니다.



이 목록은 다음 정보를 포함합니다.

- **색으로 구분된 태그**는 이유가 여러 개인 경우, 다양한 이유를 구분합니다.
- 값:
  - ? - 누락된(빈) 특성 값(비정상 동작을 나타냄).
  - 이 일탈에 대하여 이용할 수 있는 설명 없음: 탐지가 버전 2.6으로 날짜를 거슬러 올라가며 Tenable Identity Exposure에서 더 이상 이 특성을 관리하지 않습니다.

원인으로 지목된 특성을 복사하는 방법:

- 특성을 선택하고 아이콘을 클릭합니다.

참고 항목

- 위험 노출 지표
- 위험 노출 지표 세부 정보
- 일탈 개체
- 일탈 개체 검색
- 일탈 개체 무시

RSoP 기반 위험 노출 지표

Tenable Identity Exposure에서는 일련의 RSoP(정책 결과 집합) 기반 위험 노출 지표(IoE)를 사용하여 다양한 측면의 보안 및 규정 준수를 평가하고 보장합니다. 이 섹션에서는 특정 RSoP IoE의 현재 동작에 관한 인사이트를 소개하고, Tenable Identity Exposure에서 계산과 관련한 성능 우려 사항을 어떻게 해결하는지 알려드립니다.

다음과 같은 RSoP 종속 IoE는 Tenable Identity Exposure의 보안 프레임워크에서 일정한 역할을 수행합니다.

- 권한 있는 사용자의 로그온 제한
- 위험한 중요한 권한
- 사용자에게 약한 비밀번호 정책 적용
- 랜섬웨어에 대한 강화 부족
- Netlogon 프로토콜의 안전하지 않은 구성

이러한 IoE는 필요에 따라 초기화되는 RSoP 결과 캐시에 좌우되며, 기존의 값에 의존하지 않고 요청 시 추가되는 값을 계산합니다. 이전에는 `AdObjects`를 변경하면 캐시 무효화가 트리거되어 IoE의 RSoP 실행 중에 재계산이 잦았습니다.

Tenable Identity Exposure에서는 RSoP 계산과 관련한 성능 저하 문제를 다음과 같이 해결합니다.

1. **더 이상 사용되지 않을 가능성이 있는 데이터로 실시간 IoE 분석** - RSoP에 의존하는 IoE의 계산(입력/출력 이벤트)은 발생하는 대로 실시간으로 실행되며, 이는 처리에 사용되는 데이터가 최신이 아니더라도 마찬가지입니다. RSoP 캐시를 무효화할 가능성이 있는 버퍼링된 이벤트는 특정 조건에 부합하여 예상되는 계산을 유발할 때까지 저장된 상태로 유지됩니다.
2. **예약된 RSoP 무효화** - 재계산 조건에 부합하면 시스템에서 무효화 프로세스 중에 버퍼링된 이벤트를 고려하여 해당 RSoP 캐시를 무효화합니다.
3. **최신 캐시를 사용하여 IoE 재실행** - 캐시 무효화 이후에는 버퍼링된 이벤트를 반영하여 캐시에서 가져온 최신 버전의 `AdObject`를 사용하여 IoE를 재실행합니다. Tenable Identity Exposure에서는 버퍼링된 이벤트마다 IoE를 각각 계산합니다.

이러한 이유로 인해, RSoP 결과에 의존하는 IoE의 최적화된 계산 기간 때문에 RSoP와 관련된 일탈의 계산 속도가 더 느려집니다.

Microsoft Entra ID 관련 위험 노출 지표

Microsoft Entra ID 전용 위험 노출 지표

Tenable Identity Exposure에는 Microsoft Entra ID 내 자산의 잠재적 취약성에 대해 알리는 전용 위험 노출 지표(IoE)가 있습니다.

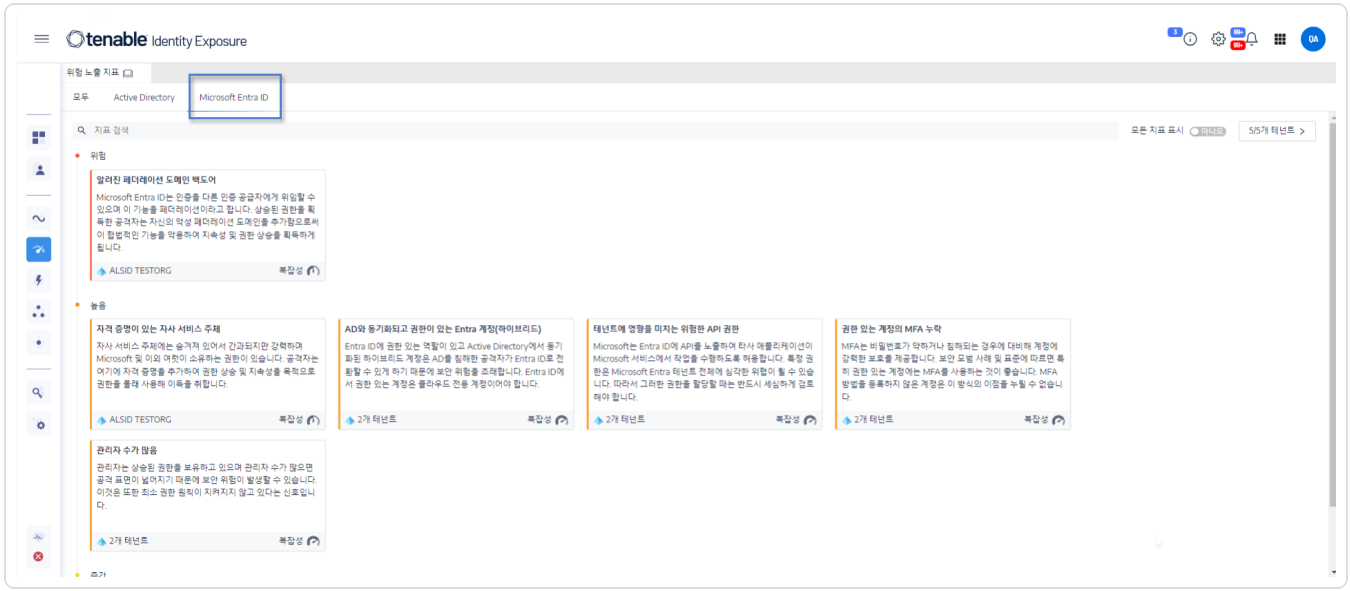
Microsoft Entra ID IoE를 표시하는 방법:

1. Tenable Identity Exposure에서 왼쪽 탐색 모음의 IoE 아이콘 을 클릭합니다.

   IoE 창이 열립니다.

2. **Microsoft Entra ID** 탭을 클릭합니다.

   Tenable Identity Exposure에서 조사 결과를 트리거한 Microsoft Entra ID 관련 IoE를 표시합니다.



3. 조사하려는 IoE가 있는 타일을 클릭합니다.
4. 지표 ID 세부 정보 창이 열리고 다음과 같은 정보가 표시됩니다.
   - **취약성 정보**: 잠재적 공격에 대한 노출이 발생하는 방식입니다.
   - **조사 결과**: ID 공급자 유형에 관한 세부 정보와 위험에 대한 세부 정보입니다.
   - **권장 사항**: 위협을 수정하기 위한 단계입니다.

위험 노출 지표의 일탈 수정

위험 노출 지표(IoE)에 수정이 필요한 일탈 개체가 발생하면 Tenable Identity Exposure가 알림을 트리거합니다.

다음은 세 가지의 특정 IoE에 대한 수정 절차를 수행하는 방법을 나타낸 예시입니다.

- AdminCount 특성을 일반 사용자에 설정
- 위험한 Kerberos 위임
- SDProp 일관성 보장

IoE에 관한 전체 정보는 Tenable Identity Exposure 사용자 인터페이스에 제공된 설명서를 참조하십시오.

AdminCount 특성을 일반 사용자에 설정

사용자 계정의 `adminCount` 특성은 관리 그룹에서의 과거 멤버 자격을 나타내며, 계정이 그룹에서 탈퇴할 때 초기화되지 않습니다. 따라서 오래된 관리 계정이라도 이 특성을 보유하며, Active Directory 권한 상속을 차단합니다. 이 특성은 원래 관리자 보호가 목적이었지만, 까다로운 권한 문제를 유발할 수 있습니다.

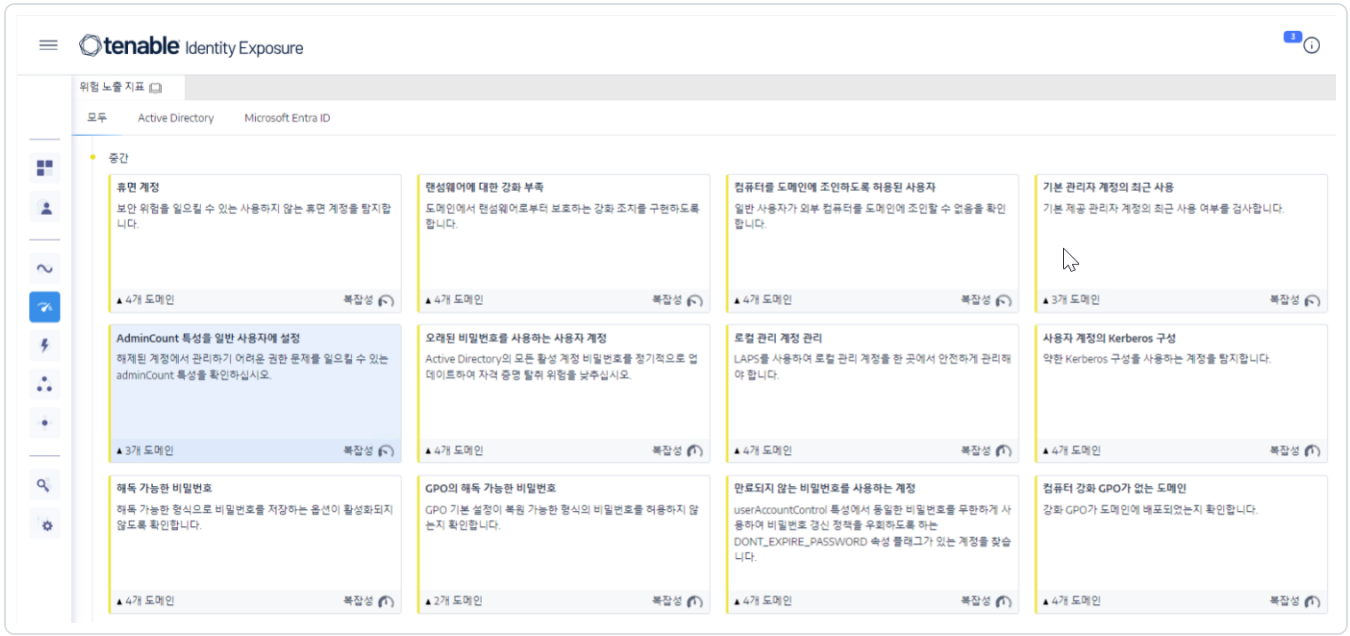
이 중간 수준 IoE는 이 특성이 있는 활성 사용자 계정과 그룹에 대해서만 보고하고, `adminCount` 특성이 `1`로 설정된 정상 구성원을 포함하는 권한 있는 그룹은 제외합니다.

AdminCount 특성을 일반 사용자에 설정 IoE의 일탈 개체를 수정하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭하여 엽니다.

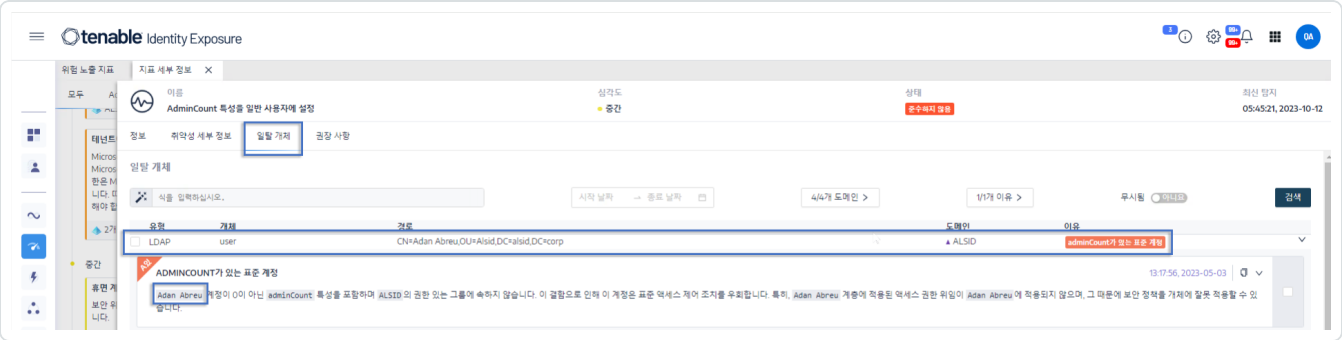
   기본적으로 Tenable Identity Exposure에서는 일탈 개체를 포함한 IoE만 표시합니다.

2. **AdminCount 특성을 일반 사용자에 설정** IoE 타일을 클릭합니다.



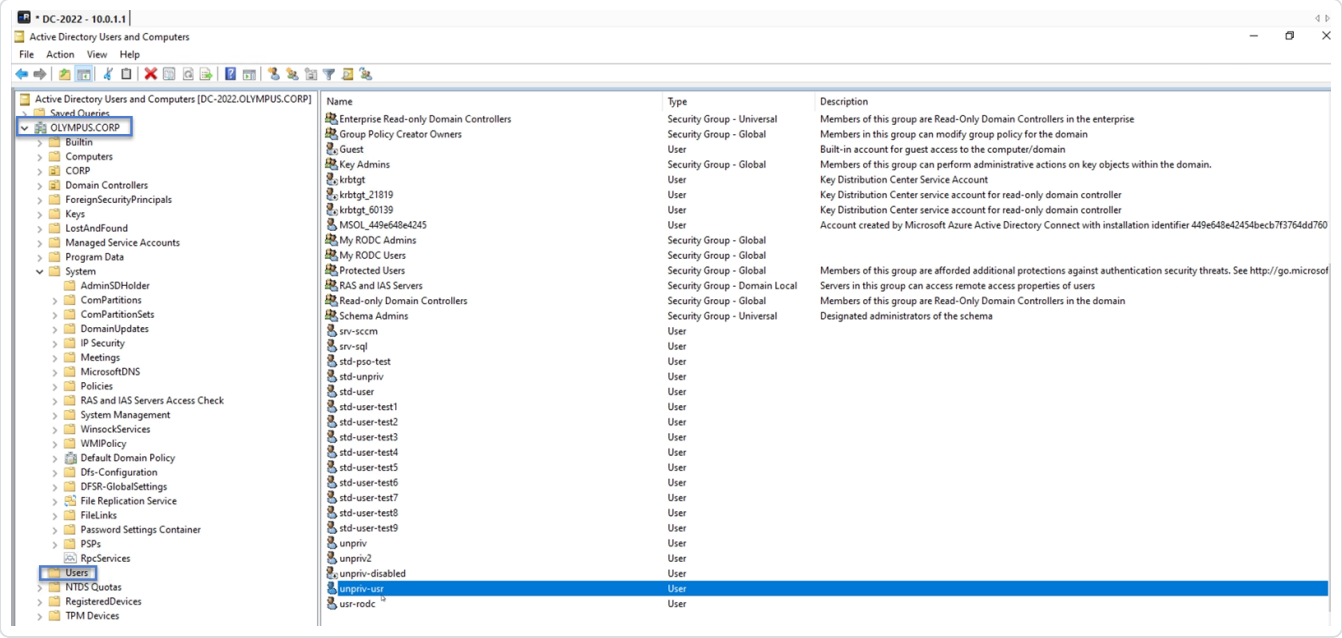
   지표 세부 정보 창이 열립니다.

3. 일탈 개체를 마우스로 가리키고 클릭하여 세부 정보를 표시하고, 도메인 이름과 계정을 기록해 둡니다. (이 예시의 경우: 도메인 = `OLYMPUS.CORP`, 일반 계정은 `unpriv-usr`)

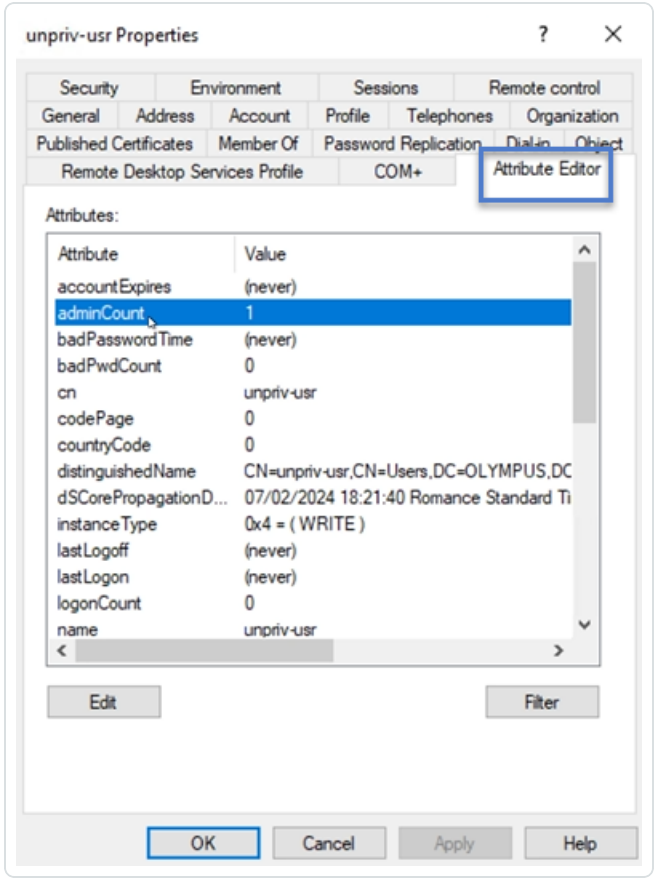


4. 원격 데스크톱 관리자(또는 그와 유사한 도구)에서 도메인 이름을 찾아 Tenable Identity Exposure가 플래그한 **사용자**와 계정으로 이동합니다.

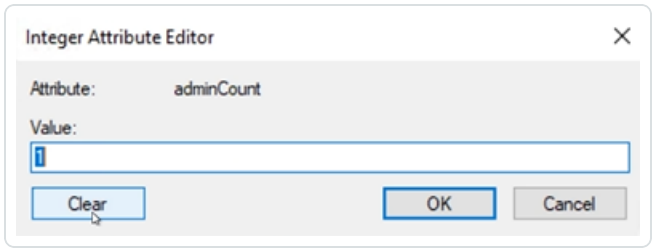
> **필요한 권한**: 이 절차를 수행하려면 도메인에 대한 관리자 계정이 있어야 합니다.



5. 계정 이름을 클릭하여 **속성** 대화 상자를 열고 **특성 편집기** 탭을 선택합니다.
6. 특성 목록에서 `adminCount`를 클릭하여 **정수 특성 편집기** 대화 상자를 엽니다.



7. 대화 상자에서 **지우기**와 **확인**을 클릭합니다.



8. Tenable Identity Exposure에서 지표 세부 정보 창으로 돌아가 페이지를 새로 고칩니다.

   일탈 개체가 더 이상 목록에 표시되지 않습니다.

위험한 Kerberos 위임

Active Directory 보안의 핵심인 Kerberos 프로토콜은 일부 서버가 사용자 자격 증명을 재사용하도록 허용합니다. 공격자가 이런 서버 중 하나를 손상하면 자격 증명을 탈취하여 다른 리소스에서 인증하는 데 사용할 수 있습니다.

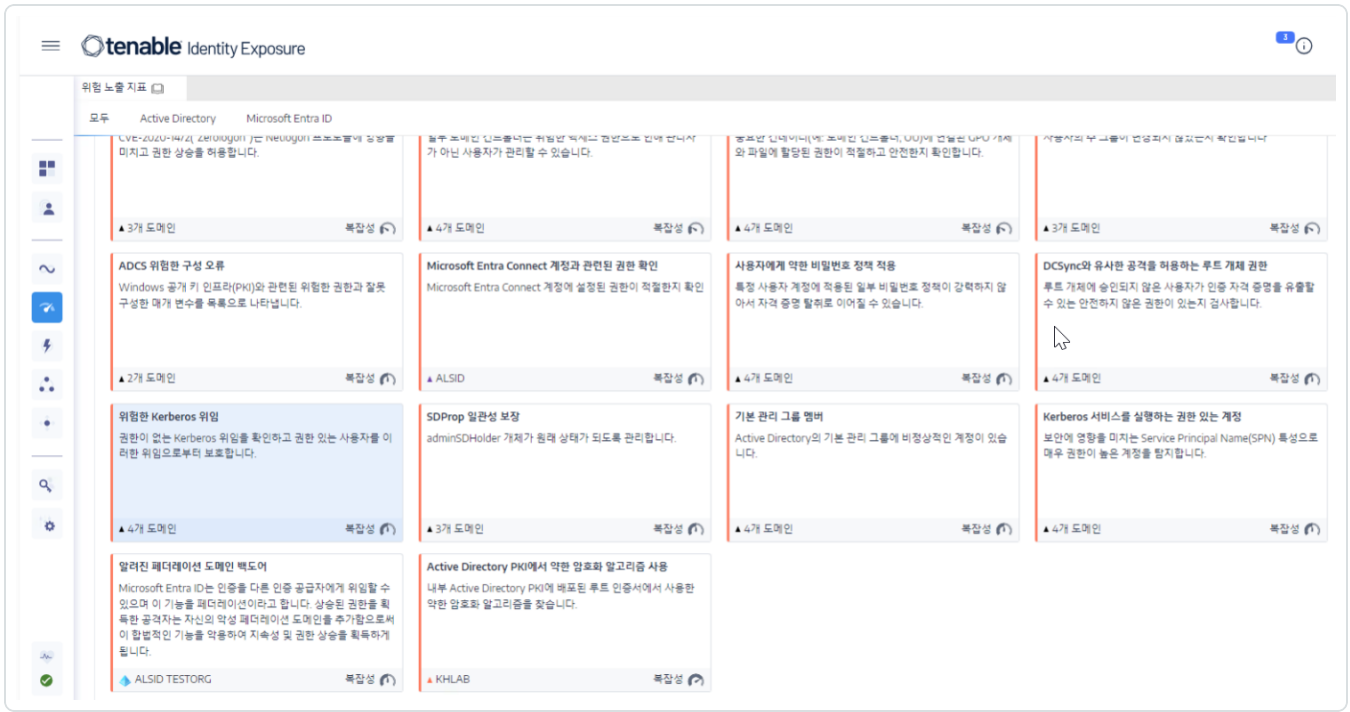
이 위험 수준 IoE는 위임 특성이 있는 모든 계정을 보고하고 사용 중지된 계정은 제외합니다. 권한 있는 사용자는 위임 특성이 있어서는 안 됩니다. 이러한 사용자 계정을 보호하려면 해당 계정을 "보호된 사용자" 그룹에 추가하고 "계정이 중요하고 위임할 수 없음"으로 표시합니다.

계정을 "보호된 그룹"에 추가하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭하여 엽니다.

   기본적으로 Tenable Identity Exposure에서는 일탈 개체를 포함한 IoE만 표시합니다.

2. **위험한 Kerberos 위임** IoE 타일을 클릭합니다.



   지표 세부 정보 창이 열립니다.

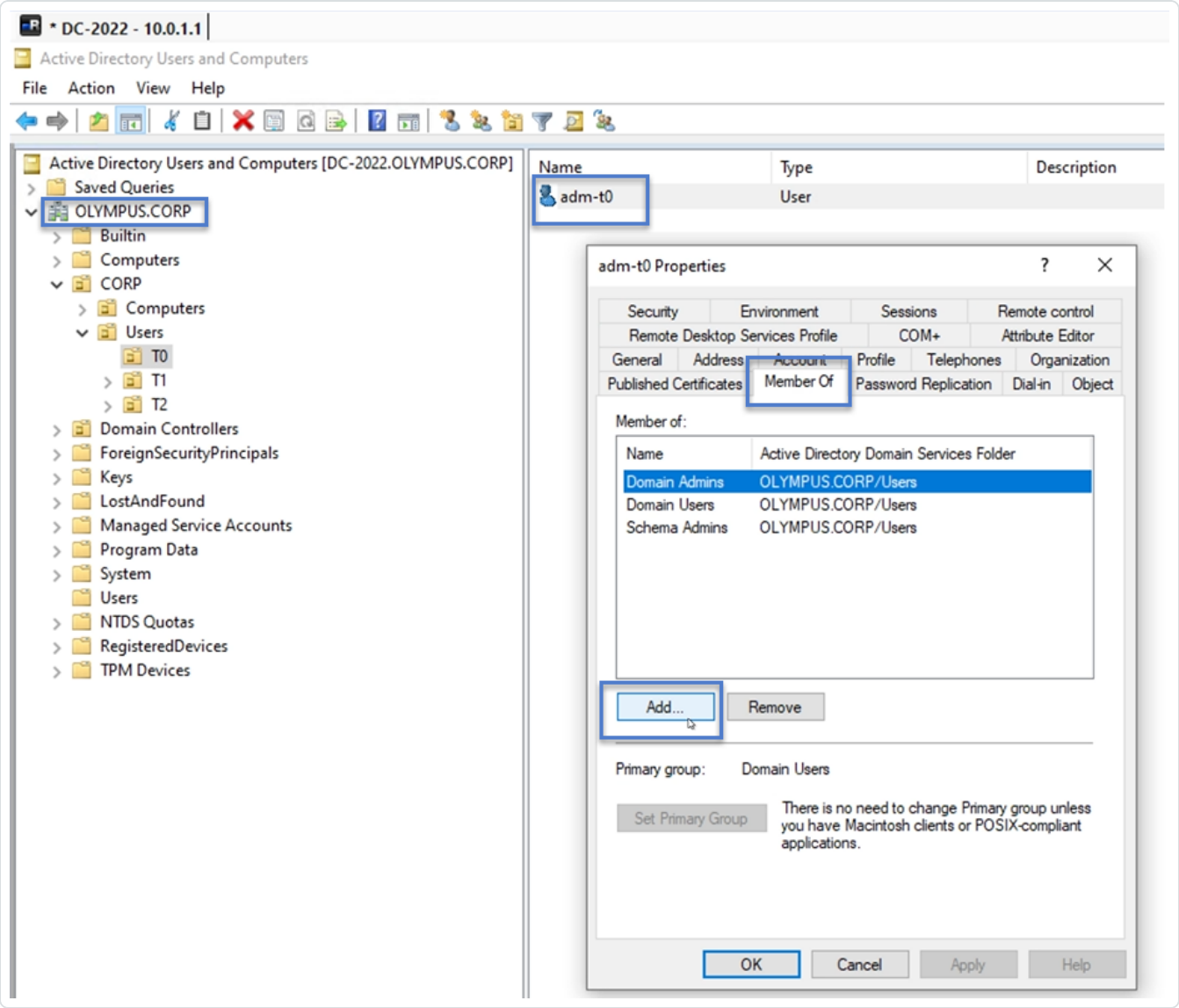
3. 일탈 개체를 마우스로 가리키고 클릭하여 세부 정보를 표시하고, 도메인 이름과 계정을 기록해 둡니다. (이 예시의 경우: 도메인 = OLYMPUS.CORP, 계정 = `adm-t0`)

4. 원격 데스크톱 관리자(또는 그와 유사한 도구)에서 도메인 이름을 찾아 Tenable Identity Exposure가 플래그한 도메인과 계정으로 이동합니다.

   필요한 권한: 이 절차를 수행하려면 도메인에 대한 관리자 계정이 있어야 합니다.

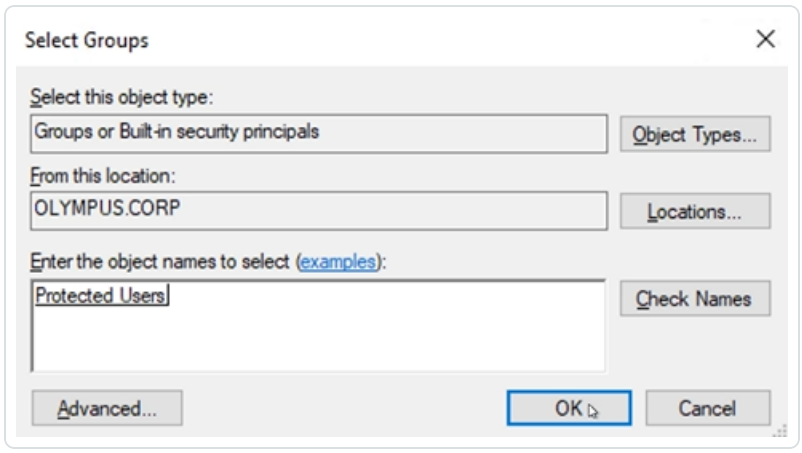
5. 계정 이름을 클릭하여 **속성** 대화 상자를 열고 **멤버의 소속** 탭을 선택합니다.

6. 멤버 목록에서 **추가**를 클릭합니다.



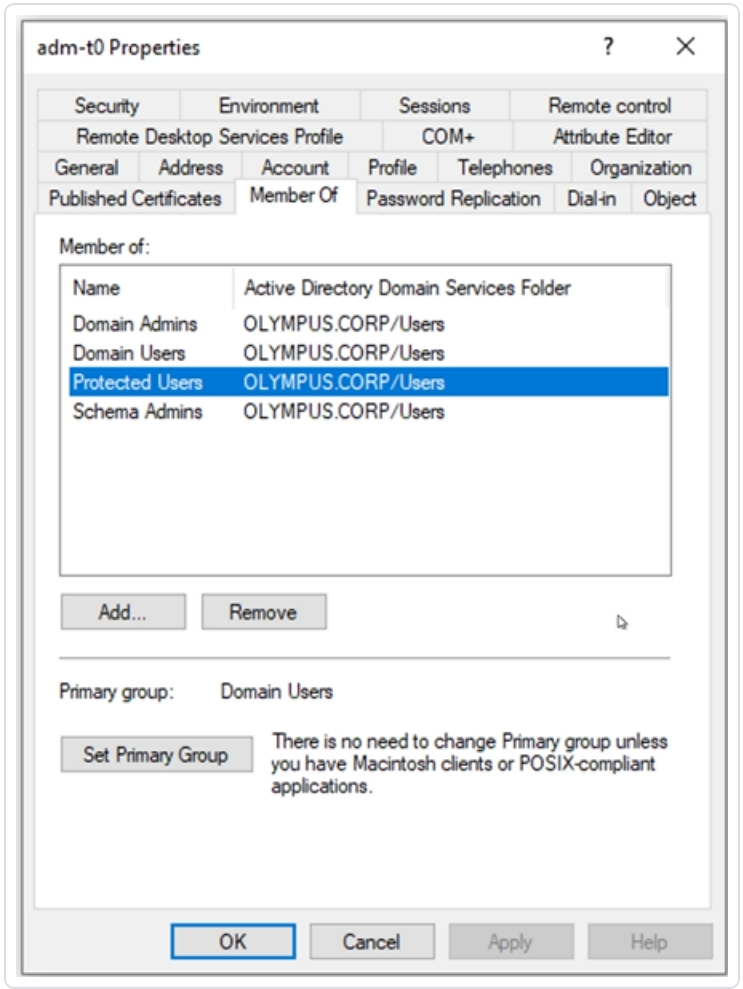
그룹 선택 대화 상자가 표시됩니다.

7. 개체 이름 "보호된 사용자"를 입력하고 **이름 검사**를 클릭합니다.



8. **확인**을 클릭하여 대화 상자를 닫습니다.
9. **속성** 대화 상자에서 **적용**을 클릭합니다.

   새 그룹이 멤버 목록에 표시됩니다.



10. **확인**을 클릭하여 대화 상자를 닫습니다.
11. Tenable Identity Exposure에서 지표 세부 정보 창으로 돌아가 페이지를 새로 고칩니다.

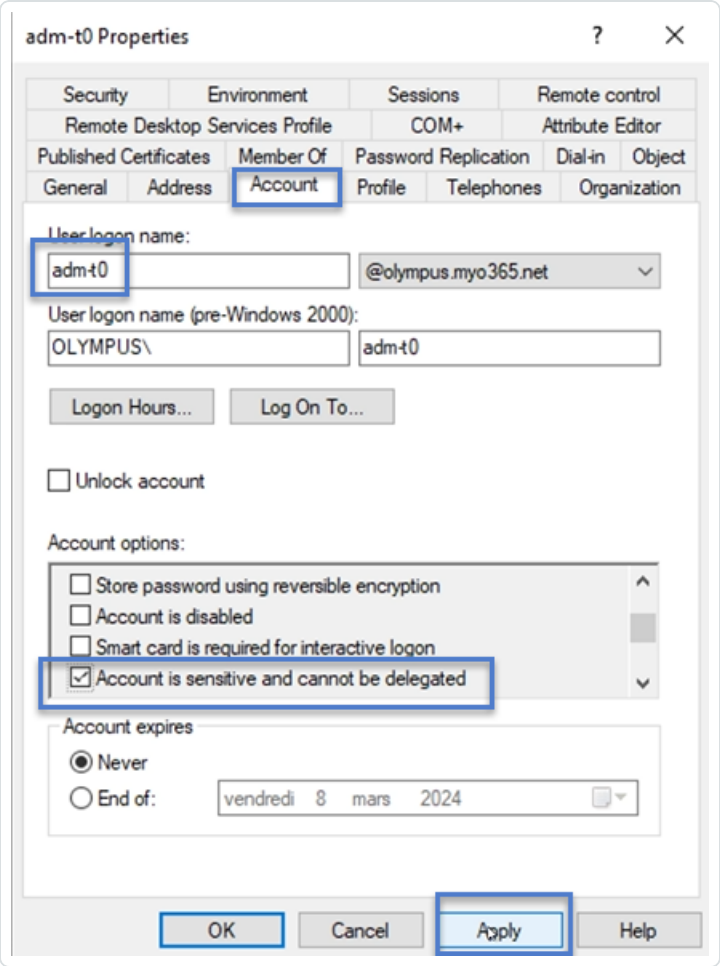
    일탈 개체가 더 이상 목록에 표시되지 않습니다.

계정을 "위임할 수 없음"으로 설정하는 방법:

1. 원격 데스크톱 관리자에서 도메인 이름을 찾아 Tenable Identity Exposure가 플래그한 도메인과 계정으로 이동합니다.

   필요한 권한: 이 절차를 수행하려면 도메인에 대한 관리자 계정이 있어야 합니다.

2. 계정 이름을 클릭하여 **속성** 대화 상자를 열고 **계정** 탭을 선택합니다.
3. 계정 옵션 목록에서 "계정이 중요하고 위임할 수 없음"을 선택하고 **적용**을 클릭합니다.



4. **확인**을 클릭하여 대화 상자를 닫습니다.

5. Tenable Identity Exposure에서 지표 세부 정보 창으로 돌아가 페이지를 새로 고칩니다.

   일탈 개체가 더 이상 목록에 표시되지 않습니다.

SDProp 일관성 보장

Active Directory 도메인을 침해하는 공격자는 보통 `adminSDHolder` 개체의 ACL을 변경하고, 공격자가 ACL에 추가하는 모든 권한이 권한 있는 사용자에게 복사되어 백도어를 설정하기 쉬워집니다.

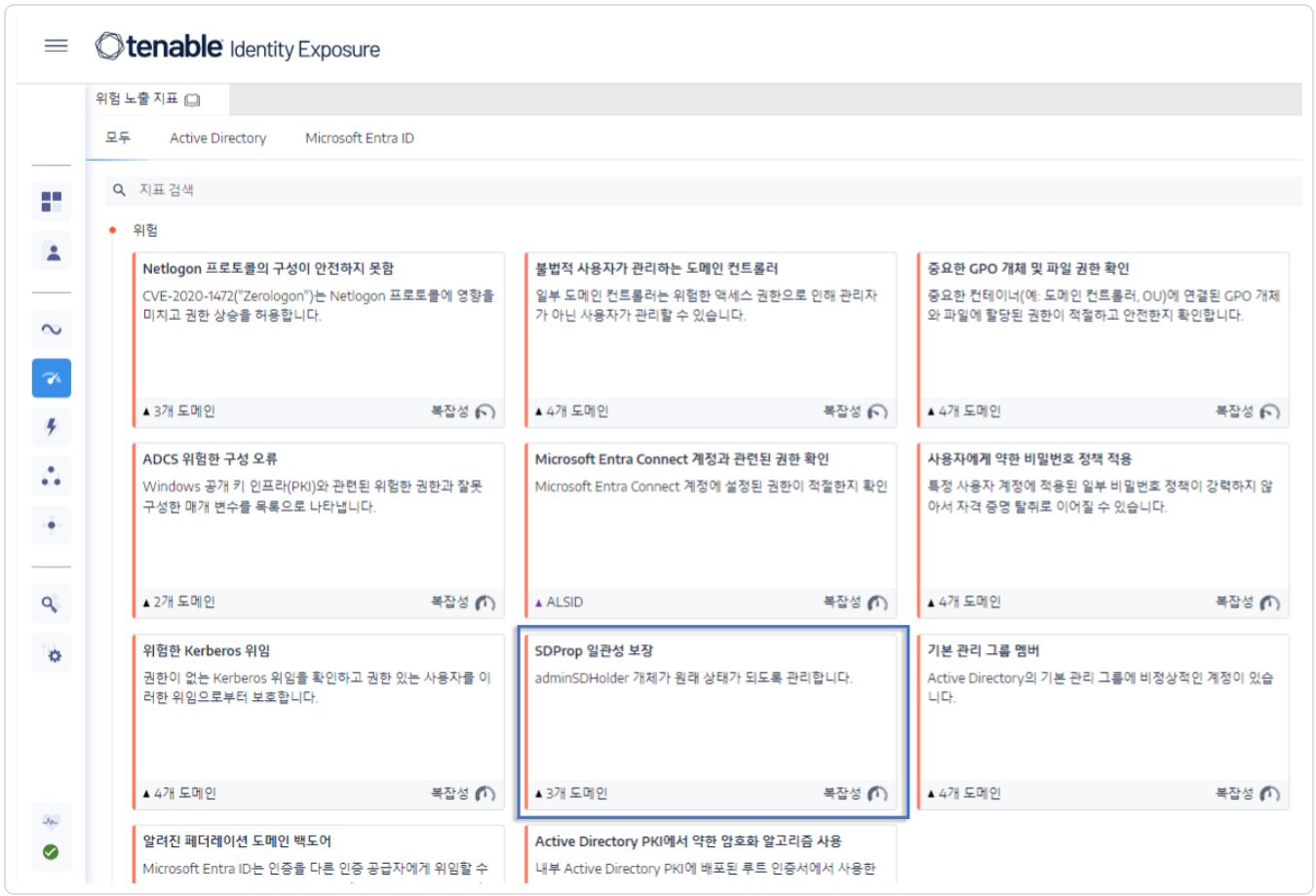
이 위험 수준 IoE는 `adminSDHolder` 개체에 대해 설정된 권한이 관리 계정에 대해 권한 있는 액세스만 허용하는지 검사합니다.

SDProp 일관성 보장 IoE의 일탈 개체를 수정하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **위험 노출 지표**를 클릭하여 엽니다.

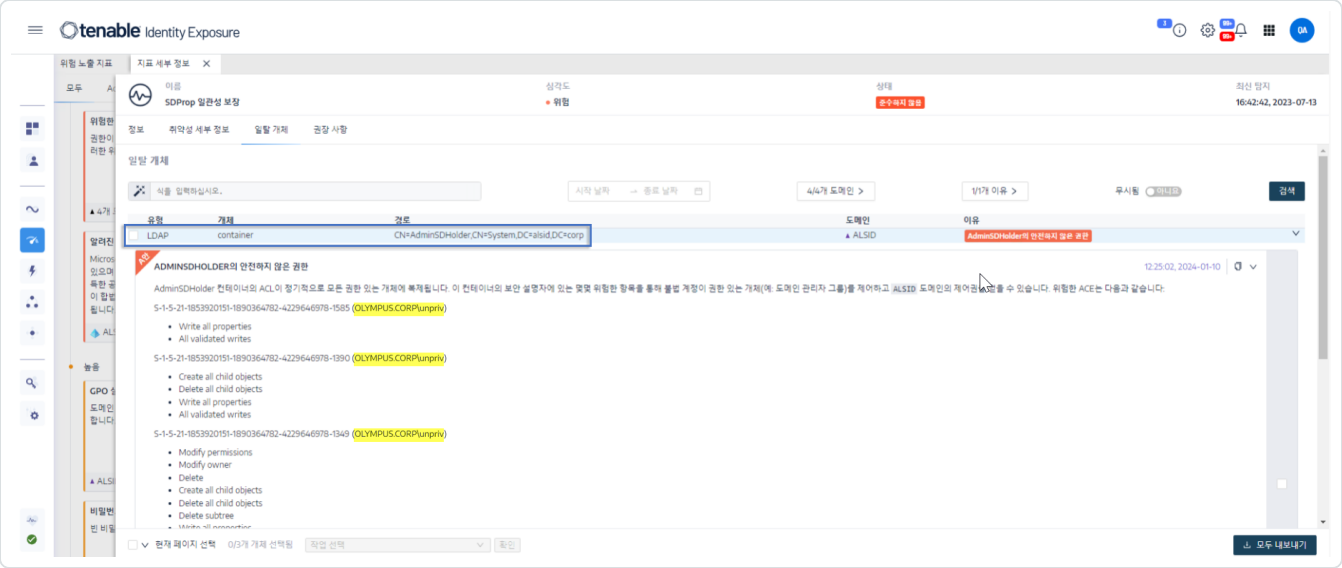
   기본적으로 Tenable Identity Exposure에서는 일탈 개체를 포함한 IoE만 표시합니다.

2. **SDProp 일관성 보장** IoE 타일을 클릭합니다.



지표 세부 정보 창이 열립니다.

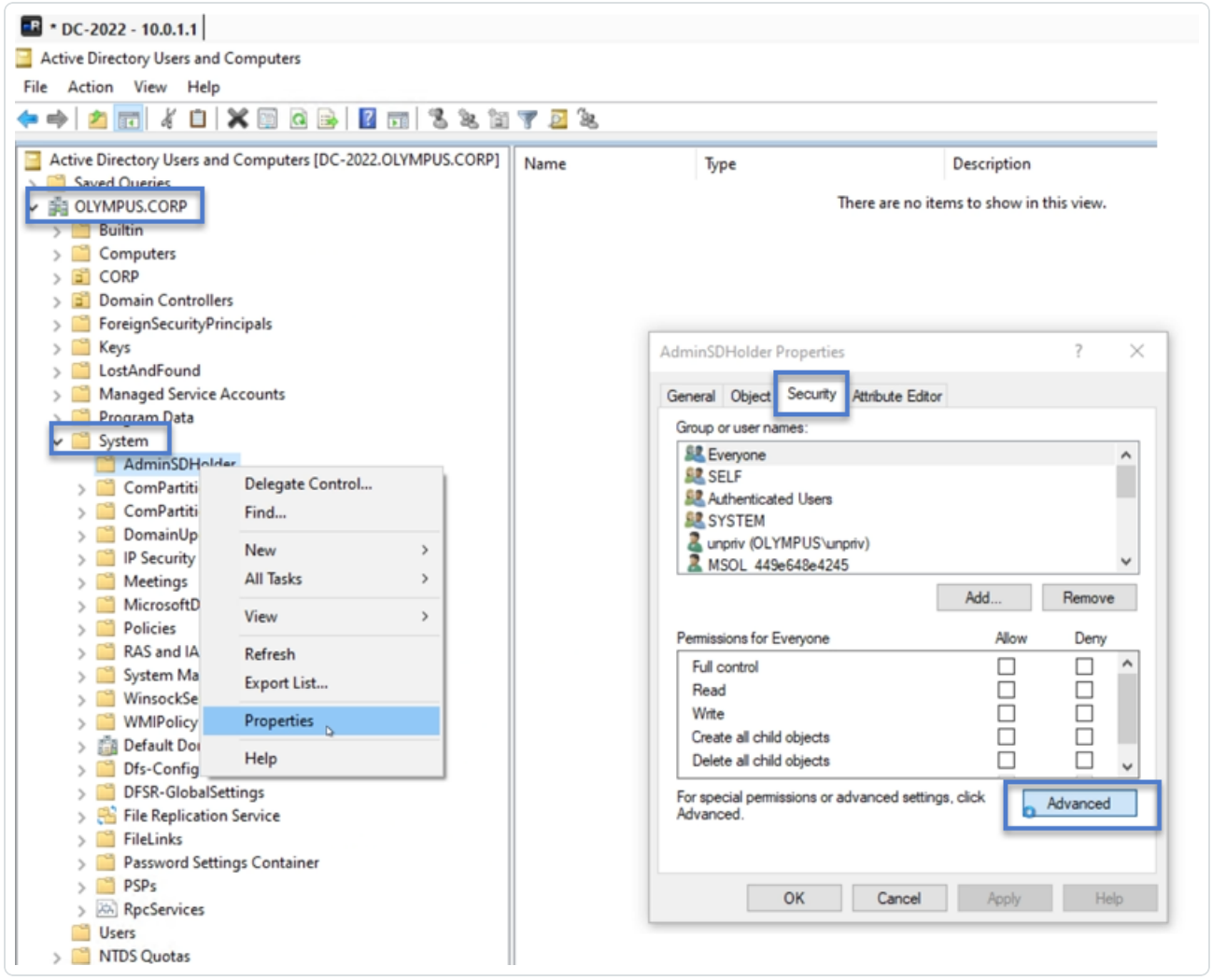
3. 일탈 개체를 마우스로 가리키고 클릭하여 세부 정보를 표시합니다. Tenable Identity Exposure가 플래그한 도메인 이름과 관련 권한을 기록해 둡니다. (이 예시의 경우: `OLYMPUS.CORP .\unpriv`)



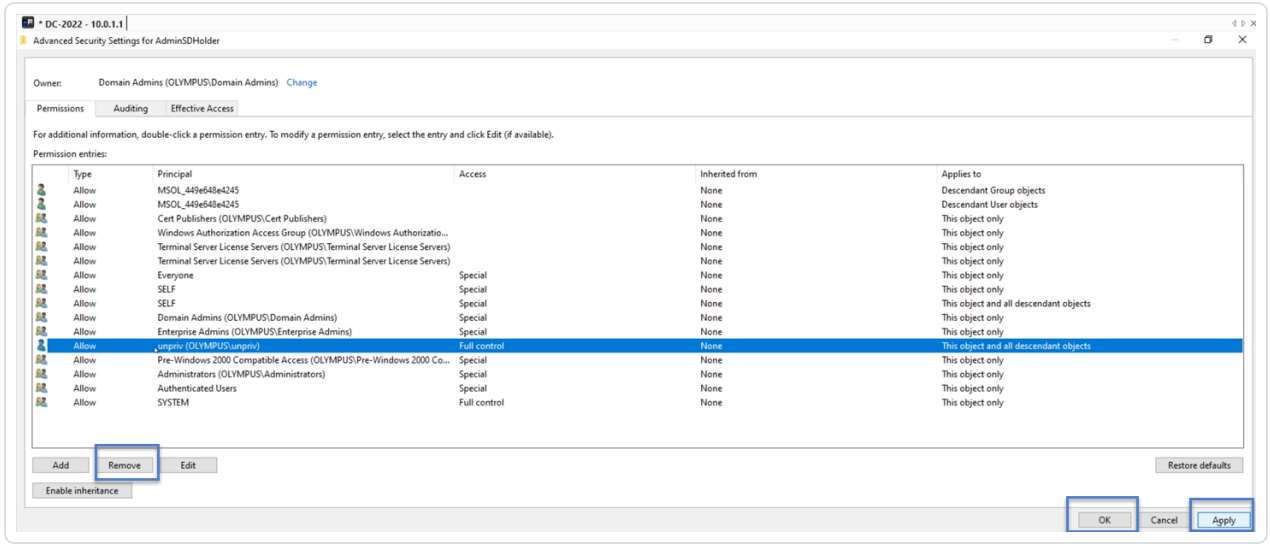
4. 원격 데스크톱 관리자(또는 그와 유사한 도구)에서 도메인 이름을 찾아 **시스템** > **AdminSDHolder**로 이동합니다.

> **필요한 권한**: 이 절차를 수행하려면 도메인에 대한 관리자 계정이 있어야 합니다.

5. **AdminSDHolder**를 마우스 오른쪽 버튼으로 클릭하고, 컨텍스트 메뉴에서 **속성**을 선택합니다.



6. **속성** 대화 상자에서 **보안** 탭을 선택하고 **고급**을 클릭합니다.
7. **고급 보안 설정** 창과 **권한** 탭으로 이동하여 권한 항목 목록에서 알림을 발생시킨 권한을 선택합니다.
8. **제거**를 클릭합니다.
9. **적용**과 **확인**을 클릭하여 설정 창을 닫습니다.
10. **확인**을 클릭하여 **속성** 창을 닫습니다.



11. Tenable Identity Exposure에서 지표 세부 정보 창으로 돌아가 페이지를 새로 고칩니다.

    일탈 개체가 더 이상 목록에 표시되지 않습니다.

공격 지표

필요한 라이선스: 공격 지표

Tenable Identity Exposure의 **공격 지표**(IoA)를 이용하면 Active Directory(AD)에서 공격을 탐지할 수 있습니다.

공격 지표 통합 보기에서는 타임라인과 AD에 영향을 미치는 3대 인시던트 실시간 정보와 공격 분포를 창 한 개에 표시합니다. 다음과 같은 작업을 수행할 수 있습니다.

- 정확한 공격 타임라인에서 모든 위협을 시각화합니다.
- 한 가지 AD 공격에 관한 세부 정보를 심층 분석합니다.
- 탐지된 인시던트에서 직접 MITRE ATT&CK 설명을 검색합니다.

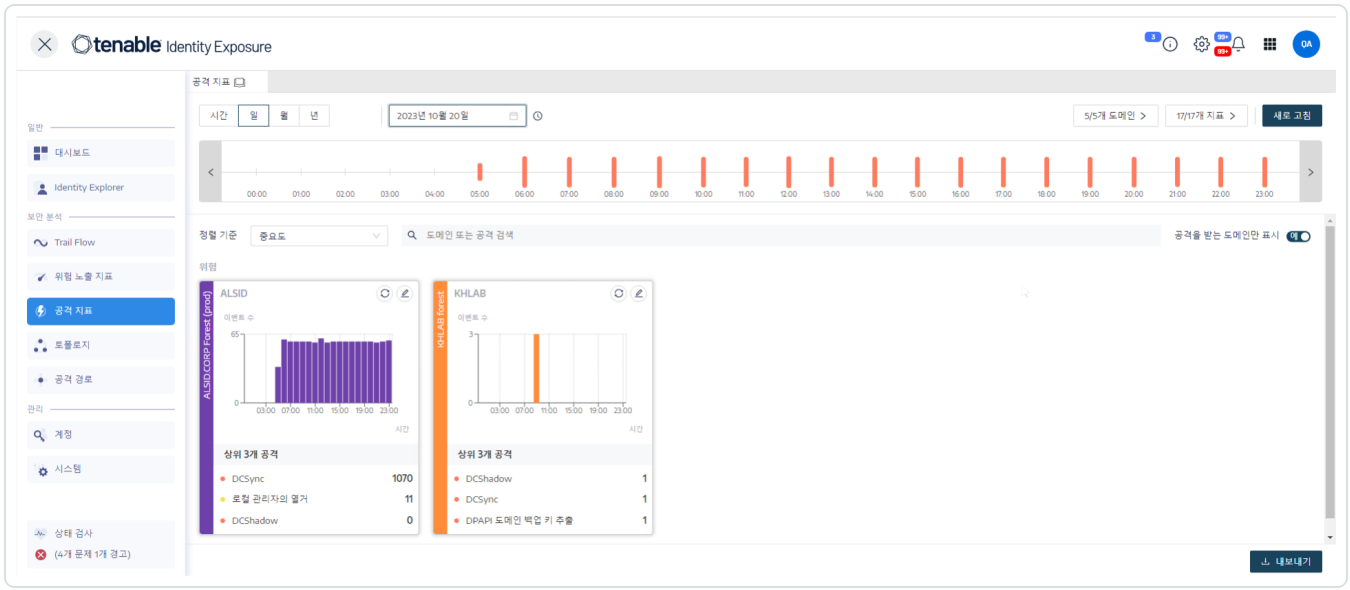
특정 IoA에 관한 자세한 정보는 Indicators of Attack and the Active Directory를 참조하십시오.

참고: 탐지된 공격 수가 많은 경우, 다양한 IoA 옵션에 대해 권장되는 값을 적용하면 관리자가 공격 지표를 올바로 보정했는지 확인할 수 있습니다. 자세한 정보는 IoA를 보정하는 방법을 참조하십시오.

공격 지표를 표시하는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **공격 지표**를 클릭합니다.

   공격 지표 창이 열립니다.



2. 기본적으로 Tenable Identity Exposure에서는 모든 AD 포리스트와 도메인을 표시합니다. 이 보기를 조정하려면 다음 중 작업을 수행합니다.

   - 표시할 기간 선택 - **시간**, **일**(기본값), **월** 또는 **년**을 클릭합니다.
   - 타임라인을 따라 이동 - 왼쪽 또는 오른쪽 화살표를 클릭하여 타임라인에서 앞으로 또는 뒤로 이동합니다.
   - 특정 시간 선택 - 날짜 선택기를 클릭하여 시간, 일, 월 또는 연도를 선택합니다.
   - 현재 날짜 및 시간으로 돌아가기 - 날짜 선택기 옆에 있는 아이콘을 클릭합니다.
   - 도메인 선택 - **n/n 도메인**을 클릭합니다.

     a. **포리스트 및 도메인** 창에서 도메인을 선택합니다.

     b. **선택 항목 필터링**을 클릭합니다.

        Tenable Identity Exposure에서 보기를 업데이트합니다.
   - IoA 선택 - **n/n 지표**를 클릭합니다.

     a. 공격 지표 창에서 IoA를 선택합니다.

     b. **선택 항목 필터링**을 클릭합니다.

        Tenable Identity Exposure에서 보기를 업데이트합니다.
   - IoA 타일 정렬 - **정렬 기준** 상자에서 화살표를 클릭하여 선택 항목 드롭다운 목록(**도메인**, **중요도** 또는 **포리스트**)을 표시합니다.
   - 도메인 또는 공격 검색 - **검색** 상자에 도메인 이름 또는 공격을 입력합니다.
   - 공격을 받는 도메인만 표시 - **공격을 받는 도메인만 표시** 토글을 클릭하여 **예**로 설정합니다.
   - 공격 보고서 내보내기 - **내보내기**를 클릭합니다.

     카드 내보내기 창이 표시됩니다.

     a. **내보내기 형식** 상자에서 드롭다운 목록 화살표를 클릭하여 형식(**PDF**, **CSV** 또는 **PPTX**)을 선택합니다.

b. **내보내기**를 클릭합니다.

Tenable Identity Exposure에서 보고서를 로컬 시스템에 다운로드합니다.

심각도 수준

Tenable Identity Exposure에서 공격을 탐지하고 공격에 심각도 수준을 할당합니다.

수준	설명
위험 - 빨간색	도메인 우위가 전제 조건으로 필요한 증명된 악용 이후 공격을 탐지했습니다.
높음 - 주황색	공격자가 도메인 우위를 점할 수 있게 해주는 중대한 공격을 탐지했습니다.
중간 - 노란색	이런 IoA는 위험한 권한 상승을 초래할 수 있거나 중요한 리소스에 대한 액세스를 허용할 수 있는 공격과 관련이 있습니다.
낮음 - 파란색	정찰 작업 또는 영향이 적은 인시던트와 관련된 의심스러운 동작에 대한 알림입니다.

참고 항목

- 공격 지표 세부 정보
- 공격 지표 인시던트

공격 지표 세부 정보

Tenable Identity Exposure의 공격 지표 창에는 Active Directory에서 발생한 공격에 관한 정보가 표시됩니다.

공격 지표를 보는 방법:

- Tenable Identity Exposure의 탐색 창에서 **공격 지표**를 클릭합니다.

  공격 지표 창이 열립니다.

타임라인에 공격 지표를 표시하는 방법:

- 타임라인을 따라 이벤트를 클릭하면 다음과 같은 내용이 표시됩니다.
  - 인시던트 탐지 날짜 및 시간.
  - 상위 3개 공격의 심각도 수준.
  - 이 날짜 및 시간에 탐지된 공격의 총 개수.

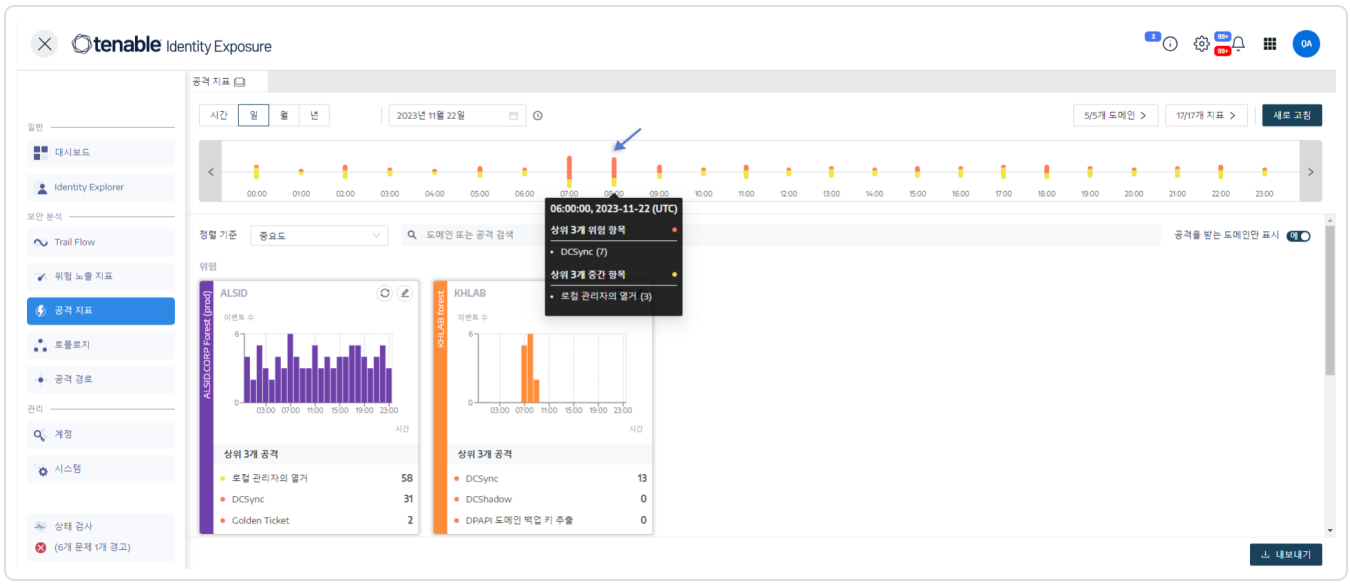


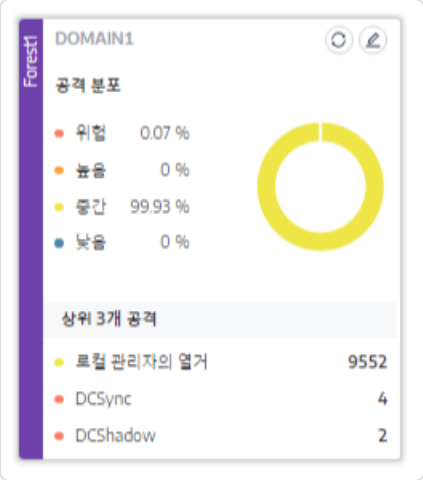
차트 유형을 변경하는 방법:

1. ✎ 아이콘을 클릭하여 도메인 타일을 편집합니다.

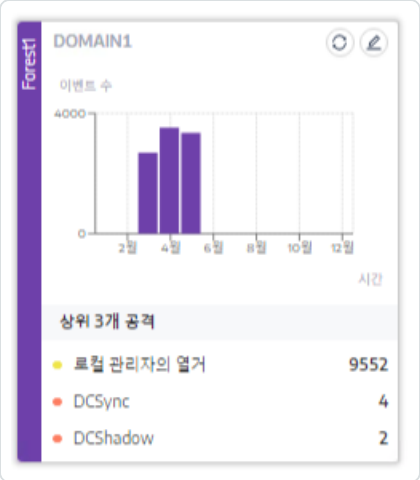
   카드 정보 편집 창이 표시됩니다.

2. 차트 유형을 선택합니다.

- **공격 분포**: 공격 심각도의 분포를 표시합니다.



- **이벤트 수:** 상위 3개의 공격과 그 공격의 발생 횟수를 표시합니다.



3. **저장**을 클릭합니다.

   Tenable Identity Exposure에서 차트를 업데이트합니다.

참고 항목

- 공격 지표
- 공격 지표 인시던트

공격 지표 인시던트

공격 지표(IoA) 인시던트 목록에는 Active Directory(AD)의 특정 공격에 관한 상세한 정보가 제공됩니다. 이를 참조하여 IoA의 심각도 수준에 따라 필요한 조치를 취할 수 있습니다.

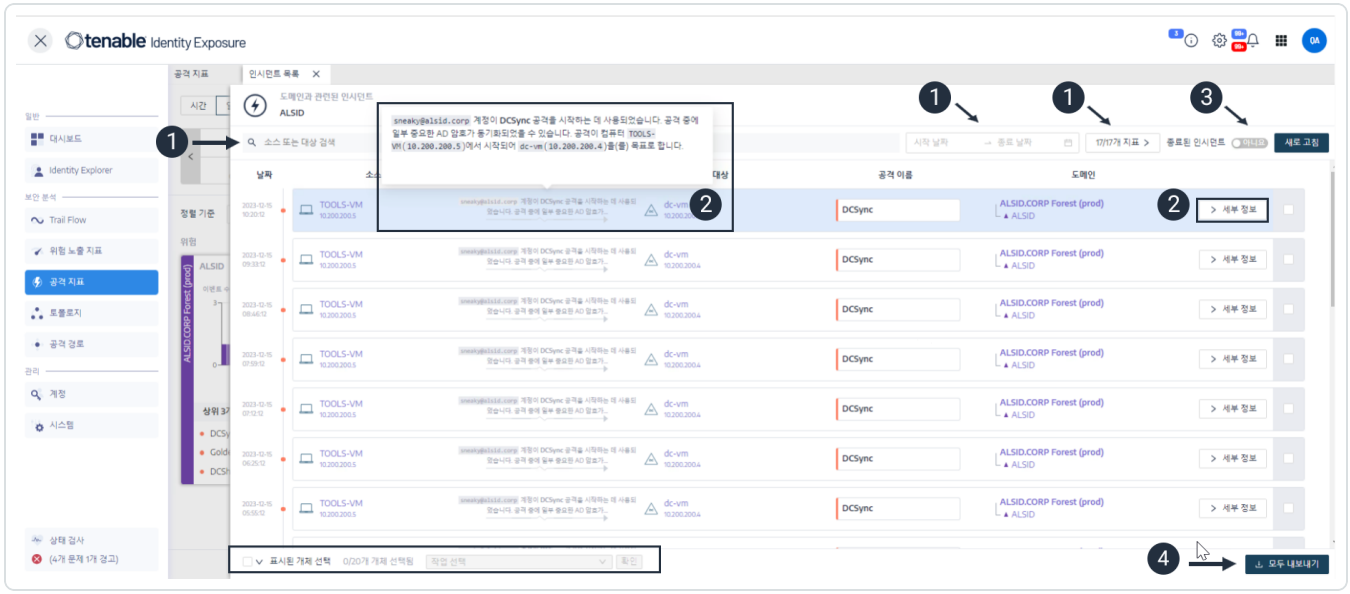
공격 인시던트를 보는 방법:

1. Tenable Identity Exposure의 탐색 창에서 **공격 지표**를 클릭합니다.

   공격 지표 창이 열립니다.

2. 도메인 타일을 클릭합니다.

   인시던트 목록 창이 표시되며 해당 도메인에서 발생한 인시던트 목록이 포함됩니다.

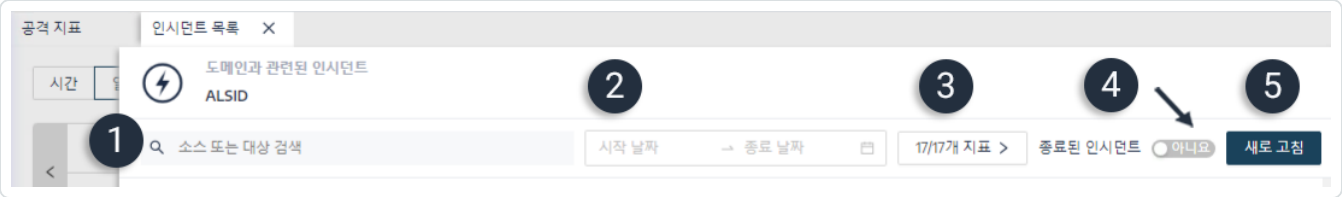


3. 이 목록에서, 다음 작업을 수행할 수 있습니다.
   - 검색 기준을 정의하여 특정 인시던트를 검색합니다. ❶
   - AD에 영향을 미치는 공격에 대한 상세한 설명에 액세스합니다.❷
   - 인시던트를 종료하거나 다시 엽니다.❸
   - 모든 인시던트를 표시하는 보고서를 다운로드합니다.❹

인시던트를 검색하는 방법:

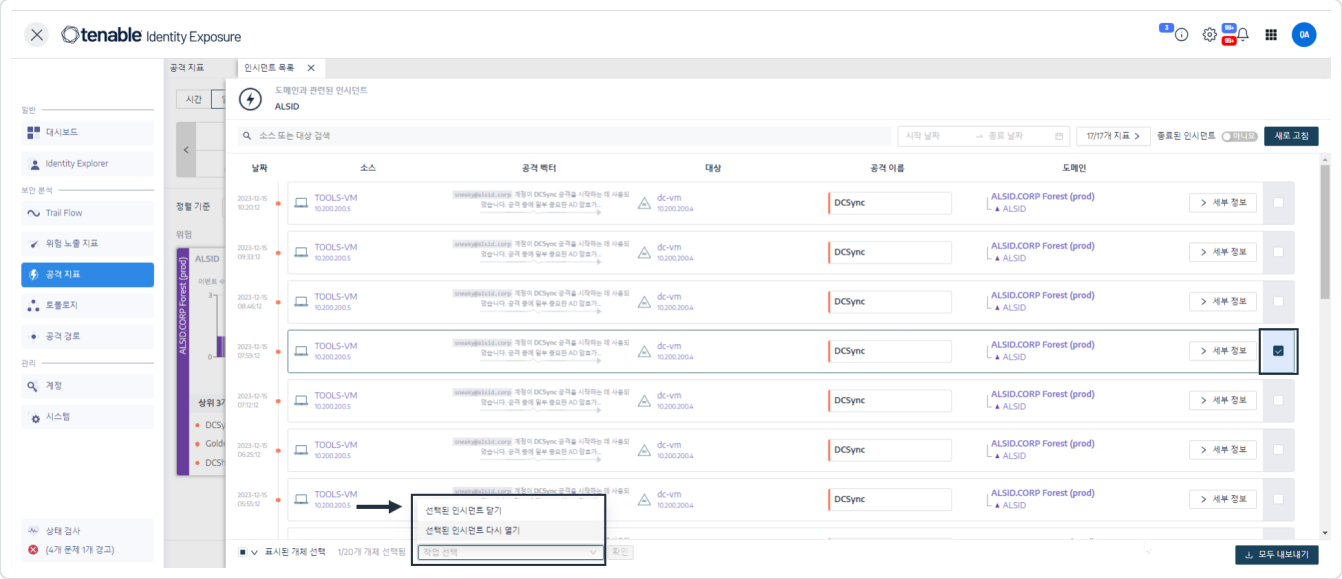
1. **검색** 상자에 소스 또는 대상의 이름을 입력합니다.
2. 날짜 선택기를 클릭하여 해당 인시던트의 시작 날짜와 종료 날짜를 선택합니다.
3. **n/n 지표**를 클릭하여 관련 지표를 선택합니다.
4. **종료된 인시던트**를 클릭하여 **예**로 토글하여 검색을 종료된 인시던트로 제한합니다.
5. **새로 고침**을 클릭합니다.

   Tenable Identity Exposure에서 일치하는 인시던트로 목록을 업데이트합니다.



인시던트를 종료하는 방법:

1. 인시던트 목록에서 종료하거나 다시 열려는 인시던트를 선택합니다.



2. 창 아래에서 드롭다운 메뉴를 클릭하고 **선택된 인시던트 종료**를 선택합니다.
3. **확인**을 클릭합니다.

   메시지가 표시되어 종료 확인을 요청합니다.

4. **확인**을 클릭합니다.

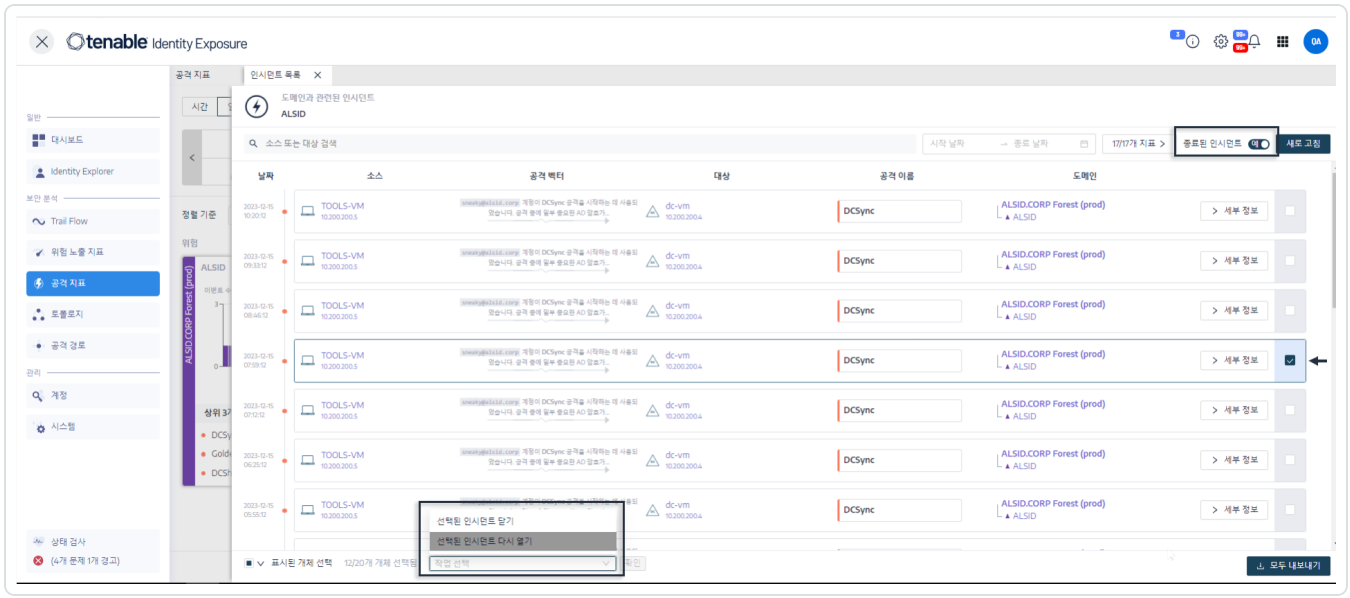
   메시지가 표시되어 Tenable Identity Exposure에서 해당 인시던트를 종료했음을 확인하고 더 이상 표시하지 않습니다.

인시던트를 다시 여는 방법:

1. **인시던트 목록** 창에서 **종료된 인시던트** 토글을 클릭하여 **예**로 설정합니다.

   Tenable Identity Exposure에서 목록을 종료된 인시던트로 업데이트합니다.

2. 다시 열려는 인시던트를 선택합니다.



3. 창 아래에서 드롭다운 메뉴를 클릭하고 **선택된 인시던트 다시 열기**를 선택합니다.

4. **확인**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 해당 인시던트를 다시 열었음을 확인합니다.

팁: 인시던트를 일괄 종료하거나 다시 열 수 있습니다. 창 아래에서 **표시된 개체 선택**을 클릭합니다.

인시던트 세부 정보

인시던트 목록의 각 항목에 다음과 같은 정보가 표시됩니다.

- **날짜** - IoA를 트리거한 인시던트가 발생한 날짜. Tenable Identity Exposure에서는 타임라인 상단에 가장 최근 항목을 표시합니다.
- **소스** - 공격이 발생한 소스와 그 IP 주소.
- **공격 벡터** - 공격 중에 발생한 사항에 대한 설명.

  팁: 공격 벡터를 마우스 커서로 가리키면 해당 IoA에 관한 자세한 정보가 표시됩니다.
- **대상** - 공격의 대상과 그 IP 주소.
- **공격 이름** - 공격의 기술적 이름.
- **도메인** - 해당 공격이 영향을 미친 도메인.

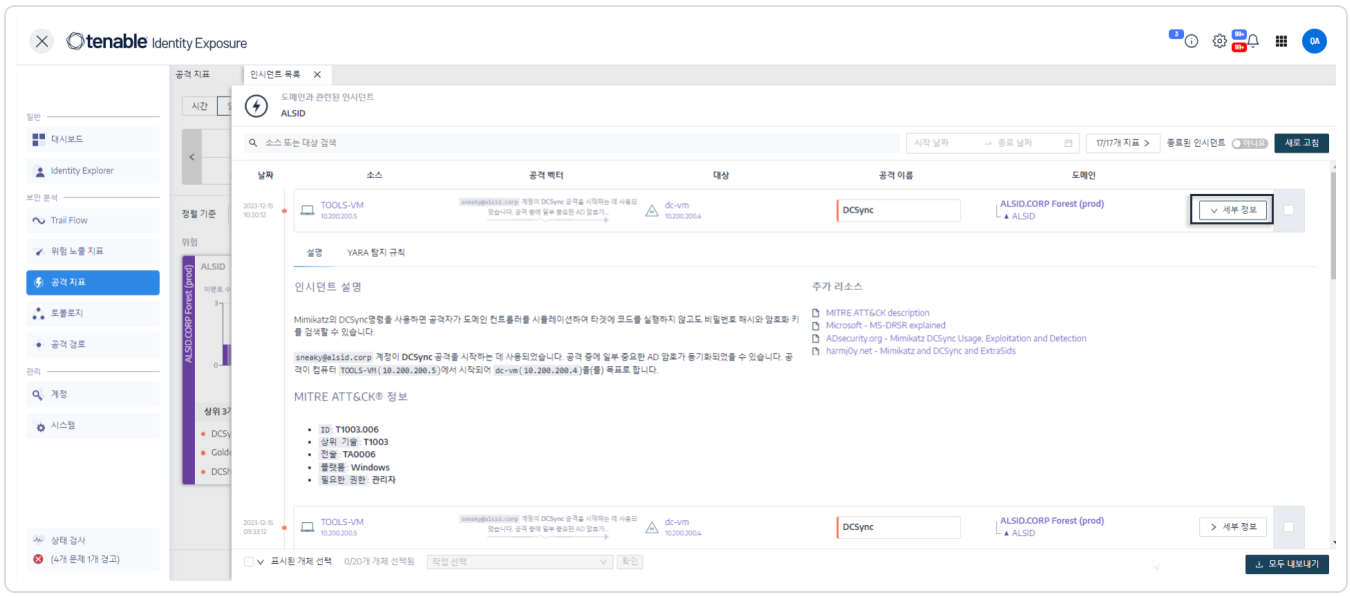
  팁: Tenable Identity Exposure에서는 사용자가 **인시던트 목록**의 여러 가지 대화형 요소(링크, 작업 버튼 등)를 클릭하여 최대 5개의 창을 표시할 수 있습니다. 모든 창을 동시에 닫으려면 페이지를 클릭하십시오.

공격 세부 정보

인시던트 목록에서 특정 공격을 드릴다운하고 수정을 위해 필요한 조치를 취할 수 있습니다.

공격 세부 정보를 표시하는 방법:

1. 인시던트 목록에서 세부 정보를 확인하기 위해 드릴다운할 인시던트를 선택합니다.
2. **세부 정보**를 클릭합니다.



Tenable Identity Exposure에서 그 공격과 연결된 세부 정보를 표시합니다.

설명

설명 탭에 다음과 같은 섹션이 포함됩니다.

- **인시던트 설명** - 공격에 대한 간략한 설명을 제공합니다.
- **MITRE ATT&CK 정보 -** Mitre Att&ck(Adversarial Tactics, Techniques, and Common Knowledge) 기술 자료에서 가져온 기술적 정보를 제공합니다. Mitre Att&ck은 공격자의 공격을 분류하고 공격자의 네트워크를 침해한 후에 작업을 설명하는 프레임워크입니다. 또한 사이버 보안 커뮤니티에서 다같이 이해할 수 있도록 보안 취약성의 표준 식별자도 제공합니다.
- **추가 리소스** - 공격에 대한 심층적 정보를 제공하는 웹사이트, 문서 및 백서로 이동하는 링크를 제공합니다.

YARA 탐지 규칙

YARA 탐지 규칙탭은 Tenable Identity Exposure에서 Tenable Identity Exposure의 탐지 체인을 강화하기 위해 네트워크 수준에서 AD 공격을 탐지하는 데 쓰는 YARA 규칙을 설명합니다.

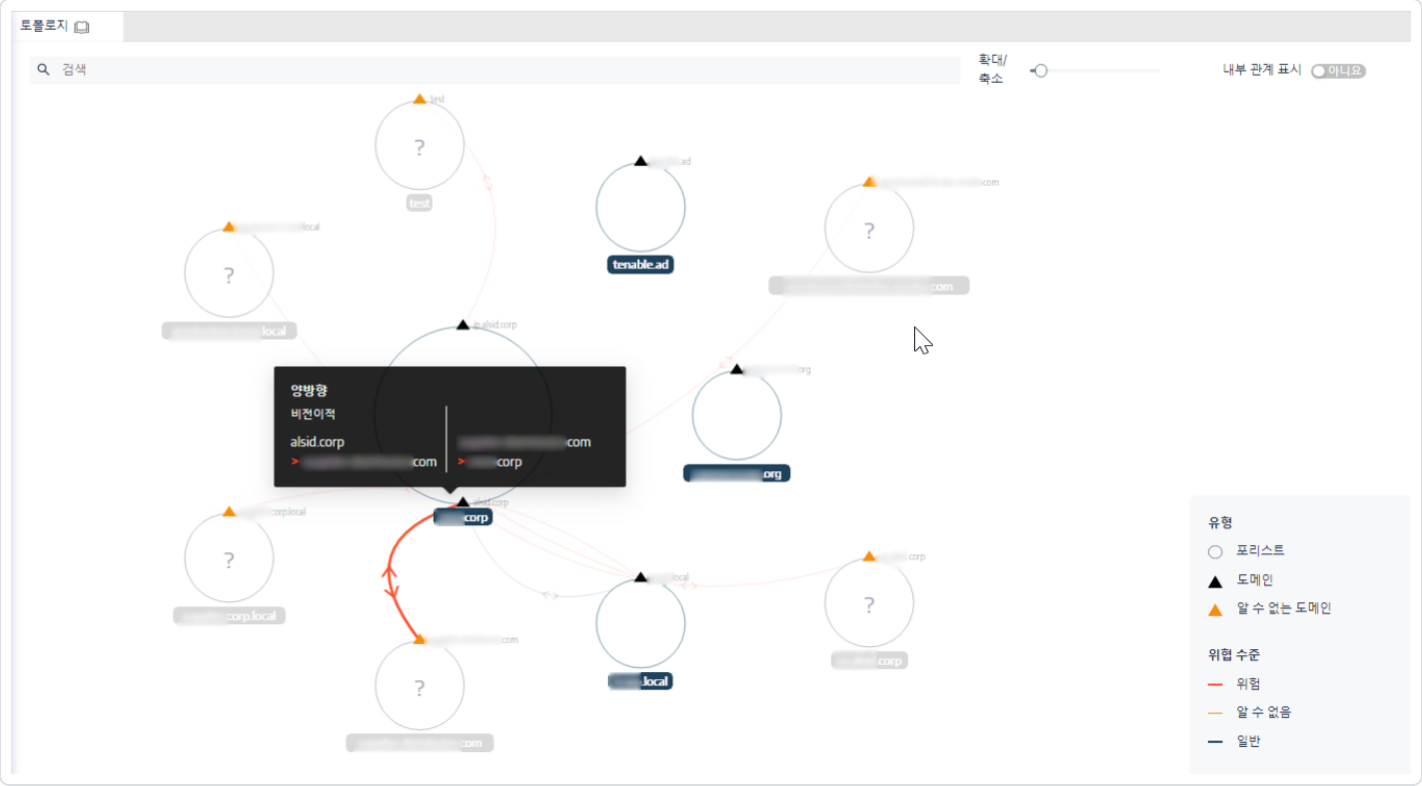
참고: YARA는 주로 맬웨어 리서치와 탐지에 사용하는 도구 이름입니다. 이 도구는 텍스트 또는 바이너리 패턴에 기반하여 맬웨어군에 대한 설명을 만드는 규칙 기반 접근 방식을 제공합니다. 설명은 기본적으로 YARA 규칙 이름이며 이러한 규칙은 여러 개의 문자열과 부울 식 하나로 이루어진 세트로 구성됩니다(출처: wikipedia.org).

참고 항목

- 공격 지표
- 공격 지표 세부 정보

토폴로지

토폴로지 페이지는 Active Directory의 대화형 그래픽 시각화를 제공합니다. **토폴로지 그래프**는 포리스트 및 도메인과 이들 사이에 존재하는 트러스트 관계를 표시합니다.



토폴로지 페이지를 여는 방법:

- Tenable Identity Exposure에서 왼쪽 탐색 메뉴에서 **토폴로지**를 클릭합니다.

  AD를 그래픽으로 나타낸 토폴로지 창이 열립니다.

도메인을 검색하는 방법:

- **토폴로지** 창의 **검색** 상자에 도메인 이름을 입력합니다.

  Tenable Identity Exposure에서 도메인을 강조 표시합니다.

그래프를 확대하는 방법:

- **토폴로지** 창에서 **확대/축소** 슬라이더를 클릭하여 그래프 크기를 조정합니다.

두 도메인 사이 링크를 표시하는 방법:

- **토폴로지** 창에서 **내부 관계 표시**를 클릭하여 토글을 **예**로 바꿉니다.

도메인에 관한 세부 정보를 표시하는 방법:

- **토폴로지** 창에서 도메인 이름의 ▲를 클릭합니다.

  도메인 세부 정보 창이 열리며 탐지된 위험 노출 지표(IoE)와 해당 도메인의 규정 준수 점수가 표시됩니다. IoE의 타일을 클릭하면 자세한 정보를 드릴다운할 수 있습니다.

참고 항목

- 트러스트 관계
- 위험한 트러스트

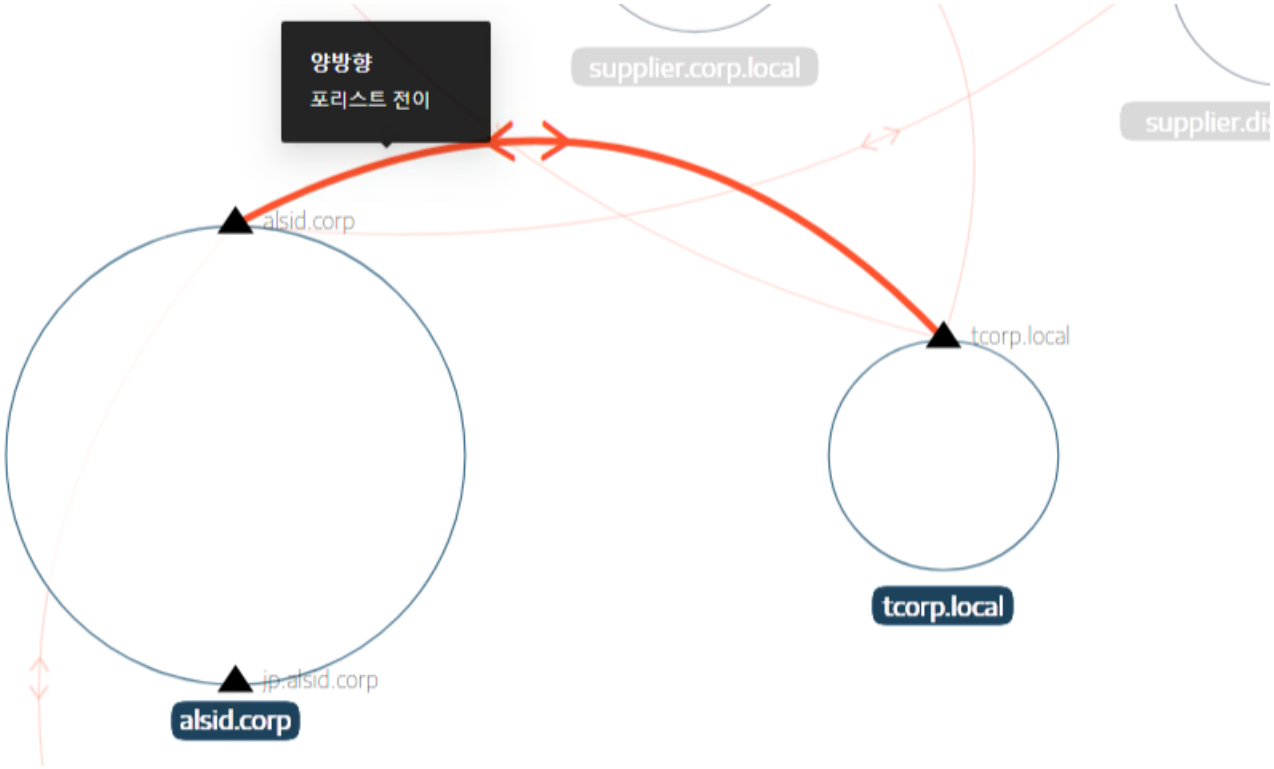
트러스트 관계

토폴로지 그래프에 있는 도메인 사이의 구부러진 화살표는 트러스트 관계를 나타냅니다.

트러스트 관계를 표시하는 방법:

- 토폴로지 그래프에서 구부러진 화살표를 마우스로 가리킵니다.

  Tenable Identity Exposure에서 두 엔터티 사이의 특정 특성을 나타내는 트러스트 관계를 표시합니다.



트러스트 관계의 색은 그 관계의 위협 수준에 따라 다릅니다.

- **빨간색**은 위험한 트러스트
- **주황색**은 일반 트러스트
- **파란색**은 알 수 없는 트러스트

자세한 내용은 위험한 트러스트을 참조하십시오.

트러스트 특성 정보는 트러스트 방향을 **단방향** 또는 **양방향**(받음/보냄)으로 나타내고 다음 중 하나의 값을 표시합니다.

값	설명
비전이적	기본적으로, 포리스트 내부의 트러스트는 전이적 트러스트입니다. Tenable Identity Exposure에서는 이 플래그를 사용하여 비전이적 트러스트로 변환합니다. 반면, 포리스트 간 트러스트는 기본적으로 비전이적이므로 포리스트 전이 플래그가 있습니다. Tenable Identity Exposure에서는 포리스트 내에 도메인 간 트러스트가 있으면 이 값을 표시합니다. 트러스트는 액세스 권한을 부여하지 않으며 포리스트를 넘어 상호 연결된 도메인에 어떤 권한도 위임하지 않습니다.
포리스트 전이적	두 포리스트 사이에 전이적 트러스트가 있음을 나타냅니다. 다른 도메인에 부여된 트러스트를 트러스트된 포리스트에 전달할 수 있습니다.
포리스트 내	같은 포리스트 내에 도메인 간 트러스트가 있음을 나타냅니다. `WITHIN_FOREST`와 `QUARANTINED_DOMAIN`이 둘 다 있는 경우, 해당 트러스트를 **QuarantinedWithinForest**라고 합니다.
상위 수준만	Windows 2000 및 그 이후 버전의 운영 체제를 실행하는 클라이언트만 이 트러스트를 사용할 수 있음을 나타냅니다.
외부로 간주	(`FOREST_TRANSITIVE`가 적용되는 경우에만) 트러스트의 외부 유형을 나타냅니다. Tenable Identity Exposure에서 해당 트러스트의 보안 식별자(SID) 필터링을 수정하고 상대 식별자(RID)가 1,000보다 크거나 같은 SID만 포리스트를 통과하도록 승인합니다.
격리됨	Tenable Identity Exposure에서 해당 트러스트에 대하여 RID가 1,000보다 크거나 같은 SID 필터링을 사용함을 나타냅니다. 기본적으로 Tenable Identity Exposure에서는 이것을 외부 트러스트에 대해서만 사용으로 설정하지만, 상위/하위 트러스트 또는 포리스트 트러스트에도 적용할 수 있습니다.
교차 조직 인증	Tenable Identity Exposure에서 선택적 인증을 사용으로 설정했으며 도메인 또는 포리스트 트러스트 전체에서 사용할 수 있음을 나타냅니다.
선택적 인증	교차 조직 인증을 참조하십시오.
TGT 위임 없는 교차 조	트러스트된 도메인의 위임이 완전히 사용 중지된 경우에 표시됩니다(발행된 서비스 티켓의 ok-as-delegate 옵션을 설정하지 않음).

직	
RC4 암호화:	트러스트가 Kerberos 교환을 위해 RC4 암호화 키를 지원함을 나타냅니다. 이 플래그는 `trustType`이 `TRUST_TYPE_MIT`에 적용되는 경우에만 있습니다.
AES 키	트러스트가 Kerberos 교환을 위해 AES 암호화 키를 지원함을 나타냅니다.
PIM 트러스트	`FOREST_TRANSITIVE` 및 `TREAT_AS_EXTERNAL` 플래그가 적용되고 `QUARANTINED_DOMAIN` 플래그가 없는 경우, PIM 트러스트 플래그는 트러스트된 포리스트가 SID 필터링(로컬 SID가 이 트러스트를 통과할 수 있음)과 관련하여 권한 있는 ID를 관리함(권한 있는 ID 관리)을 나타냅니다. PIM 트러스트는 배스천 포리스트를 구현하는 역할을 합니다.
특성 없음	외부 트러스트에 특정 특성이 없음을 나타냅니다.

위험한 트러스트

트러스트 관계의 색은 그 관계의 위협 수준에 따라 다릅니다.

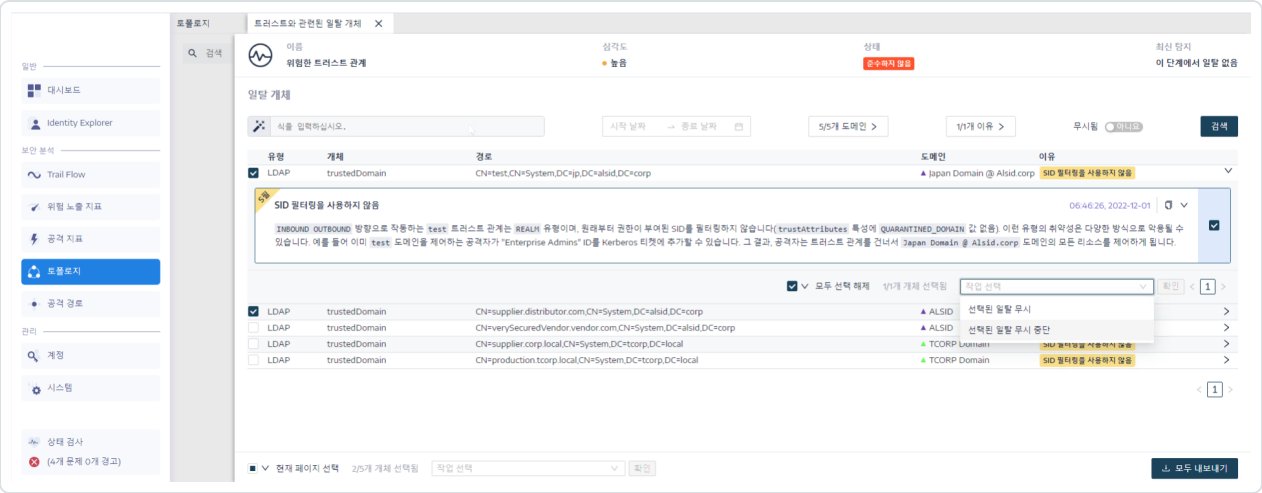
- **빨간색**은 위험한 트러스트
- **주황색**은 일반 트러스트
- **파란색**은 알 수 없는 트러스트

위험한 트러스트를 조사하는 방법:

1. 토폴로지 그래프에서 구부러진 화살표를 클릭합니다.

   트러스트와 관련된 일탈 개체 창이 열립니다.

   > **팁**: 이 위험한 트러스트 관계 창에 표시된 이벤트의 세부 정보는 모두 **위험한 트러스트 관계** 위험 노출 지표(**위험 노출 지표** 탐색 메뉴에서도 액세스 가능)에도 연결되어 있습니다.



2. 목록의 일탈 개체를 가리키고 클릭하면 세부 정보가 표시됩니다.

일탈 개체를 내보내는 방법:

1. 토폴로지 그래프에서 구부러진 화살표를 클릭합니다.

   트러스트와 관련된 일탈 개체 창이 열립니다.

2. **모두 내보내기**를 클릭합니다.

   일탈 개체 내보내기 창이 열립니다.

3. **내보내기 형식** 상자에서 드롭다운 화살표를 클릭하여 형식을 선택합니다.
4. **모두 내보내기**를 클릭합니다.

   Tenable Identity Exposure에서 선택한 형식으로 파일을 컴퓨터에 다운로드합니다.
5. **X**를 클릭하여 창을 닫습니다.

공격 경로

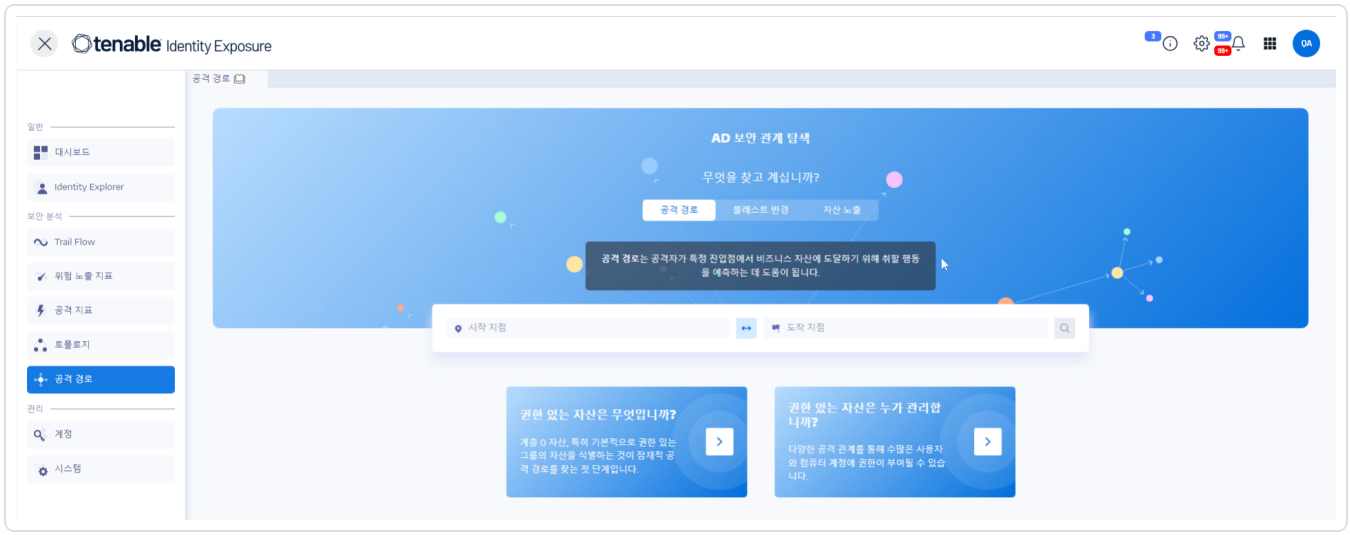
Tenable Identity Exposure에는 다양한 방식으로 그래픽 표현을 통해 비즈니스 자산의 잠재적인 취약성을 표시합니다.

- **공격 경로**: 한 진입 지점에서 한 자산을 침해하기 위해 공격자가 취할 수 있는 가능한 경로를 표시합니다.
- **블래스트 반경**: 모든 자산에서 Active Directory 내부로 이동하기 위해 가능한 내부 확산 이동 방법을 표시합니다.
- **자산 노출**: 한 자산의 통제권을 장악할 가능성이 있는 모든 경로를 표시합니다.

공격 경로를 표시하는 방법:

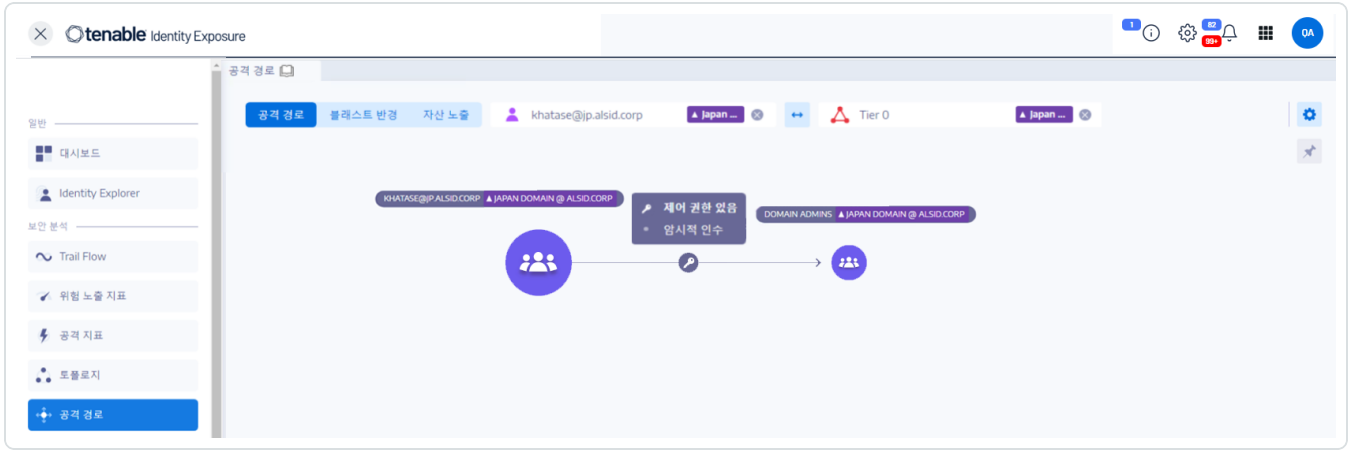
1. Tenable Identity Exposure의 사이드바 메뉴에서 **공격 경로**를 클릭합니다.

   공격 경로 창이 표시됩니다.



2. 배너에서 **공격 경로**를 클릭합니다.
3. **시작 지점** 상자에 진입 지점에 있는 자산을 입력합니다.
4. **도착 지점** 상자에 경로 끝에 있는 자산을 입력합니다.
5. 아이콘을 클릭합니다.

   Tenable Identity Exposure에서 두 자산 사이의 공격 경로를 표시합니다.



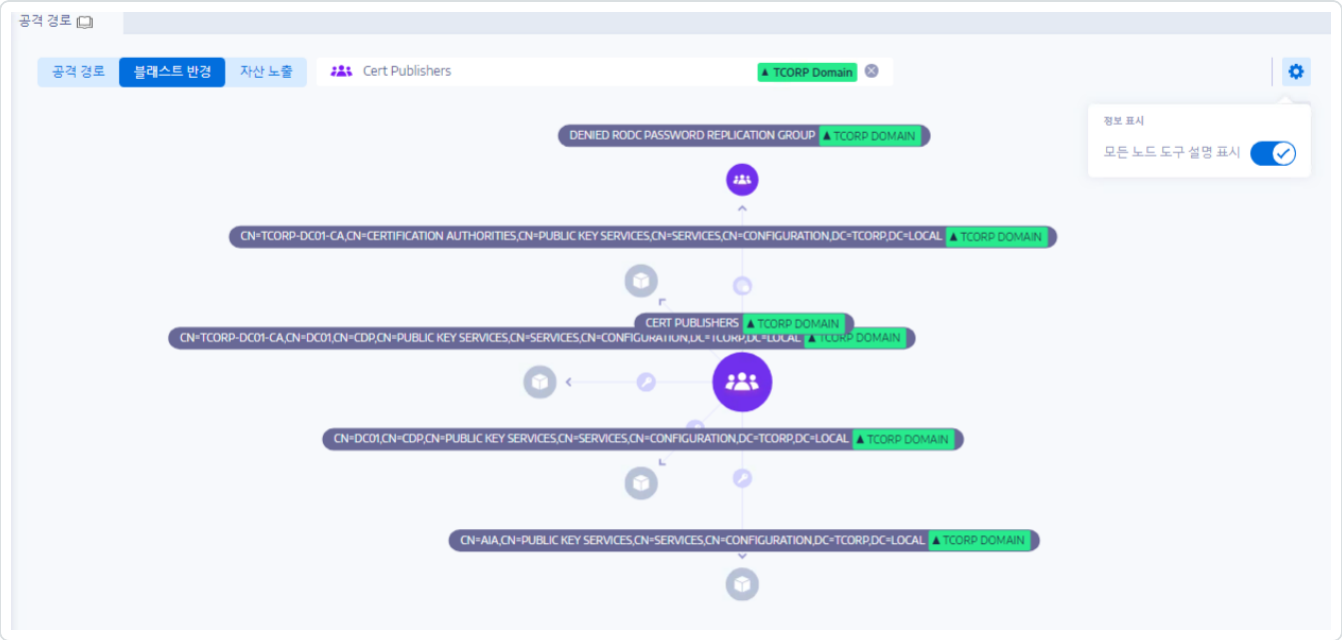
6. 선택 사항으로,  아이콘을 클릭하여 다음과 같은 작업을 수행할 수도 있습니다.
    - **확대/축소** 슬라이더를 클릭하여 그래픽 배율을 조정합니다.
    - **모든 노드 도구 설명 표시** 토글을 클릭하여 해당 자산에 관한 정보 표시를 설정합니다.

블래스트 반경을 표시하는 방법:

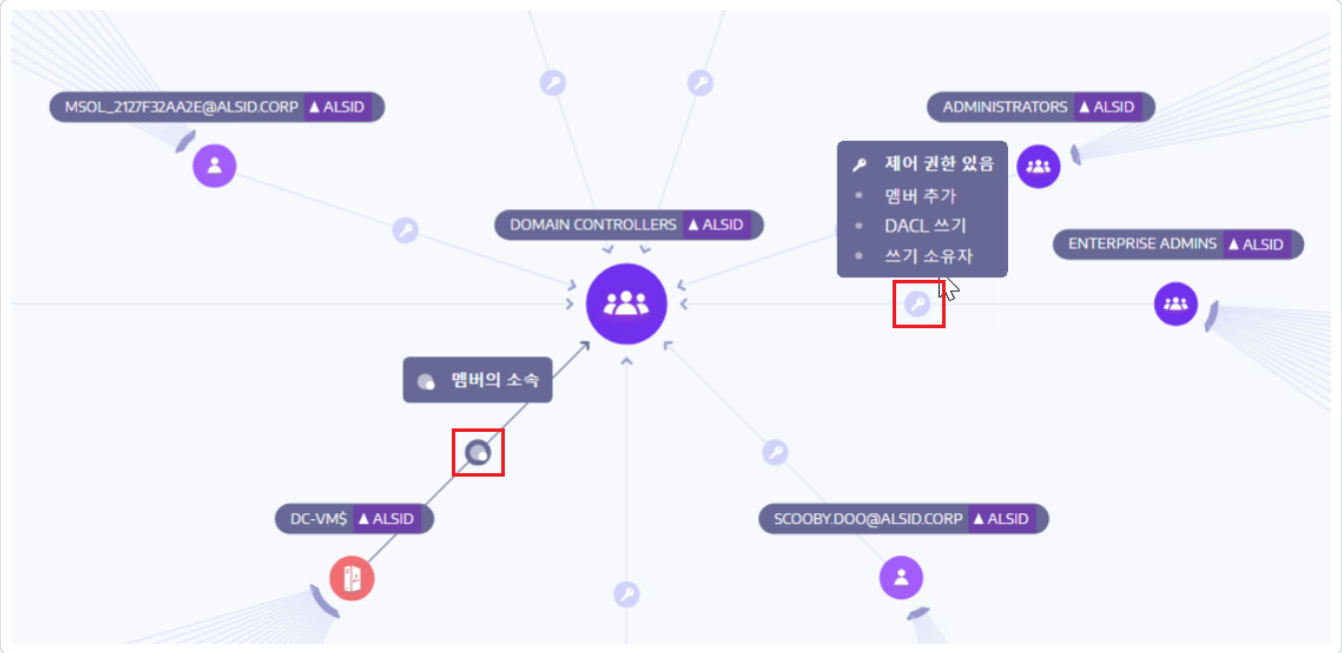
1. Tenable Identity Exposure의 사이드바 메뉴에서 **공격 경로**를 클릭합니다.

   공격 경로 창이 표시됩니다.
2. 배너에서 **블래스트 반경**을 클릭합니다.
3. **개체 검색** 상자에 자산 이름을 입력합니다.
4.  아이콘을 클릭합니다.

   Tenable Identity Exposure에서 해당 자산에서 퍼지는 내부망 연결을 표시합니다.



5. 자산 사이의 화살표에 있는 아이콘을 클릭하면 자산 사이의 관계가 표시됩니다.



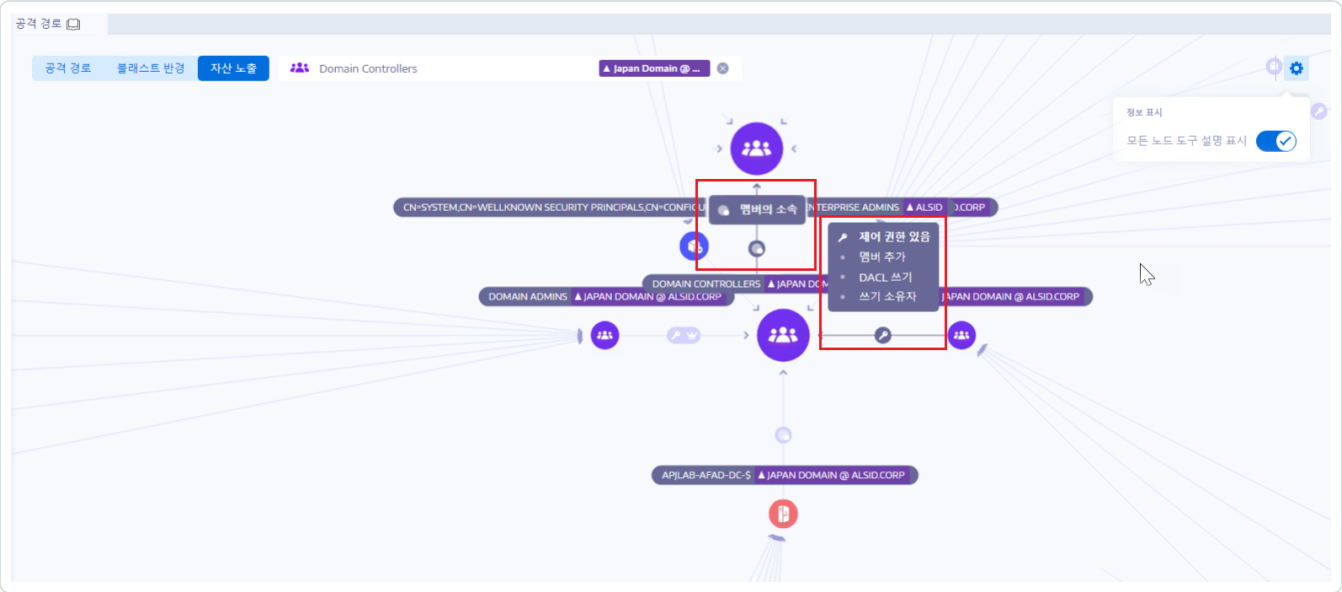
자산 노출을 표시하는 방법:

1. 블래스트 반경을 표시하는 방법:
2. Tenable Identity Exposure의 사이드바 메뉴에서 **공격 경로**를 클릭합니다.

   공격 경로 창이 표시됩니다.

3. 배너에서 **자산 노출**을 클릭합니다.
4. **개체 검색** 상자에 자산 이름을 입력합니다.
5. 아이콘을 클릭합니다.

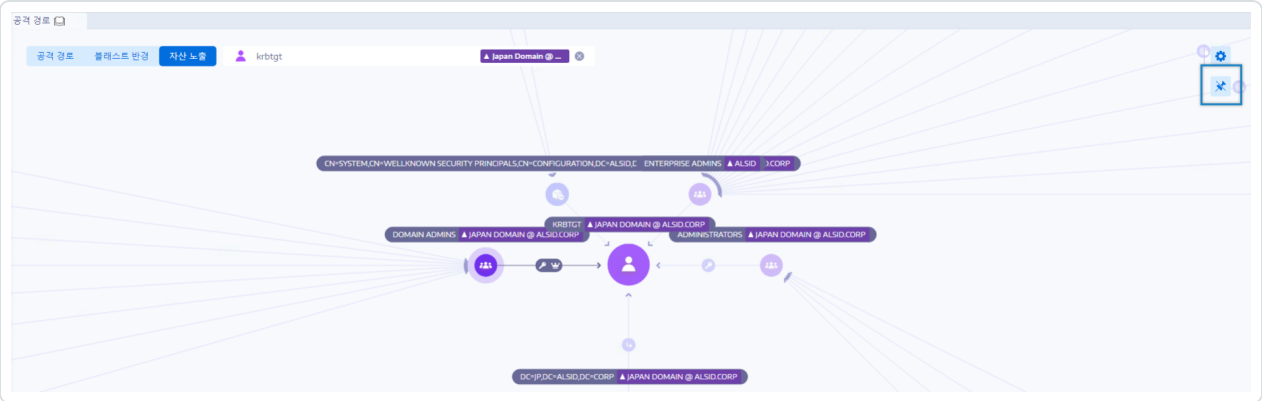
   Tenable Identity Exposure에서 자산으로 이어지는 경로와 해당 자산 사이의 관계를 표시합니다.
6. 자산 사이의 화살표에 있는 아이콘을 클릭하면 자산 사이의 관계가 표시됩니다.



공격 경로를 고정하는 방법:

1. 강조 표시하려는 공격 경로의 노드를 클릭합니다.

   Tenable Identity Exposure에서 그 공격 경로를 화면에 고정합니다.
2. 공격 경로를 고정 해제하려면 아이콘을 클릭하거나 다른 공격 경로의 다른 노드를 클릭합니다.

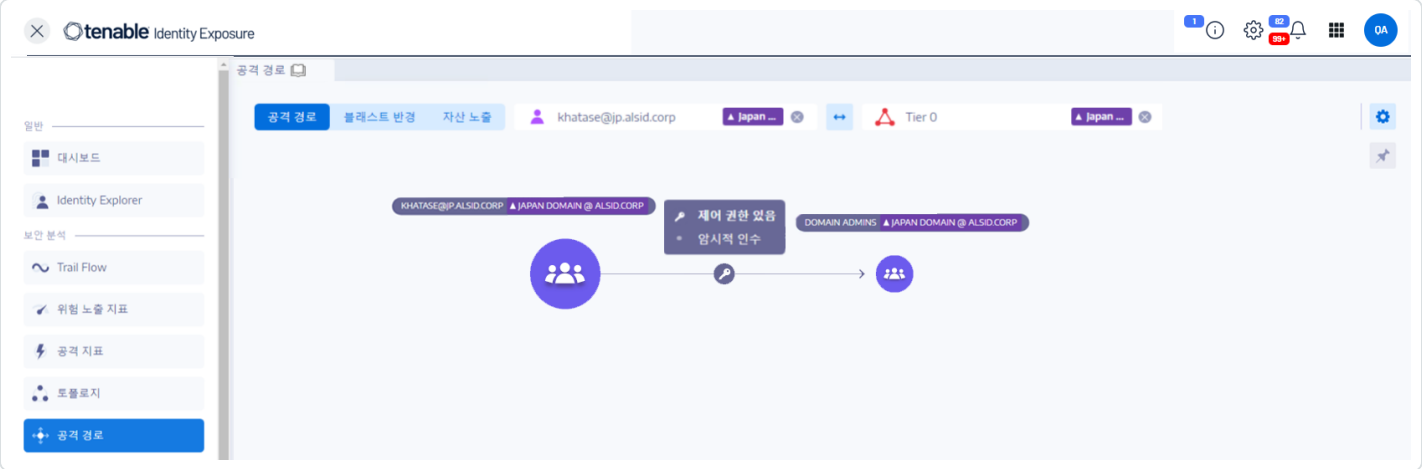

공격 경로
공격 경로
블래스트 반경
자산 노출
krbtgt
Japan Domain @ ...
CN=SYSTEM,CN=WELLKNOWN SECURITY PRINCIPALS,CN=CONFIGURATION,DC=ALSID,C
ENTERPRISE ADMINS
ALSID
)CORP
KRBTGT
JAPAN DOMAIN @ ALSID.CORP
DOMAIN ADMINS
JAPAN DOMAIN @ ALSID.CORP
ADMINISTRATORS
JAPAN DOMAIN @ ALSID.CORP
DC=JP,DC=ALSID,DC=CORP
JAPAN DOMAIN @ ALSID.CORP

참고 항목

- 공격 관계

공격 관계

공격 관계는 소스 노드에서 대상 노드로 단방향입니다. 관계는 전이적이므로, 공격자가 체인으로 연결하여 "공격 경로"를 만들 수 있습니다.



Tenable Identity Exposure에는 다음과 같은 공격 관계가 있습니다.

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유

- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

키 자격 증명 추가

설명

소스 보안 주체는 키 트러스트 계정 매핑(키 자격 증명 또는 "섀도 자격 증명"으로도 알려짐)을 악용하여 대상을 가장할 수 있습니다.

이것은 소스에 대상의 `msDS-KeyCredentialLink` 특성을 편집할 권한이 있기 때문에 가능합니다.

WHfB(Windows Hello for Business)는 보통 이 기능을 사용하지만, 이 기능을 사용하지 않더라도 공격자가 이를 악용할 수 있습니다.

악용

소스 보안 주체를 침해하는 공격자는 Whisker나 DSInternals와 같은 전문 해커 도구를 사용해 대상 컴퓨터의 `msDS-KeyCredentialLink` 특성을 편집해야 합니다.

공격자의 목표는 이 대상의 특성에 새 인증서(자신이 이 특성의 비공개 키를 가지고 있음)를 추가하는 것입니다. 그러면 알려진 프라이빗 키를 사용해 대상으로 인증할 수 있으며, 이 경우 Kerberos PKINIT 프로토콜을 사용해 TGT를 획득합니다. 이 프로토콜은 공격자는 대상의 NTLM 해시를 가져올 수도 있습니다.

수정

여러 네이티브하게 권한이 있는 보안 주체가 기본적으로 이 권한을 소유합니다. 구체적으로 계정 운영자, 관리자, 도메인 관리자, 엔터프라이즈 관리자, 엔터프라이즈 키 관리자, 키 관리자와 시스템 등이 이에 해당합니다. 이와 같은 합법적인 보안 주체는 수정이 필요하지 않습니다.

이 특성을 수정할 적법한 이유가 없는 소스 보안 주체의 경우, 이 권한을 제거해야 합니다. "모든 속성 쓰기", "msDS-AllowedToActOnBehalfOfOtherIdentity 쓰기", "전체 제어" 등의 권한을 검색하십시오.

참고 항목

- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함

- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

멤버 추가

설명

소스 보안 주체는 자기 자신(검증된 쓰기 권한) 또는 다른 누구라도(속성 쓰기 권한) 대상 그룹의 멤버에 추가하여 해당 그룹에 주어진 액세스 권한을 유리하게 이용할 수 있습니다.

이 작업을 수행하는 악의적인 보안 주체는 "멤버 관계" 공격 관계를 만들게 됩니다.

악용

소스 보안 주체를 침해하는 공격자는 "넷 그룹/도메인"과 같은 네이티브 Windows 명령, "Add-ADGroupMember"와 같은 PowerShell, "Active Directory 사용자 및 컴퓨터"와 같은 관리 도구나 PowerSploit와 같은 전용 해커 도구 등을 통해 대상 그룹의 "멤버" 특성을 편집하기만 하면 됩니다.

수정

소스 보안 주체에게 대상 그룹에 멤버를 추가할 권한이 필요하지 않은 경우, 이 권한을 반드시 제거해야 합니다.

대상 그룹의 보안 설명자를 수정하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 **속성** > **보안**을 마우스 오른쪽으로 클릭합니다.
2. "멤버 쓰기", "모든 속성 쓰기", "전체 제어", "모든 확인된 쓰기", "자신을 멤버로 추가/제거" 등의 권한을 제거합니다.

> **참고**: 한 그룹은 Active Directory 트리에서 수준이 더 높은 개체로부터 권한을 상속할 수 있습니다.

참고 항목

- 키 자격 증명 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync

- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

작업 허용

설명

소스 보안 주체가 대상 컴퓨터에서 Kerberos 리소스 기반 제한된 위임을 수행할 수 있습니다. 이것은 이 주체가 대상 컴퓨터에서 실행 중인 모든 서비스에 대하여 Kerberos를 사용해 인증하면 어느 사용자로든 가장할 수 있다는 의미입니다.

따라서 이렇게 하면 대상 컴퓨터 전체를 침해하는 결과를 초래하는 경우가 많습니다.

이 공격은 일명 리소스 기반 제한 위임(Resource-Based Constrained Delegation, RBCD), Kerberos 리소스 기반 제한 위임(KRBCD), 리소스 기반 Kerberos 제한 위임(RBKCD)으로도 알려져 있으며 "다른 ID를 대신하여 작업할 수 있습니다".

악용

소스 보안 주체를 침해하는 공격자는 Rubeus와 같은 전용 해커 도구를 사용해 적법한 Kerberos 프로토콜 확장자(S4U2self 및 S4U2proxy)를 악용해 Kerberos 서비스 티켓을 위조하고 표적 사용자로 가장할 수 있습니다. 공격자는 권한 있는 사용자로 가장하여 권한 있는 액세스를 얻을 가능성이 큽니다.

공격자는 서비스 티켓을 위조한 다음, Kerberos와 호환되는 각종 네이티브 관리 도구나 전문 해커 도구를 사용해 원격으로 임의의 명령을 실행할 수 있습니다.

악용 시도가 성공하려면 다음과 같은 제약을 충족해야 합니다.

- 소스와 대상 보안 주체에 ServicePrincipalName이 있어야 합니다. Tenable Identity Exposure는 이 조건 없이 이 공격 관계를 만들지 않습니다.
- 스푸핑 표적인 계정이 "중요하고 위임할 수 없음"(UserAccountControl의 `ADS_UF_NOT_DELEGATED`)으로 표시되거나 "보호된 사용자" 그룹의 멤버여서는 안 됩니다. 이러한 계정은 Active Directory가 위임 공격으로부터 보호하기 때문입니다.

수정

소스 보안 주체에게 대상 컴퓨터에서 Kerberos 리소스 기반 제한 위임(RBCD)을 수행할 권한이 필요하지 않은 경우, 제거해야 합니다. 이 수정은 대상 쪽에서 수행해야 합니다("위임 허용" 위임 공격 관계와는 다름).

RBCD는 "Active Directory 사용자 및 컴퓨터"와 같은 기존의 그래픽 관리 도구로 관리할 수 없습니다. 대신 PowerShell을 사용해 `msDS-AllowedToActOnBehalfOfOtherIdentity` 특성의 내용을 수정해야 합니다.

다음 명령을 사용하여 대상에서 작업이 허용된 소스 보안 주체를 나열합니다("액세스:" 섹션에서).

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

나열된 보안 주체 중 원하는 것이 없으면, 다음 명령으로 모두 지울 수 있습니다.

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

목록에서 보안 주체를 하나만 제거해야 하는 경우, 아쉽게도 Microsoft에서 직접적인 명령을 제공하지 않습니다. 제거할 항목만 뺀 동일한 목록으로 해당 특성을 덮어써야 합니다. 예를 들어 "sourceA", "sourceB"와 "sourceC"가 모두 허용되어 있고 "sourceB"만 제거하려는 경우, 다음을 실행합니다.

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

마지막으로, 중요한 권한 있는 계정이 그러한 위임 공격에 노출되는 정도를 제한하기 위한 일반적인 권장 사항으로, Tenable Identity Exposure에서는 관련된 운영상 영향을 주의하여 확인한 후에 "중요하고 위임할 수 없음"(`ADS_UF_NOT_DELEGATED`)으로 표시하거나 "보호된 사용자" 그룹에 추가하는 것을 권장합니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음

- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

위임 허용

설명

소스 보안 주체가 대상 컴퓨터에서 프로토콜 전환을 사용하여 Kerberos 제한 위임(KCD)을 수행할 수 있습니다. 이것은 이 주체가 대상 컴퓨터에서 실행 중인 모든 서비스에 대하여 Kerberos를 사용해 인증하면 어느 사용자로든 가장할 수 있다는 의미입니다.

따라서 이렇게 하면 대상 컴퓨터 전체를 침해하는 결과를 초래하는 경우가 많습니다.

악용

소스 보안 주체를 침해하는 공격자는 Rubeus와 같은 전용 해커 도구를 사용해 적법한 Kerberos 프로토콜 확장자(S4U2self 및 S4U2proxy)를 악용해 Kerberos 서비스 티켓을 위조하고 표적 사용자로 가장할 수 있습니다. 공격자는 권한 있는 액세스를 얻기 위해 권한 있는 사용자로 가장할 가능성이 큽니다.

공격자는 서비스 티켓을 위조한 다음, Kerberos와 호환되는 각종 네이티브 관리 도구나 전문 해커 도구를 사용해 원격으로 임의의 명령을 실행할 수 있습니다.

악용 시도가 성공하려면 다음과 같은 제약을 충족해야 합니다.

- 소스 보안 주체가 프로토콜 전환에 대해 사용으로 설정되어야 합니다(UserAccountControl의 `ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION`/위임 GUI의 "모든 인증 프로토콜 사용"). 좀 더 정확히 말하자면, 공격은 프로토콜 전환 없이도(위임 GUI의 "Kerberos만 사용") 작동할 수 있지만 공격자가 우선 대상 사용자에게서 소스 보안 주체로 Kerberos 인증을 강제해야 하므로 공격이 더 어려워집니다. 따라서 이 경우 Tenable Identity Exposure에서는 공격 관계를 만들지 않습니다.
- 소스와 대상 보안 주체에 ServicePrincipalName이 있어야 합니다. Tenable Identity Exposure는 이 조건 없이 이 공격 관계를 만들지 않습니다.
- 스푸핑 표적인 계정이 "중요하며 위임할 수 없음"(UserAccountControl의 `ADS_UF_NOT_DELEGATED`)으로 표시되어서도, "보호된 사용자" 그룹의 멤버여서도 안 됩니다. 이러한 계정은 Active Directory가 위임 공격으로부터 보호하기 때문입니다.

반대로, 위임이 허용된 대상 컴퓨터는 SPN(Service Principal Name)이 지정되므로 특정 서비스를 포함합니다(예: SMB의 경우 "cifs/host.example.net", HTTP의 경우 "http/host.example.net" 등). 단, 공격

자는 실제로 "sname 대체 공격"을 사용해 동일한 대상 계정 아래에서 실행되는 다른 모든 SPN과 서비스를 표적으로 삼을 수 있습니다. 따라서 이것은 제한 사항이 아닙니다.

수정

소스 보안 주체에게 대상 컴퓨터에서 Kerberos 제한 위임(KCD)을 수행할 권한이 필요하지 않은 경우, 제거해야 합니다. 수정은 소스 쪽에서 수행해야 합니다("작업 허용" 위임 공격 관계와는 다름).

소스 보안 주체를 제거하는 방법:

1. "Active Directory 사용자 및 컴퓨터" 관리 GUI에서 소스 개체의 **속성** > **위임** 탭으로 이동합니다.
2. 대상에 해당하는 서비스 주체 이름을 제거합니다.
3. 이 소스에서 위임을 원하지 않으면 모든 SPN을 제거하고 "이 컴퓨터를 위임에 대해 신뢰하지 않음"을 선택합니다.

또는 PowerShell을 사용해 소스의 "msDS-AllowedToDelegateTo" 특성을 수정할 수 있습니다.

- 예를 들어, PowerShell에서 이 명령을 실행하여 모든 값을 바꿉니다.

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-
AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```

- 이 소스에서 위임을 원하지 않는 경우, 다음 명령을 실행하여 특성을 지웁니다.

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-
AllowedToDelegateTo"
```

프로토콜 전환을 사용 중지하여 위험을 완화하면서도 이 공격 경로를 완전히 닫지는 않을 수도 있습니다. 이렇게 하려면 모든 보안 주체가 소스에 NTLM이 아니라 Kerberos만 사용하여 연결해야 합니다.

프로토콜 전환을 사용 중지하는 방법:

1. "Active Directory 사용자 및 컴퓨터" 관리 GUI에서 소스 개체의 **속성** > **위임** 탭으로 이동합니다.
2. "모든 인증 프로토콜 사용" 대신 "Kerberos만 사용"을 선택합니다.

아니면 PowerShell에서 다음 명령을 실행하여 프로토콜 전환을 사용 중지할 수 있습니다.

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation
$false
```

마지막으로, 중요한 권한 있는 계정이 그러한 위임 공격에 노출되는 정도를 제한하기 위한 일반적인 권장 사항으로, Tenable Identity Exposure에서는 관련된 운영상 영향을 주의하여 확인한 후에 "중요하고 위임할 수 없음"(`ADS_UF_NOT_DELEGATED`)으로 표시하거나 "보호된 사용자" 그룹에 추가하는 것을 권장합니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

GPO에 속함

설명

SYSVOL공유의 소스 GPO 파일 또는 폴더가 대상 GPC(GPO)에 속합니다. 이는 이것이 해당 GPO가 적용하는 설정 또는 프로그램/스크립트를 정의함을 나타냅니다.

악용

이것은 공격자가 단독으로 사용할 만한 공격 관계가 아닙니다. 그렇지만 예를 들어 GPO에 속하는 GPO 파일/폴더에 대한 제어 권한을 가진 공격자가 공격 경로의 끝에 있는 사용자/컴퓨터를 상대로 임의의 설정을 적용하거나 스크립트를 실행할 수 있는 공격 경로 전체를 표시할 수 있습니다.

수정

이 관계는 SYSVOL에 위치한 GPO 파일과 폴더가 상응하는 GPC(GPO) 개체와 어떤 식으로 관련되어 있는지 보여줍니다. 이것은 일반적이고 의도된 것입니다.

따라서 수정할 필요가 없습니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO

- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

DCSync

설명

DCSync는 도메인 컨트롤러가 변경 사항을 복제하는 데만 사용하는 적법한 Active Directory 기능이지만 불법 보안 주체도 이것을 사용할 수 있습니다.

소스 보안 주체는 DCSync 기능을 사용해 대상 도메인에서 중요한 암호(비밀번호 해시, Kerberos 키 등)을 요청할 수 있고, 궁극적으로 도메인을 완전히 침해하는 결과를 초래할 수 있습니다.

암호를 가져오려면 보안 권한이 두 개 필요합니다. 하나는 "디렉터리 변경 사항 복제"(`DS-Replication-Get-Changes`)이고 다른 하나는 "디렉터리 변경 사항 모두 복제"(`DS-Replication-Get-Changes-All`)입니다. 이 관계는 소스에 이러한 권한을 둘 다 부여하는 경우에만 발생합니다. 권한은 직접 부여할 수도 있고 중첩된 그룹 멤버 자격을 통해 부여할 수도 있습니다.

악용

소스 보안 주체를 침해하는 공격자는 *mimikatz* 또는 *impacket*와 같은 전용 해커 도구를 사용해 암호를 가져올 수 있습니다.

- **Golden ticket**: "krbtgt" 계정의 비밀번호 해시를 가져오면 발생합니다. 이것을 통해 Kerberos TGT를 위조할 수 있고 모든 컴퓨터/서비스에서 누구든 가장할 수 있습니다. 특히 이렇게 하면 도메인의 모든 컴퓨터에 대해 관리 권한을 부여하게 됩니다.
- **Silver ticket**: 컴퓨터/서비스 계정의 비밀번호 해시를 가져오면 발생합니다. 이렇게 하면 Kerberos 서비스 티켓을 위조할 수 있고 주어진 컴퓨터/서비스에서 누구든 가장할 수 있습니다.

수정

기본적으로 DCSync를 활용하도록 허용된 적법한 보안 주체는 다음과 같습니다.

- 관리자
- 도메인 관리자
- 엔터프라이즈 관리자
- 시스템

또한, Microsoft Entra ID Connect 구성을 사용하면 비밀번호 해시 동기화 서비스 계정(MSOL_...)이 DCSync를 활용하도록 허용합니다.

마지막으로, 특정 보안 도구의 서비스 계정을 검색할 수도 있습니다. 특히 비밀번호 감사 솔루션이 대표적입니다. 이러한 솔루션이 적합한지 책임자에게 문의하여 확인하십시오.

소스 보안 주체에게 DCSync를 수행할 적법한 필요가 없는 경우, 이 권한을 제거해야 합니다.

대상 도메인의 보안 설명자를 수정하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 도메인 이름을 마우스 오른쪽으로 클릭하고 속성 > 보안을 선택합니다.
2. 불법 보안 주체의 "디렉터리 변경 사항 복제" 및 "디렉터리 변경 사항 모두 복제" 권한을 제거합니다.

참고: DCSync 관계는 중첩된 그룹 멤버 자격의 권한을 통해 발생할 수 있습니다. 따라서 정확한 상황에 따라 그룹 자체를 제거해야 하거나 해당 그룹의 일부 멤버만 제거해야 할 수도 있습니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유

- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

작업 허용 권한 부여

설명

소스 보안 주체는 대상 컴퓨터와 관련하여 자신 또는 다른 누구에게 작업 허용 관계를 부여할 수 있습니다. 이렇게 하면 Kerberos RBCD 위임 공격을 통해 대상 컴퓨터가 완전히 침해되는 경우가 많습니다.

이것은 소스에 대상의 "msDS-AllowedToActOnBehalfOfOtherIdentity" 특성을 편집할 권한이 있기 때문에 가능합니다.

이 작업을 수행하는 악의적인 보안 주체는 "작업 허용" 공격 관계를 만들 수 있습니다.

악용

소스 보안 주체를 침해하는 공격자는 반드시 PowerShell을 사용해 대상 컴퓨터의 `msDS-AllowedToActOnBehalfOfOtherIdentity` 특성을 편집해야 합니다(예: "Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount ...").

수정

여러 네이티브하게 권한이 있는 보안 주체가 기본적으로 이 권한을 소유합니다. 구체적으로 계정 운영자, 관리자, 도메인 관리자, 엔터프라이즈 관리자와 시스템 등이 이에 해당합니다. 이들 보안 주체는 합법적이며 수정하지 않아도 됩니다.

Kerberos RBCD는 컴퓨터의 관리자가 해당 컴퓨터에서 위임을 수행할 권한을 이 권한이 필요한 사용자 누구에게나 부여할 수 있도록 고안되었습니다. 이것은 도메인 관리자 수준의 권한이 필요한 다른 Kerberos 위임 모드와는 다릅니다. 이렇게 하면 낮은 수준의 관리자도 이러한 보안 설정을 직접 관리할 수 있습니다. 이것은 위임이라고 하는 원칙입니다. 이 경우, 관계는 합법적입니다.

단, 소스 보안 주체가 대상 컴퓨터의 적법한 관리자가 아닌 경우, 관계는 적법하지 않으며 이 권한을 반드시 제거해야 합니다.

대상 컴퓨터의 보안 설명자를 수정하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 **속성** > **보안**을 마우스 오른쪽으로 클릭합니다.
2. 소스 보안 주체에게 부여된 권한을 제거합니다. "msDS-AllowedToActOnBehalfOfOtherIdentity 쓰기", "모든 속성 쓰기", "계정 제한 사항 쓰기", "전체 제어" 등의 권한을 검색합니다.

참고: 소스 보안 주체는 Active Directory 트리에서 더 높은 위치의 개체로부터 권한을 상속할 수 있습니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

SID 기록 있음

설명

소스 보안 주체에는 SIDHistory 특성에 대상 보안 주체의 SID가 있습니다. 이것은 소스가 대상과 같은 권리를 갖고 있음을 의미합니다.

SID 기록은 이전의 SID 기능을 참조하는 모든 인증을 유지하기 위해 여러 도메인 사이에서 보안 주체를 마이그레이션할 때 사용하는 적법한 메커니즘입니다.

다만 이것은 공격자가 사용하는 지속성 메커니즘이기도 합니다. 이것을 사용하면 비밀스런 백도어 계정이 관리자 계정과 같이 바람직한 대상과 동일한 권한을 가질 수 있기 때문입니다.

악용

소스 보안 주체를 침해하는 공격자가 대상 보안 주체로서 직접 인증할 수 있습니다. 대상의 SID가 Active Directory 인증 메커니즘이 생성하는 토큰(NTLM 및 Kerberos)에 투명하게 추가되기 때문입니다.

수정

소스와 대상 보안 주체가 승인된 도메인 마이그레이션과 관련이 있는 경우, 해당 관계를 적법한 것으로 간주하고 어떤 작업을 수행하지 않아도 됩니다. 이 관계는 계속 표시되어 잠재적인 공격 경로를 상기시키는 역할을 합니다.

마이그레이션 후에 원본의 도메인이 삭제되거나 Tenable Identity Exposure에서 구성되지 않는 경우, 대상 보안 주체가 확인되지 않음(unresolved)으로 표시됩니다. 위험은 대상에 있으며 그 대상이 존재하지 않으므로 위험이 존재하지 않고 따라서 수정이 필요하지 않습니다

반대로, 기본적으로 권한 있는 사용자나 그룹에 대한 SID 기록 관계의 경우 Active Directory에서 만드는 것을 방지하므로 악성일 가능성이 매우 큽니다. 이러한 관계가 아마 "DCShadow" 공격과 같은 해커 기술을 사용해 만들어졌을 가능성이 있음을 의미합니다. 이러한 사례는 "SID 기록"과 관련된 IoE에서도 확인됩니다.

이런 경우, Tenable Identity Exposure에서는 Active Directory 포리스트 전체에 대한 포렌식 검사를 추천합니다. 공격자가 소스의 SID 기록을 악의적으로 편집하기 위해 높은 수준의 권한(도메인 관리자나 그와 동급)을 얻은 것이기 때문입니다. 포렌식 검사를 하면 공격에 상응하는 수정 참고 자료로 공격을 분석하고 제거해야 할 잠재적인 백도어를 식별할 수 있습니다.

마지막으로, Microsoft에서는 이 마이그레이션을 완료한 뒤 모든 서비스(SMB 공유, Exchange 등)의 모든 액세스 권한을 수정하여 새 SID를 사용하도록 하고, 불필요한 SIDHistory 값은 제거하도록 권장합니다. 이것이 하우스키핑 모범 사례입니다. 다만, 모든 ACL을 철저하게 식별하여 수정하기는 매우 힘든 작업입니다.

소스 개체 자체에서 SIDHistory 특성을 편집할 권한이 있는 사용자가 SIDHistory 값을 제거할 수 있습니다. 만들기와 달리 이 작업에는 도메인 관리자 권한이 필요하지 않습니다.

이렇게 하려면 PowerShell을 사용할 수밖에 없습니다. Active Directory 사용자 및 컴퓨터와 같은 그래픽 도구는 실패하기 때문입니다. 예:

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

주의: SIDHistory 값을 제거하기는 쉽지만, 이 작업을 되돌리기는 매우 복잡합니다. SIDHistory 값을 다시 만들어야 하며, 그러려면 다른 도메인이 있어야 하고 그 도메인은 서비스 해제될 가능성이 있기 때문입니다. 이 때문에 Microsoft에서는 스냅샷 또는 백업을 준비해두는 것도 권장합니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유

- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

암시적 인수

설명

소스가 계층0 보안 주체입니다. 계층0은 도메인에서 최고 수준의 권한을 소유한 Active Directory 개체 집합입니다. 예를 들어 도메인 관리자나 도메인 컨트롤러 그룹의 멤버가 대표적입니다. 모든 계층0 자산은 도메인 내 다른 모든 개체를 암시적으로 침해할 수 있으며 명시적인 다른 관계가 없더라도 암시적으로 침해할 수 있습니다.

이 관계가 있기 때문에 암시적 권한을 Active Directory에 기본 제공 방식으로 모델링할 수 있습니다. 이러한 권한은 의도된 것으며 문서화되므로, 공격자에게 알려져 있습니다. 그러나 Tenable Identity Exposure에서는 이러한 권한을 일반적인 수단으로 수집할 수 없습니다. 또한 이 단계는 공격 경로 그래프를 간소화합니다. 공격자가 계층0 노드를 침해하는 즉시 다른 명시적 관계를 통과하지 않고 여타 모든 개체를 직접 공격할 수 있기 때문입니다.

간략하게 소스 계층0 자산은 그래프상의 모든 대상 노드에 대하여 모두 "암시적 인수" 관계가 있는 것으로 간주됩니다.

악용

정확한 악용 방식은 표적이 된 소스 계층0 자산의 유형에 따라 다르지만, 이것은 문서화된 기술이며 공격자가 효율적으로 습득합니다.

수정

이 관계는 의도된 것이며 수정할 수 없습니다. 계층0에 도달한 공격자가 추가 공격을 감행하지 못하게 막기란 불가능에 가깝습니다.

공격 경로의 업스트림 관계에 주안점을 두고 수정해야 합니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용

- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

GPO 상속

설명

조직 구성 단위(OU) 또는 도메인(사이트 제외)과 같이 소스를 연결할 수 있는 컨테이너는 LDAP에 대상 OU, 사용자, 장치, DC 또는 읽기 전용 도메인 컨트롤러(RODC)를 포함합니다. 이것은 연결할 수 있는 컨테이너의 하위 개체가 자신이 연결된 GPO를 상속하기 때문입니다("연결된 GPO" 관계 참조).

Tenable Identity Exposure에서는 OU가 상속을 차단할 때마다 이를 감안합니다.

악용

공격 경로의 업스트림에 있는 GPO를 침해하는 데 성공하기만 하면 공격자가 이 관계를 악용할 일이 전혀 없습니다. 이 관계는 연결할 수 있는 컨테이너와 그 아래의 개체에 적용하도록 설계되었습니다(GPO 상속 관계 참조).

수정

대부분의 경우, GPO가 상위 컨테이너에서 연결할 수 있는 하위 컨테이너에 적용되는 것은 일반적이고 적법합니다. 그러나 이 연결로 인해 더 많은 공격 경로가 노출됩니다.

따라서 위험을 완화하려면 GPO를 (가능하면 항상) 조직 구성 단위 계층 구조에서 가장 낮은 수준에 연결하는 것이 좋습니다.

또한 GPO를 다른 공격 관계에 노출하지 않으려면 공격자가 무단으로 수정할 수 없도록 보호해야 합니다.

마지막으로, OU가 "상속 차단" 옵션을 통해 더 높은 수준에서 GPO 상속을 사용 중지할 수도 있습니다. 그러나 이 옵션은 최후의 수단으로만 사용해야 합니다. 이 옵션은 도메인 최고 수준에서 정의한, 보안을 강화할 수 있는 GPO까지 포함해 모든 GPO를 차단하기 때문입니다. 또한 이 때문에 적용된 GPO에 관한 추론도 더 어려워집니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용

- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

연결된 GPO

설명

소스 GPO가 도메인 또는 조직 구성 단위(OU)와 같이, 대상의 연결할 수 있는 컨테이너에 연결되어 있습니다. 이것은 소스 GPO가 대상에 포함된 장치와 사용자에 설정을 할당하고 여기에서 프로그램을 실행할 수 있음을 나타냅니다. 소스 GPO는 "GPO 상속" 관계를 통해 그 아래 컨테이너에 포함된 개체에도 적용됩니다.

궁극적으로 GPO는 자신이 적용되는 장치와 사용자를 침해할 수 있습니다.

악용

공격자는 다른 공격 관계를 통해 소스 GPO부터 침해해야 합니다.

그런 다음, 여러 가지 기술을 동원해 대상에 포함된 장치 및 사용자와 그 아래 항목에 악성 작업을 수행합니다. 예를 들면 다음과 같습니다.

- 적법한 "일회성 예약 작업"을 남용하여 장치에서 임의의 스크립트를 실행합니다.
- 모든 장치에 관리자 권한을 가진 새 로컬 사용자 추가
- MSI 프로그램 설치
- 방화벽 또는 바이러스 백신 사용 중지
- 추가 권한 부여
- 및 이외의 예가 있습니다.

공격자는 "그룹 정책 관리"와 같은 관리 도구나 PowerSploit와 같은 전용 해커 도구를 사용해 GPO의 내용을 편집하여 GPO를 수정할 수 있습니다.

수정

대부분의 경우, GPO를 연결할 수 있는 컨테이너에 연결하는 작업은 일반적이고 적법합니다. 그러나 이 연결로 인해 연결이 발생하는 위치와 그 아래 컨테이너의 공격 표면이 넓어질 수 있습니다.

따라서 위험을 완화하려면 GPO를 (가능하면 항상) 조직 구성 단위 계층 구조에서 가장 낮은 수준에 연결하는 것이 좋습니다.

또한 GPO를 다른 공격 관계에 노출하지 않으려면 공격자가 무단으로 수정할 수 없도록 보호해야 합니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

멤버 관계

설명

소스 보안 주체가 대상 그룹의 멤버입니다. 따라서 그룹이 보유한 모든 액세스 권한의 이점을 누립니다. 예를 들어 파일 공유에 액세스하거나 비즈니스 애플리케이션에서 역할을 가장할 수 있습니다.

악용

공격자는 아무것도 하지 않아도 이 공격 관계를 악용할 수 있습니다. 소스 보안 주체로 인증하기만 하면 로컬 또는 원격 보안 토큰 또는 Kerberos 티켓의 대상 그룹을 가져올 수 있습니다.

수정

소스 보안 주체가 대상 그룹의 불법 멤버인 경우, 제거해야 합니다.

"Active Directory 사용자 및 컴퓨터"와 같은 각종 표준 Active Directory 관리 도구 또는 Remove-ADGroupMember와 같은 PowerShell을 사용할 수 있습니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO

- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

소유

설명

소스 보안 주체가 대상 개체의 선언된 소유자입니다. 이것이 대상 개체를 생성했을 가능성이 크기 때문입니다. 소유자에게는 암시적 권한("읽기 제어" 및 "DACL 쓰기")이 있어 자신 또는 다른 누군가를 위해 더 많은 권한을 얻을 수 있고, 나아가 대상 개체를 침해할 수 있습니다.

악용

소스 보안 주체를 침해하는 공격자는 대상 개체의 보안 설명자를 편집하기만 하면 됩니다. "dsacls"와 같은 네이티브 Windows 명령, "Set-ACL"과 같은 PowerShell, "Active Directory 사용자 및 컴퓨터"와 같은 관리 도구 또는 PowerSploit와 같은 전용 해커 도구가 사용됩니다.

개체를 만들 때 낮은 수준의 권한 있는 사용자가 이를 만들어서 소유하는 경우, 권한 상승의 위험이 있습니다. 예를 들어 일반적인 기술 지원팀 기술자가 만든 개체가 더 높은 권한, 예를 들어 관리자로 상승합니다. 원래 소유자가 그대로 유지되며 새로 권한이 생긴 개체를 침해하여 그에 속한 권한을 유리하게 이용할 수 있습니다.

수정

소스 보안 주체가 대상 개체의 적법한 소유자가 아닌 경우, 반드시 변경해야 합니다.

대상 개체의 소유자를 변경하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 **속성** > **보안** > **고급**을 마우스 오른쪽으로 클릭합니다.
2. 맨 위의 **소유자** 줄에서 **변경**을 클릭합니다.

가장 중요한 Active Directory 개체에 기본적으로 사용되는 안전한 대상 개체 소유자는 다음과 같습니다.

- 도메인 파티션의 개체: "관리자" 또는 "도메인 관리자"
- 구성 파티션의 개체: "엔터프라이즈 관리자"
- 스키마 파티션의 개체: "스키마 관리자"

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

비밀번호 초기화

설명

소스 보안 주체가 대상의 비밀번호를 초기화할 수 있으며, 따라서 새로 특성이 부여된 비밀번호를 사용해 대상으로서 인증하여 대상의 권한을 유리하게 이용할 수 있습니다.

비밀번호를 초기화한다는 것은 현재 비밀번호를 아는 사용자가 수행할 수 있는 비밀번호 변경과는 다릅니다. 비밀번호 변경은 보통 비밀번호가 만료되면 발생합니다.

악용

소스 보안 주체를 침해하는 공격자는 "net user /domain"과 같은 네이티브 Windows 명령, "Set-ADAccountPassword -Reset"과 같은 PowerShell, "Active Directory 사용자 및 컴퓨터"와 같은 관리 도구 또는 PowerSploit와 같은 전용 해커 도구를 사용해 대상의 비밀번호를 초기화할 수 있습니다.

그런 다음 공격자는 새로 선택한 비밀번호를 가지고 적법한 인증 방식을 사용해 온전히 대상으로 가장하고 Active Directory 또는 표적 리소스에 인증하기만 하면 됩니다.

그러나 공격자는 대개 이전 비밀번호를 모르기 때문에 공격한 뒤에 비밀번호를 원래대로 되돌릴 수 없습니다. 따라서 이 공격은 대상 뒤의 적법한 사용자의 눈에 띌 때가 많고 특히 서비스 계정의 경우, 심하면 서비스 거부를 초래할 수도 있습니다.

수정

IT 관리자와 기술 지원팀 직원은 적법하게 비밀번호를 초기화할 수 있습니다. 하지만 이 작업을 각자 허용된 경계 내에서만 수행하게 하기 위해 적절한 위임을 마련해야 합니다.

또한, 계층화 모델에 따라 일반 사용자 대상의 기술 지원팀와 같이 낮은 수준의 직원이 높은 수준의 계정(예: 도메인 관리자) 비밀번호를 초기화하지 못하도록 해야 합니다. 이것은 권한 상승 기회이기 때문입니다.

대상의 보안 설명자를 수정하고 불법 권한을 제거하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 속성 > 보안을 마우스 오른쪽으로 클릭합니다.
2. 소스 보안 주체의 "비밀번호 초기화" 권한을 제거합니다.

> **참고**: 이 권한을 "비밀번호 변경"과 혼동하지 마십시오.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- RODC 관리
- DACL 쓰기
- 쓰기 소유자

RODC 관리

설명

소스 보안 주체가 대상 읽기 전용 도메인 컨트롤러(RODC)의 "ManagedBy" 특성에 있습니다. 소스에 대상 RODC에 대한 관리 권한이 있음을 의미합니다.

> **참고**: 다른 Active Directory 개체 유형은 "ManagedBy" 특성을 정보 제공용으로만 사용하고 선언된 관리자에게 아무런 관리 권한도 부여하지 않습니다. 따라서 이 관계는 RODC 유형의 대상 노드에 대해서만 존재합니다.

RODC는 좀 더 보편적인 쓰기 가능한 도메인 컨트롤러보다 덜 중요하지만 여전히 공격자에게는 가치가 높은 표적입니다. RODC에서 자격 증명을 훔쳐 다른 시스템으로 다시 이동할 수 있기 때문입니다. 이것은 RODC 구성 내 강화 수준에 따라 다릅니다. 예를 들어, 동기화할 수 있는 암호를 포함한 개체 수가 대표적입니다.

악용

악용 방법은 "AdminTo" 관계의 악용 방법과 동일합니다.

소스 보안 주체를 침해한 공격자는 그 주체의 ID를 사용해 관리자 권한으로 대상 RODC에 원격으로 접속하여 명령을 실행할 수 있습니다. 이들은 이용 가능한 네이티브 프로토콜, 예를 들어 관리자 공유를 포함한 서버 메시지 블록(Server Message Block, SMB), 원격 데스크톱 프로토콜(Remote Desktop Protocol, RDP), Windows Management Instrumentation(WMI), 원격 절차 호출(Remote Procedure Call, RPC), Windows Remote Management (WinRM) 등을 악용할 수 있습니다.

공격자는 PsExec, 서비스, 예약된 작업, Invoke-Command 등의 네이티브 원격 관리 도구를 사용할 수도 있고 wmiexec, smbexec, Invoke-DCOM, SharpRDP 등과 같은 전문 해커 도구를 사용할 수도 있습니다.

공격의 최종 목표는 대상 RODC를 손상시키거나 mimikatz와 같은 자격 증명 덤핑 도구를 사용하여 더 많은 자격 증명과 비밀을 획득하여 다른 시스템으로 전환하는 것입니다.

수정

소스 보안 주체가 대상 읽기 전용 도메인 컨트롤러(RODC)의 적법한 관리자가 아닌 경우, 적절한 관리자로 바꿔야 합니다.

도메인 관리자는 보통 RODC를 관리하지 않으므로, 전용 "관리자" 설정을 이용해야 합니다. RODC는 트러스트 수준이 낮으며 권한 수준이 높은 도메인 관리자가 여기에서 인증하여 자신의 자격 증명을 노출해서는 안 되기 때문입니다.

따라서 Active Directory RODC 규칙에 따라 RODC의 적절한 "중간 수준" 관리자(예: 조직에 속한 지점의 IT 관리자)를 선택해야 합니다.

"ManagedBy" 특성을 변경하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 RODC > **속성** > "**ManagedBy**" 탭을 선택합니다.
2. **변경**을 클릭합니다.

PowerShell에서 다음과 같은 명령을 실행할 수도 있습니다.

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유

- 비밀번호 초기화
- DACL 쓰기
- 쓰기 소유자

DACL 쓰기

설명

소스 보안 주체에는 임의 액세스 제어 목록(DACL)의 대상 개체 권한을 변경할 권한이 있습니다. 이 때문에 소스가 스스로 추가적인 권한을 획득하거나 다른 사람에게 권한을 부여하여 궁극적으로 대상 개체를 침해할 수 있습니다.

악용

소스 보안 주체를 침해하는 공격자는 대상 개체의 보안 설명자를 편집하기만 하면 됩니다. "dsacls"와 같은 네이티브 Windows 명령, "Set-ACL"과 같은 PowerShell, "Active Directory 사용자 및 컴퓨터"와 같은 관리 도구 또는 PowerSploit와 같은 전용 해커 도구가 사용됩니다.

수정

소스 보안 주체에 대상 개체의 권한을 변경할 적법한 권한이 없는 경우, 이 권한을 제거해야 합니다.

대상 개체의 보안 설명자를 수정하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 개체를 마우스 오른쪽으로 클릭한 다음 **속성** > **보안** > **고급**을 선택합니다.
2. 소스 보안 주체의 "권한 수정" 권한을 제거합니다.

> **참고**: 개체는 Active Directory 트리에서 더 높은 수준의 개체로부터 이 권한을 상속할 수 있습니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용
- 위임 허용
- GPO에 속함
- DCSync

- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- 쓰기 소유자

쓰기 소유자

설명

소스 보안 주체에는 대상 개체의 소유자를 변경할 권한이 있으며, 여기에는 자신을 소유자로 지정하는 권한도 포함합니다. 소유자에게는 암시적 권한("읽기 제어" 및 "DACL 쓰기")이 있어 자신 또는 다른 누군가를 위해 더 많은 권한을 얻을 수 있고, 나아가 대상 개체를 침해할 수 있습니다.

자세한 정보는 소유 관계를 참조하십시오.

악용

소스 보안 주체를 침해하는 공격자는 "dsacls /takeownership"과 같은 네이티브 Windows 명령, "Set-ACL"과 같은 PowerShell, "Active Directory 사용자 및 컴퓨터"와 같은 관리 도구 또는 PowerSploit와 같은 전용 해커 도구를 사용하여 자신을 대상의 소유자로 지정할 수 있습니다.

그런 다음 유사한 방법을 사용하여 대상 개체의 보안 설명자를 편집할 수 있습니다.

수정

소스 보안 주체에 대상 개체의 소유자를 변경할 적법한 권한이 없는 경우, 이 권한을 제거해야 합니다.

대상 개체의 보안 설명자를 수정하는 방법:

1. "Active Directory 사용자 및 컴퓨터"에서 개체를 마우스 오른쪽으로 클릭하고 **속성** > **보안** > **고급**을 선택합니다.
2. 소스 보안 주체의 "소유자 수정" 권한을 제거합니다.

> **참고**: 개체는 Active Directory 트리에서 더 높은 수준의 개체로부터 이 권한을 상속할 수 있습니다.

참고 항목

- 키 자격 증명 추가
- 멤버 추가
- 작업 허용

- 위임 허용
- GPO에 속함
- DCSync
- 작업 허용 권한 부여
- SID 기록 있음
- 암시적 인수
- GPO 상속
- 연결된 GPO
- 멤버 관계
- 소유
- 비밀번호 초기화
- RODC 관리
- DACL 쓰기

계층 0 자산 식별

계층 0 자산에는 Active Directory 포리스트 및 도메인에 대한 직간접적인 관리 제어 권한이 있는 계정, 그룹 및 기타 자산이 포함됩니다.

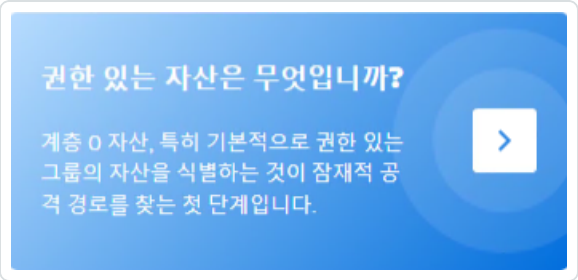
Tenable Identity Exposure에서는 계층 0 자산과 공격 경로가 해당 자산으로 이어질 가능성이 있는 계정을 나열합니다.

계층 0 자산을 나열하는 방법:

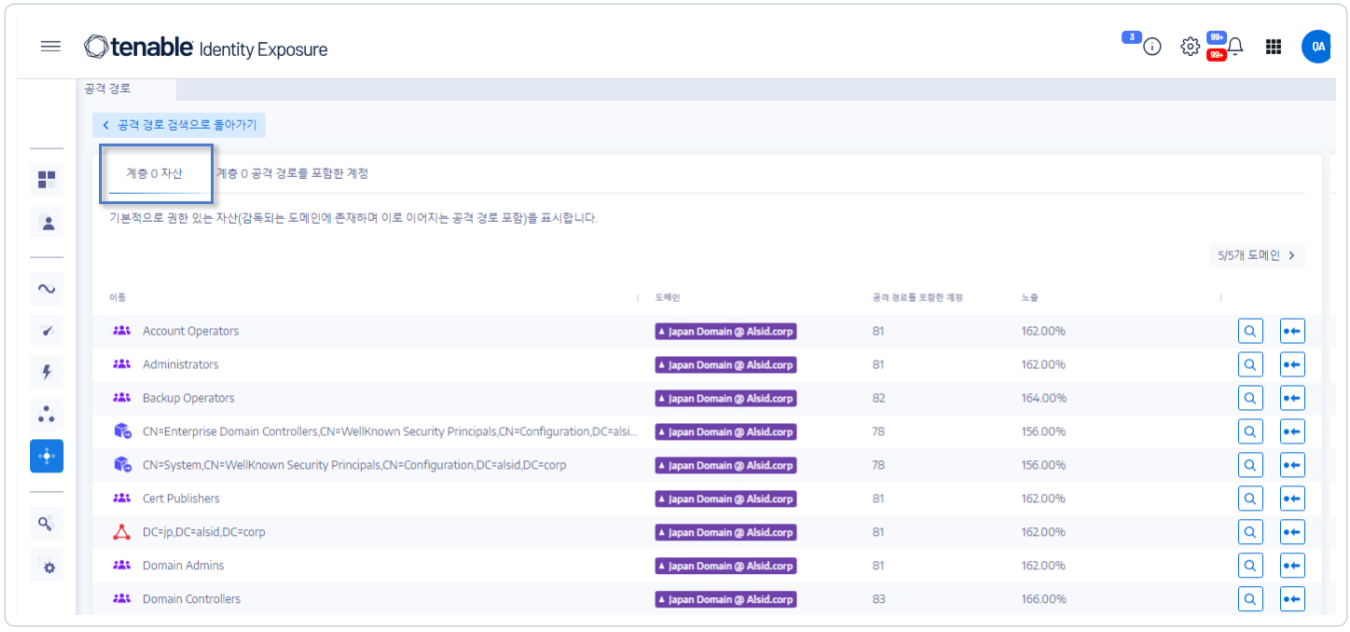
1. Tenable Identity Exposure에서 왼쪽 탐색 모음의 공격 경로 아이콘 을 클릭합니다.

   공격 경로 창이 열립니다.

2. "**권한 있는 자산은 무엇입니까?**" 타일을 클릭합니다.



   Tenable Identity Exposure에서 AD의 계층 0 자산 목록을 보여줍니다.



   각 줄에는 **자산 이름**, 해당 **도메인**과 다음 정보가 제공됩니다.

- **공격 경로가 있는 계정**: 공격 경로가 계층 0 자산으로 이어지는 자산의 수.
- **노출**: 공격 경로가 계층 0 자산으로 이어지는 자산의 도메인에 있는 총 계정 수의 백분율.

특정 도메인의 자산을 필터링하려면:

1. **n/n** 버튼을 클릭합니다.

   포리스트 및 도메인 창이 열립니다. 다음 중 하나를 수행할 수 있습니다.

   - **검색** 상자에 포리스트 또는 도메인 이름을 입력합니다.
   - **모두 펼치기** 상자를 선택하고 원하는 포리스트 또는 도메인을 선택합니다.

2. **선택 항목 필터링**을 클릭합니다.

   Tenable Identity Exposure에서 자산 목록을 업데이트합니다.

공격 경로가 계층 0 자산으로 이어지는 계정을 나열하는 방법:

- 계층 0 자산 이름의 줄 끝에서  아이콘을 클릭합니다.

  Tenable Identity Exposure에서 공격 경로가 해당 계층 0 자산으로 이어지는 계정 목록을 보여줍니다.

계층 0 자산의 자산 노출을 확인하는 방법:

- 계층 0 자산 이름이 있는 줄 끝에서  아이콘을 클릭합니다.

  Tenable Identity Exposure에서 해당 계층 0 자산에 대한 자산 노출 페이지를 엽니다. 자세한 내용은 공격 관계를 참조하십시오

공격 경로가 있는 계정

Tenable Identity Exposure는 다양한 공격 관계를 통해 사용자와 컴퓨터 계정에 권한이 부여될 수 있기 때문에 계층 0 자산으로 이어지는 공격 경로가 있는 계정을 표시하여 잠재적인 보안 위협을 포괄적으로 보여줍니다.

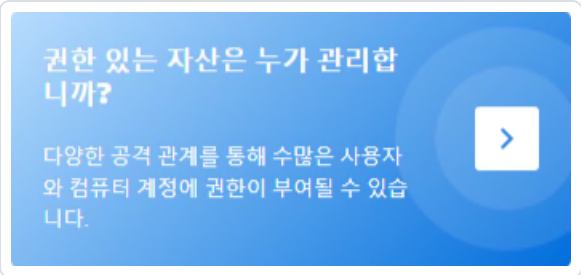
자세한 내용은 계층 0 자산 식별을 참조하십시오.

공격 경로가 있는 자산을 표시하는 방법:

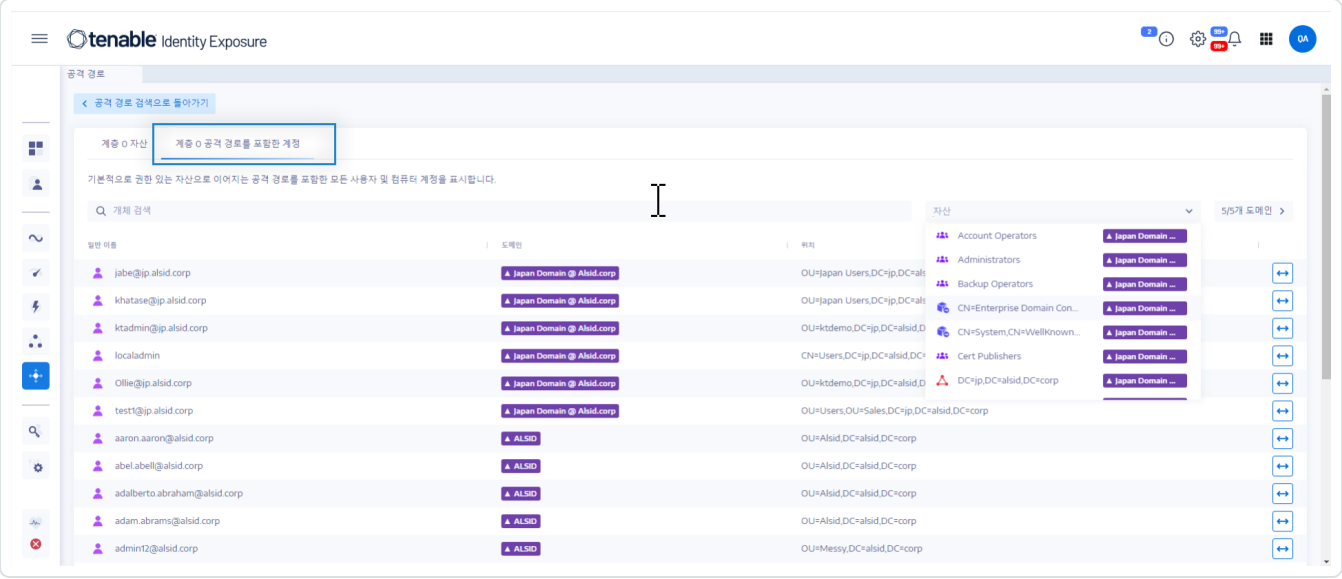
1. Tenable Identity Exposure에서 왼쪽 탐색 모음의 공격 경로 아이콘 을 클릭합니다.

   공격 경로 창이 열립니다.

2. "**권한 있는 자산은 누가 관리합니까?**" 타일을 클릭합니다.



   Tenable Identity Exposure는 공격 경로가 계층 0 자산으로 이어지는 모든 사용자 및 컴퓨터 계정을 보여줍니다.



특정 자산을 검색하는 방법:

1. **검색** 상자에 자산 이름을 입력합니다.
2. **자산** 상자에서 화살표 **>**를 클릭하여 계층 0 자산의 드롭다운 목록을 표시하고 하나를 선택합니다.

   Tenable Identity Exposure에서 일치하는 결과로 목록을 업데이트합니다.

특정 도메인의 자산을 필터링하려면:

1. **n/n** 버튼을 클릭합니다.

   포리스트 및 도메인 창이 열립니다. 다음 중 하나를 수행할 수 있습니다.

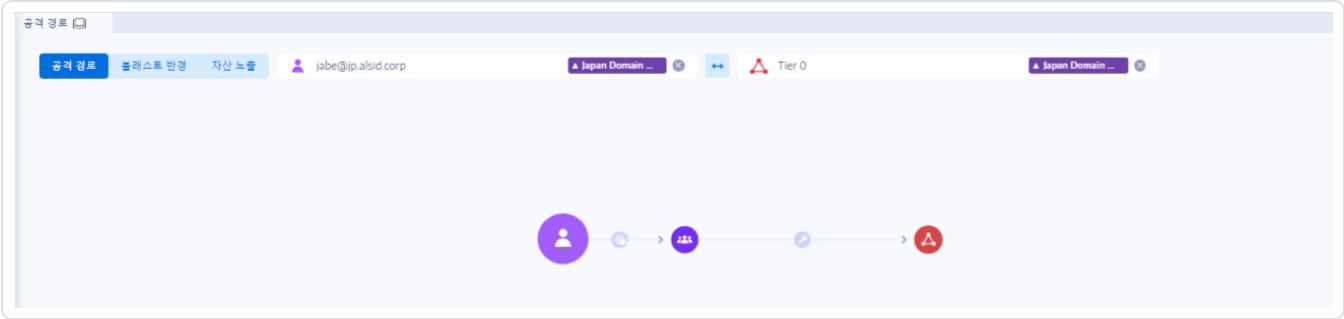
   - **검색** 상자에 포리스트 또는 도메인 이름을 입력합니다.
   - **모두 펼치기** 상자를 선택하고 원하는 포리스트 또는 도메인을 선택합니다.
2. **선택 항목 필터링**을 클릭합니다.

   Tenable Identity Exposure에서 자산 목록을 업데이트합니다.

공격 경로를 탐색하는 방법:

- 자산 이름 줄 끝에 있는  아이콘을 클릭합니다.

  Tenable Identity Exposure는 해당 자산에서 모든 계층 0 자산으로 공격 경로 페이지를 시작합니다. 자세한 내용은 공격 경로 및 공격 관계를 참조하십시오.



공격 경로 노드 유형

Tenable Identity Exposure의 공격 경로 기능에는 Active Directory 환경 내에서 공격자에게 열려 있는 공격 경로를 나타낸 그래프가 표시됩니다. 이 그래프는 공격 관계를 나타내는 **경계**와 Active Directory(LDAP/SYSVOL) 개체를 나타내는 **노드**로 구성됩니다.

다음 목록에서는 공격 경로 그래프에 표시될 것으로 예상할 수 있는 가능한 모든 노드 유형을 설명합니다.

노드 유형	위치	아이콘	설명
사용자	LDAP		`objectClass` 특성에 `user` 클래스는 포함하지만 `computer`는 없는 LDAP 개체입니다.
그룹	LDAP		`objectClass` 특성에 `class` 그룹을 포함하는 LDAP 개체입니다.
장치	LDAP		`objectClass` 특성에 `computer` 클래스는 포함하지만 `msDS-GroupManagedServiceAccount`는 없는 LDAP 개체입니다. 이것의 `primaryGroupID` 특성은 516(DC) 또는 521(RODC)과 같지 않습니다. **참고**: Tenable 제품을 구분하기 위해, 이 카테고리를 "컴퓨터" 대신 더 포괄적인 "장치"로 칭합니다.
조직 단위(OU)	LDAP		`objectClass` 특성에 `organizationalUnit` 클래스를 포함하는 LDAP 개체입니다. `container` 클래스의 개체를 컨테이너 역할을 할 수 있는 모든 Active Directory(AD) 개체와 혼동하여 여기에 다른 개체를 포함하도록 허용하면 안 됩니다.
도메인	LDAP		`objectClass` 특성에 `domainDNS` 클래스 및 특정 특성을 포함하는 LDAP 개체입니다.
도메인 컨트롤러(DC)	LDAP		`objectClass` 특성에 `computer` 클래스를 포함하며 `primaryGroupID` 특성이 516과 같은(따라서 RODC가 아닌) LDAP 개체입니다.

읽기 전용 도메인 컨트롤러 (RODC)	LDAP		objectClass 특성에 computer 클래스를 포함하고 primaryGroupID 특성이 521과 같은(따라서 일반 DC가 아닌) LDAP 개체입니다.
그룹 정책 (GPC)	LDAP		objectClass 특성에 groupPolicyContainer 클래스를 포함하는 LDAP 개체입니다.
GPO 파일	SYSVOL		특정 GPO의 SYSVOL 공유에서 찾은 파일(예: "\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml")
GPO 폴더	SYSVOL		특정 GPO의 SYSVOL 공유에서 찾은 폴더입니다. GPO마다 하나씩 있음(예: "\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup")
그룹 관리 서비스 계정(gMSA)	LDAP		objectClass 특성에 msDS-GroupManagedServiceAccount 클래스를 포함하는 LDAP 개체입니다.
Enterprise NtAuth 스토어	LDAP		objectClass 특성에 certificationAuthority 클래스를 포함하는 LDAP 개체입니다.
PKI 인증서 템플릿	LDAP		objectClass 특성에 pKICertificateTemplate 클래스를 포함하는 LDAP 개체입니다.
확인되지 않은 보안 주체	LDAP		관계를 빌드할 때 어느 시점에 objectSid 또는 DistinguishedName 특성이 사용된 LDAP 개체입니다. 단, 이에 대해 알려지지 않은 해당 LDAP 보안 주체 개체가 있습니다(전형적인 "확인되지 않은 SID" 사례). 또한 이와 연관된 특정 보안 주체 유형(사용자, 컴퓨터, 그룹 등)에 관한 정보가 없고, SID/DN만 알려져 있습니다.

특수 ID	LDAP		Windows와 Active Directory는 내부에서 잘 알려진 ID를 사용합니다. 이러한 ID는 그룹과 비슷하게 작동하지만, AD가 이를 그룹으로 선언하지는 않습니다. 자세한 내용은 특수 ID 그룹을 참조하십시오.
기타			현재 앞서 언급한 카테고리에 속하지 않는 모든 AD/SYSVOL 개체입니다.

활동 로그

Tenable Identity Exposure의 활동 로그를 이용하면 특정 IP 주소, 사용자 또는 작업과 관련하여 Tenable Identity Exposure 플랫폼에서 발생한 모든 활동의 흔적을 볼 수 있습니다.

참고: 기술적 한계로 인해, 테넌트 관리(추가, 편집, 제거 포함)와 같은 특정 보기와 관련한 활동 로그는 현재 표시되지 않습니다.

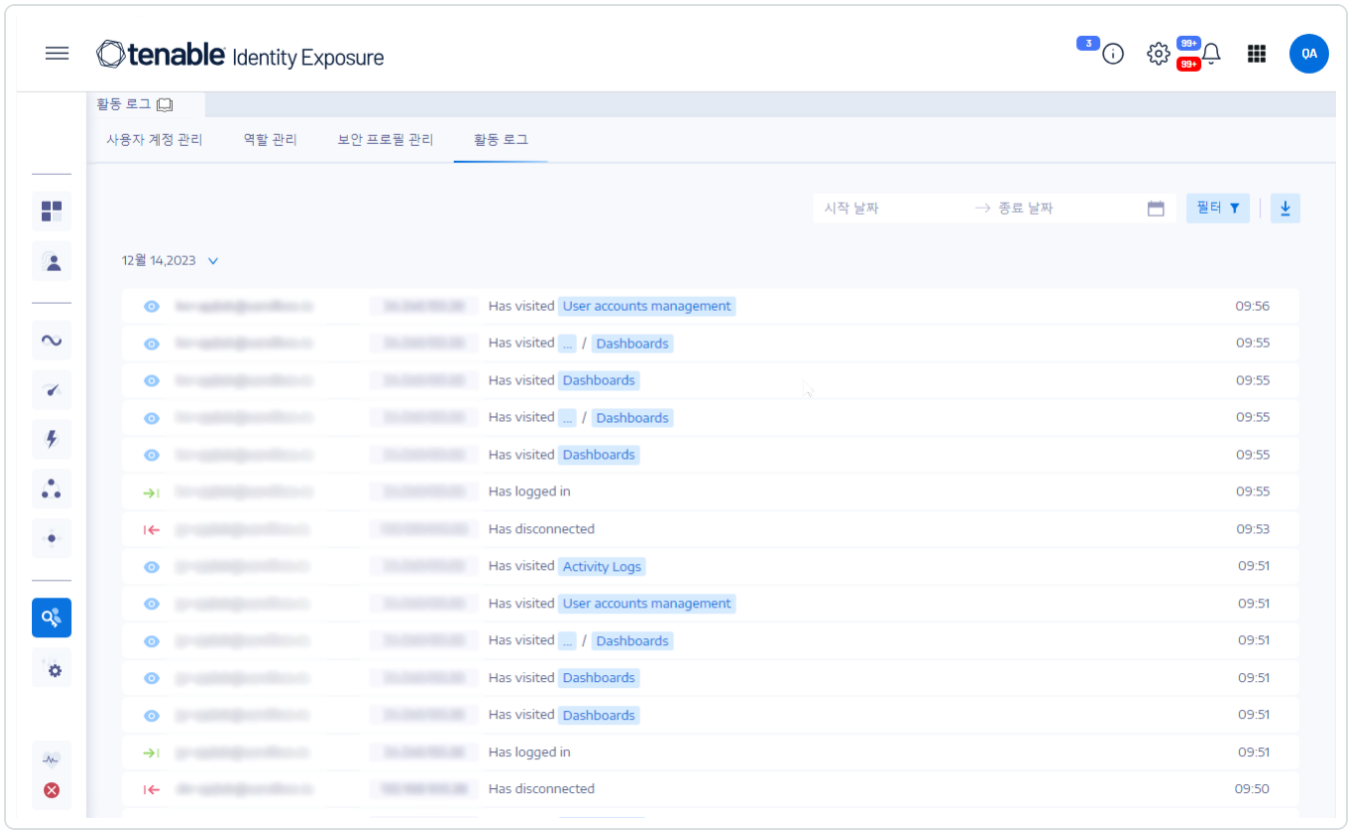
활동 로그를 보는 방법:

1. Tenable Identity Exposure에서 왼쪽 탐색 메뉴에 있는 **계정**  아이콘을 클릭합니다.

   사용자 계정 관리 창이 표시됩니다.

2. **활동 로그** 탭을 선택합니다.

   활동 로그 창이 시작됩니다.



특정 기간에 대한 활동 로그를 표시하는 방법:

1. 활동 로그 창 상단에서 날짜 선택기를 클릭합니다.
2. 원하는 기간의 시작 날짜와 종료 날짜를 선택합니다.
3. (선택 사항) 스크롤 막대를 사용하여 시간을 선택합니다(기본값: 현재 시간).
4. **확인**을 클릭합니다.

   Tenable Identity Exposure에서 해당 기간의 활동 로그를 표시합니다.

활동 로그를 필터링하는 방법:

1. 활동 로그 창 상단에서 Filters 버튼을 클릭합니다.

   필터 창이 표시됩니다.
2. 다음 상자에서 >를 클릭합니다.
   - IP 주소
   - 사용자
   - 작업
3. **유효성 검사**를 클릭합니다.

   Tenable Identity Exposure에서 사용자가 정의한 필터에 해당하는 활동 로그를 표시합니다.

필터를 지우는 방법:

- **필터** 창 아래에서 **필터 지우기**를 클릭합니다.

  Tenable Identity Exposure에서 필터링되지 않은 활동 로그를 표시합니다.

활동 로그를 내보내는 방법:

- 활동 로그 창 상단에서 아이콘을 클릭합니다.

  Tenable Identity Exposure에서 활동 로그를 CSV 형식으로 컴퓨터에 다운로드합니다.

Tenable Identity Exposure 관리자 가이드

마지막 업데이트: 2024년 4월 30

관리자 가이드는 Tenable Identity Exposure(이전의 Tenable.ad)의 관리 작업에 관한 정보를 제공합니다.

Tenable에서는 Tenable Identity Exposure에서 관리자로 시작할 때 다음 중 몇 가지를 권장합니다.

- 준비 및 설치
- 프로필 및 사용자 구성
- 탐지 및 모니터링

팁: Tenable Identity Exposure에 관한 자세한 정보는 다음 고객 교육 자료를 참조하십시오.

- Tenable Identity Exposure 자체 도움말 가이드
- Tenable Identity Exposure 개요(Tenable University)

준비 및 설치

Tenable Identity Exposure 설치를 준비하고 완료하는 방법은 다음과 같습니다.

- *Tenable Identity Exposure 설치 가이드*에 설명된 대로 Tenable Identity Exposure을(를) 설치합니다.
- Tenable Identity Exposure에 연결하고 로그인합니다.

프로필 및 사용자 구성

그런 다음 Tenable Identity Exposure 인터페이스를 구성하고 탐색하기 위해 다음과 상호 작용하는 것이 좋습니다.

- 프로필 기본 설정: 기본 언어를 구성하고 암호를 변경하고 프로필에 대한 기타 기본 설정을 지정합니다.
- Tenable Identity Exposure 인스턴스에 사용자를 만들고 추가합니다.
- 역할 기반 액세스 제어(RBAC)를 구성하여 조직 내 데이터 및 기능에 대한 액세스 보안을 유지합니다.

탐지 및 모니터링

비즈니스 요구 사항에 맞게 Tenable Identity Exposure를 구성하고 미세 조정했으면 데이터 작업을 시작할 수 있습니다.

- 공격 지표 모듈을 배포합니다.
- Tenable Identity Exposure 포털을 사용하여 모니터링하는 인프라의 보안 상태에 대한 관련 정보를 관리하고 수신합니다.
- 특정 도메인에서 모니터하려는 Tenable Identity Exposure에 대한 공격 유형을 선택하여 공격 시나리오를 정의합니다.

참고: Tenable Identity Exposure을(를) 단독으로 구입하거나 Tenable One 패키지의 일부분으로 구입할 수 있습니다. 자세한 내용은 Tenable One을 참조하십시오.

Tenable One 위험 노출 관리 플랫폼

Tenable One은 조직이 최신 공격 표면에 대한 가시성을 확보하고 가능한 공격을 방지하기 위한 노력을 집중하며 최적의 비즈니스 성과를 지원하기 위해 사이버 위험을 정확하게 커뮤니케이션할 수 있도록 지원하는 위험 노출 관리 플랫폼입니다.

이 플랫폼은 IT 자산, 클라우드 리소스, 컨테이너, 웹 앱 및 ID 시스템을 아우르는 가장 폭넓은 취약성 범위를 결합하고 Tenable Research에서 제공하는 취약성 범위의 속도와 폭을 기반으로 종합적인 분석을 더해 작업의 우선 순위를 지정하고 사이버 위험을 커뮤니케이션합니다. Tenable One은 조직에 다음과 같은 이점을 제공합니다.

- 최신 공격 표면 전체에 걸친 종합적 가시성 확보
- 위협을 예측하고 공격을 방지하기 위한 노력의 우선 순위를 지정
- 더 나은 결정을 내리기 위해 사이버 위험을 커뮤니케이션

Tenable Identity Exposure을(를) 독립 실행형 제품으로 사용하거나 Tenable One 위험 노출 관리 플랫폼의 일부분으로 구입할 수 있습니다.

> **팁:** Tenable One 제품을 시작하는 방법에 관한 자세한 정보는 Tenable One 배포 가이드를 참조하십시오.

자세한 내용은 다음을 참조하십시오.

Active Directory 구성

Tenable Identity Exposure에는 모니터링되는 Active Directory에 몇 가지 구성을 적용해야 특정 기능이 제대로 작동합니다.

- AD 개체 또는 컨테이너에 대한 액세스
- 권한 있는 분석에 대한 액세스
- 공격 지표 배포

AD 개체 또는 컨테이너에 대한 액세스

참고: 이 섹션은 위험 노출 지표 모듈의 Tenable Identity Exposure 라이선스에만 해당합니다.

Tenable Identity Exposure에서 보안 모니터링을 수행하려면 관리 권한이 필요하지 않습니다.

이 방식은 Tenable Identity Exposure에서 한 도메인(사용자 계정, 조직 단위, 그룹 등 포함)에 저장된 모든 Active Directory 개체를 읽는 데 사용하는 사용자 계정의 기능에 의존합니다.

기본적으로, 대부분의 개체에는 Tenable Identity Exposure 서비스 계정에서 사용하는 그룹 도메인 사용자에 대한 읽기 액세스 권한이 있습니다. 단, Tenable Identity Exposure 사용자 계정에 읽기 액세스를 허용하려면 몇몇 컨테이너를 수동으로 구성해야 합니다.

다음 표에서는 Tenable Identity Exposure에서 모니터링하는 각 도메인에서 읽기 액세스를 얻기 위해 수동 구성이 필요한 Active Directory 개체와 컨테이너를 자세히 설명합니다.

컨테이너의 위치	설명
`CN=Deleted Objects,DC=<DOMAIN>,DC=<TLD>`	삭제된 개체를 호스팅하는 컨테이너입니다.
`CN=Password Settings Container,CN=System, DC=<DOMAIN>,DC=<TLD>`	(선택 사항) 비밀번호 설정 개체를 호스팅하는 컨테이너입니다.

AD 개체와 컨테이너에 대한 액세스 권한을 부여하는 방법:

- 도메인 컨트롤러의 명령줄 인터페이스에서 다음과 같은 명령을 실행하여 Active Directory 개체 또는 컨테이너에 대한 액세스 권한을 부여합니다.

  참고: 이 명령을 Tenable Identity Exposure에서 모니터링하는 각 도메인 모두에서 실행해야 합니다.

  ```
  dsacls "<__CONTAINER__>" /takeownership
  dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
  ```

  여기에서:

- <__CONTAINER__>는 액세스가 필요한 컨테이너를 가리킵니다.
- <__SERVICE_ACCOUNT__>는 Tenable Identity Exposure에서 사용하는 서비스 계정입니다.

권한 있는 분석에 대한 액세스

선택 사항인 권한 있는 분석 기능에는 관리자 권한이 필요합니다. Tenable Identity Exposure에서 사용하는 서비스 계정에 대하여 권한을 할당해야 합니다.

자세한 내용은 권한 있는 분석을 참조하십시오.

참고: 권한 있는 분석을 사용하는 각 도메인에 권한을 할당해야 합니다.

명령줄을 사용하여 권한을 할당하는 방법:

요구 사항: 권한을 할당하려면 도메인 관리자 권한이나 그와 동급의 권한이 있는 계정이 필요합니다.

- 도메인 컨트롤러의 명령줄 인터페이스에서 다음과 같은 명령을 실행하여 두 가지 권한을 모두 추가합니다.

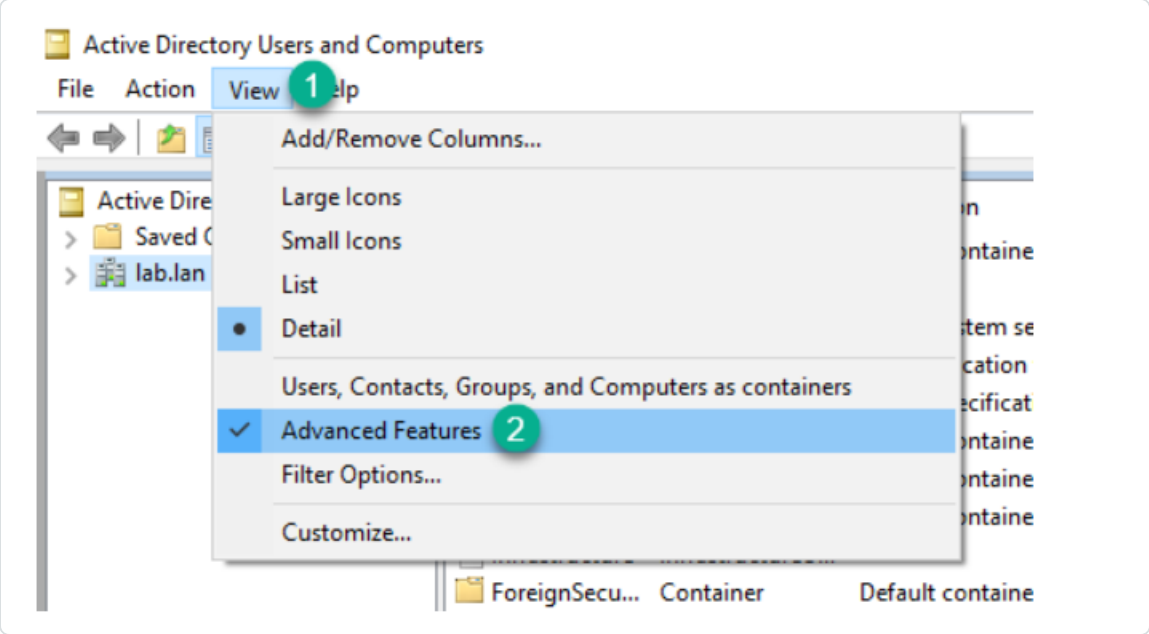
```
dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

  여기에서:

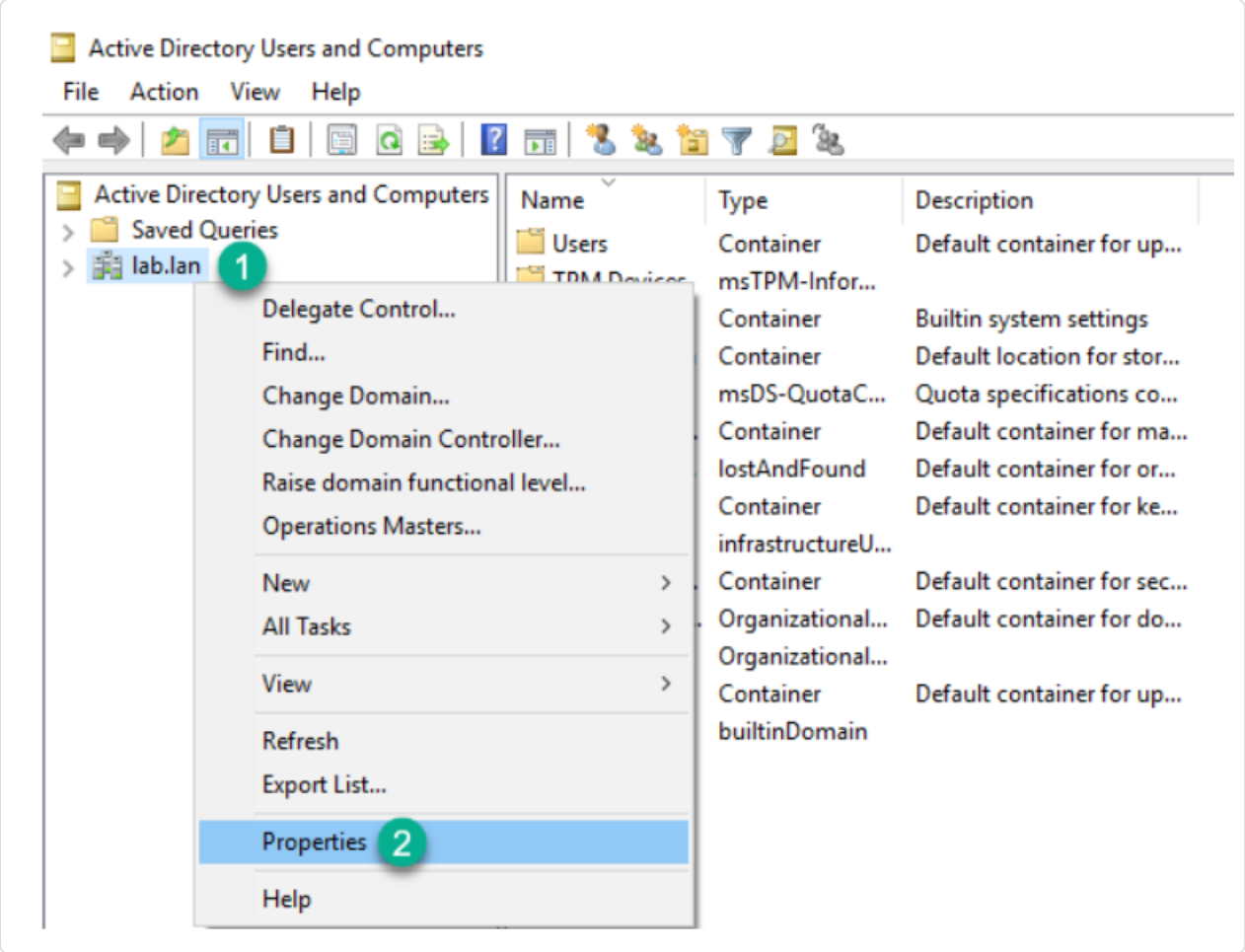
  - `<__DOMAIN_ROOT__>`는 도메인 루트의 고유 이름을 나타냅니다. 예: “DC=<DOMAIN>,DC=<TLD>”
  - `<__SERVICE_ACCOUNT__>`는 Tenable Identity Exposure에서 사용하는 서비스 계정입니다. 예: “DOMAIN\tenablead”.

그래픽 사용자 인터페이스를 사용하여 권한을 할당하는 방법:

1. Windows의 **시작** 메뉴에서 **Active Directory 사용자 및 컴퓨터**를 엽니다.
2. **보기** 메뉴에서 **고급 기능**을 선택합니다.

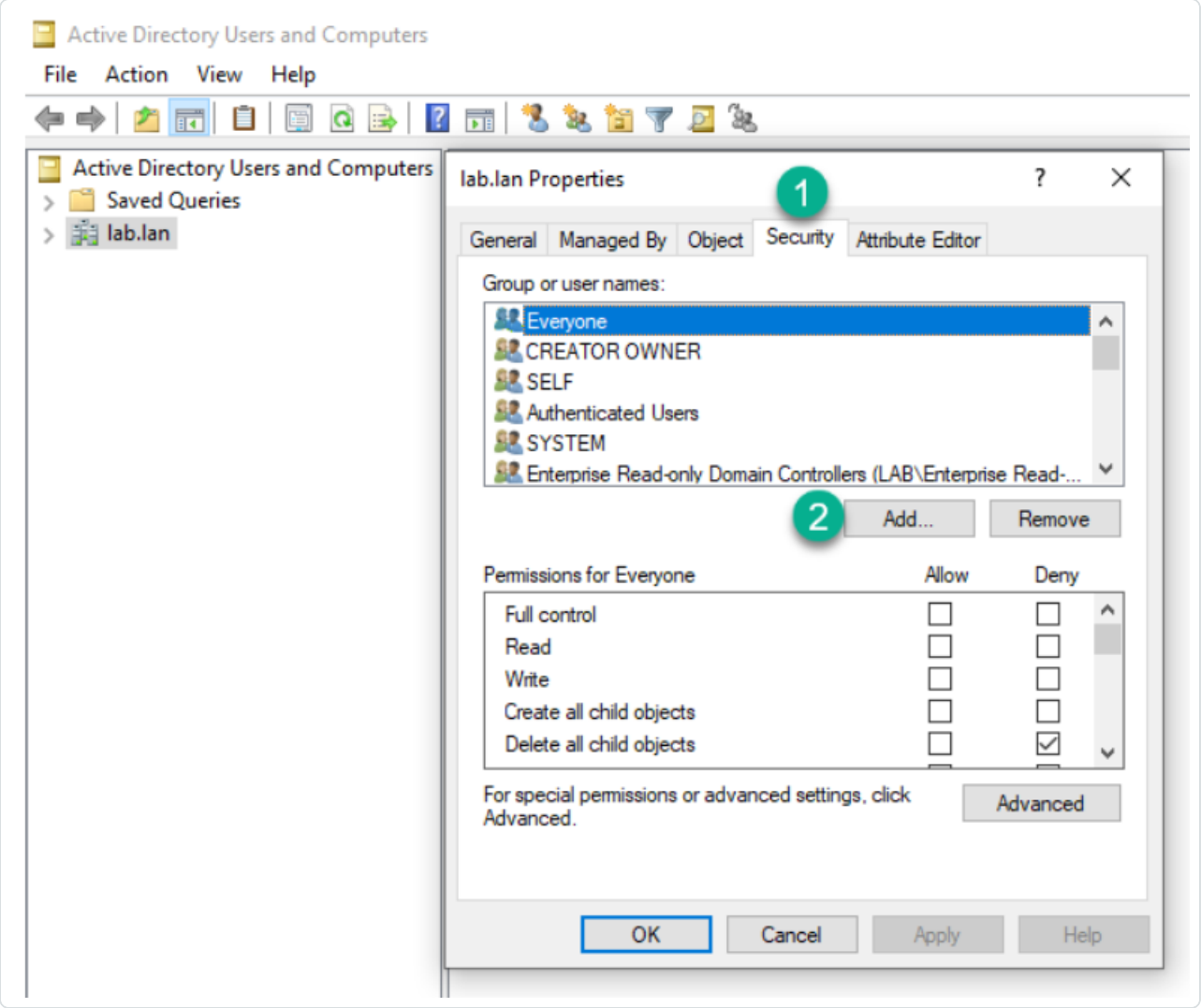


3. 도메인 루트를 마우스 오른쪽으로 클릭하여 **속성**을 선택합니다.



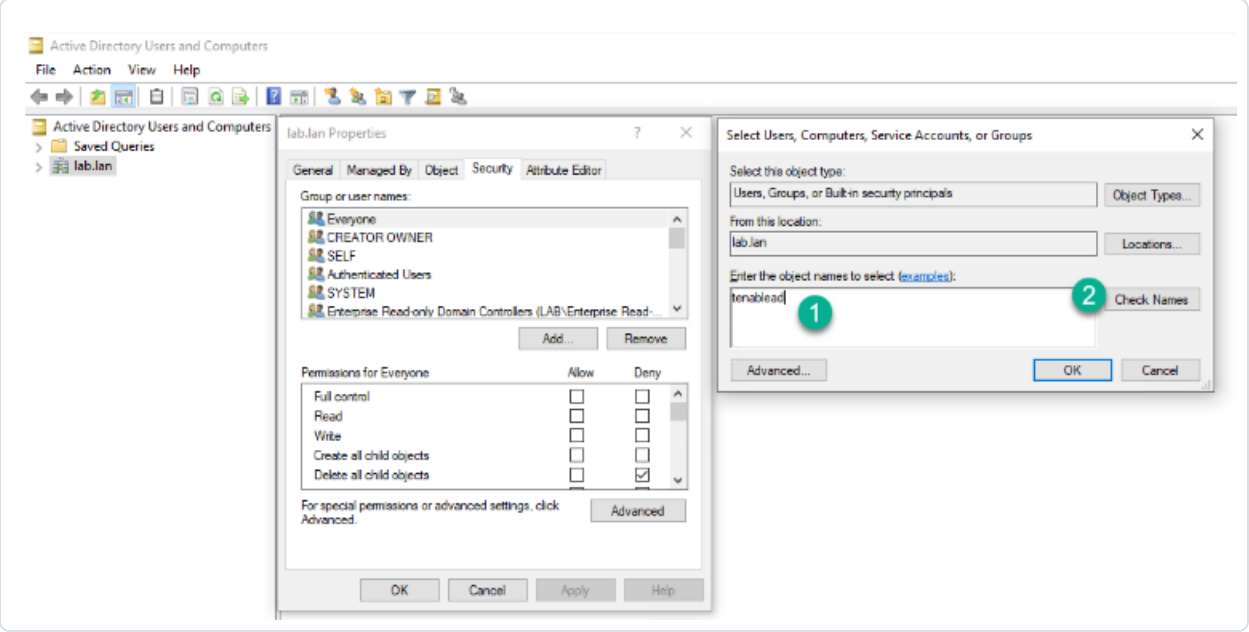
도메인 루트의 속성 창이 열립니다.

4. **보안** 탭을 클릭하고 **추가**를 클릭합니다.



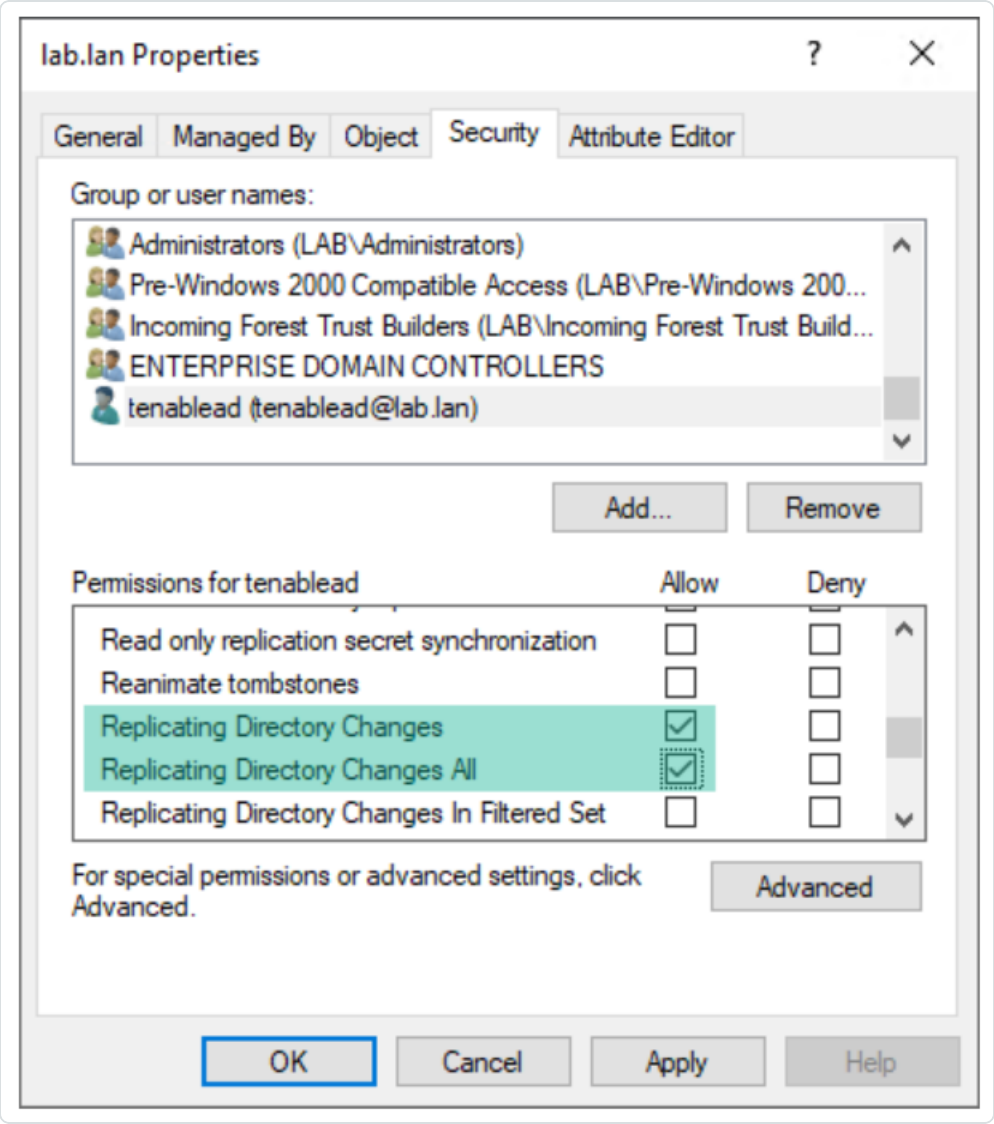
5. Tenable Identity Exposure 서비스 계정을 찾습니다.

참고: 여러 도메인이 있는 포리스트 환경에서는 서비스 계정이 다른 Active Directory 도메인에 있을 수 있습니다.



6. 목록 아래로 스크롤하여 기본적으로 설정된 모든 권한을 선택 취소합니다.

7. **허용** 열에서 *디렉터리 변경 사항 복제* 및 *디렉터리 변경 사항 모두 복제*의 권한을 둘 다 선택합니다.



8. **확인**을 클릭합니다.

중요 참고 사항

Tenable Identity Exposure에는 포리스트당 서비스 계정 하나만 있으면 됩니다. 따라서 도메인에 권한을 할당할 때 **다른 도메인의 서비스 계정을 검색**해야 할 수도 있습니다.

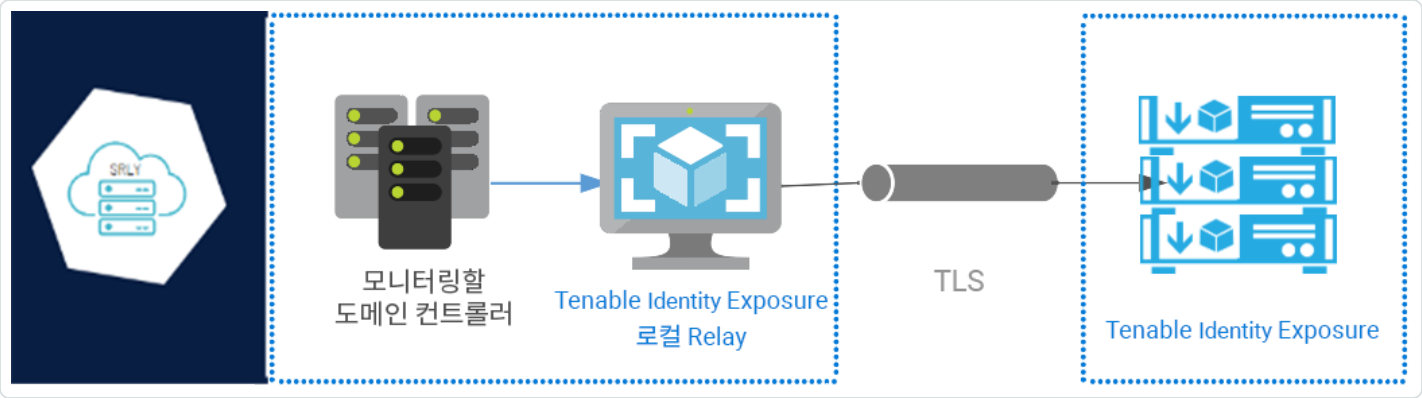
추가 권한은 **도메인 루트 수준**에서 할당해야 합니다. Active Directory는 조직 단위나 특정 사용자에게 할당된 권한을 지원하지 않으므로(예: 권한 있는 분석을 OU나 사용자로 제한) 이렇게 해도 아무런 영향이 없습니다.

이러한 권한은 Active Directory 도메인에 대해 Tenable Identity Exposure 서비스 계정에 훨씬 더 많은 권한을 부여합니다. 그런 다음 이를 **권한 있는 계정(계층 0)**으로 간주하고 도메인 관리자 계정과 비슷하게 보호해야 합니다. 전체 절차는 서비스 계정 보호를 참조하십시오.

Secure Relay

Secure Relay는 네트워크에서 Tenable Identity Exposure로 Active Directory 데이터를 보내는 전송 모드이며 이 다이어그램에서 볼 수 있는 것처럼 VPN 대신 TLS(전송 계층 보안)를 사용합니다. Relay 기능은 네트워크에서 인터넷에 연결하기 위해 프록시 서버가 필요한 경우 HTTP 프록시도 지원합니다(인증 포함 또는 미포함).

Tenable Identity Exposure에서는 여러 Secure Relay를 지원하므로 필요에 따라 도메인에 매핑할 수 있습니다.

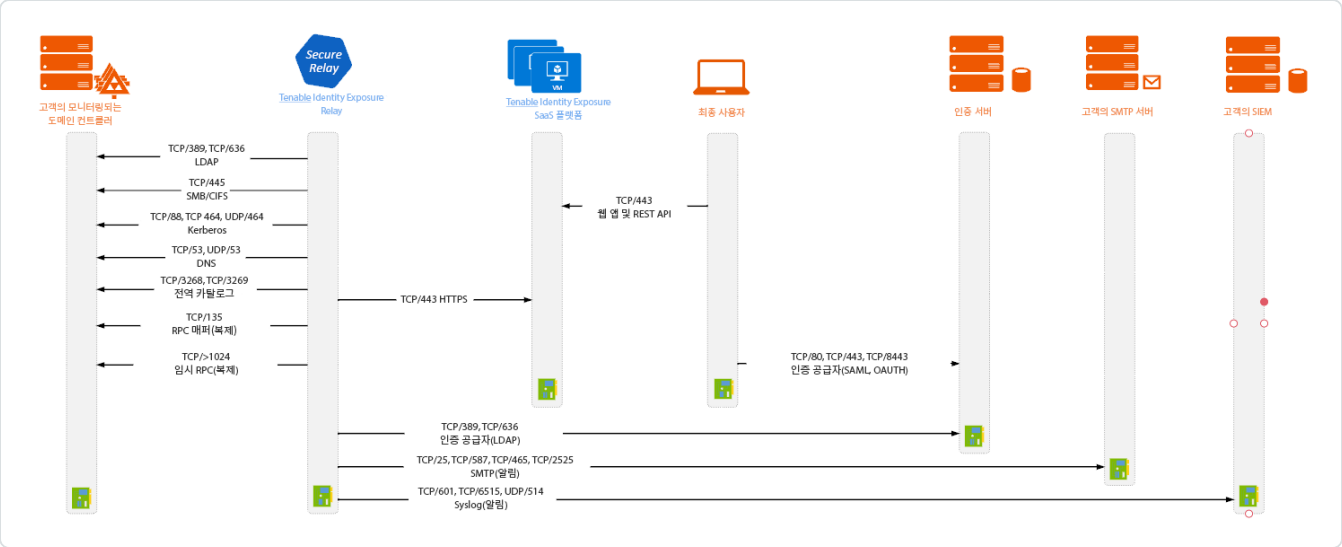


참고: 현재 Secure Relay 기능은 Tenable Identity Exposure에서 플랫폼이 Secure Relay를 사용하도록 프로비저닝하는 경우에만 이용할 수 있습니다. 프로비저닝을 VPN에서 Secure Relay로 수동으로 전환할 수는 없습니다. 플랫폼을 VPN에서 Secure Relay로 마이그레이션하는 데 도움이 필요한 경우, Tenable Identity Exposure 고객 지원 담당자에게 문의하십시오.

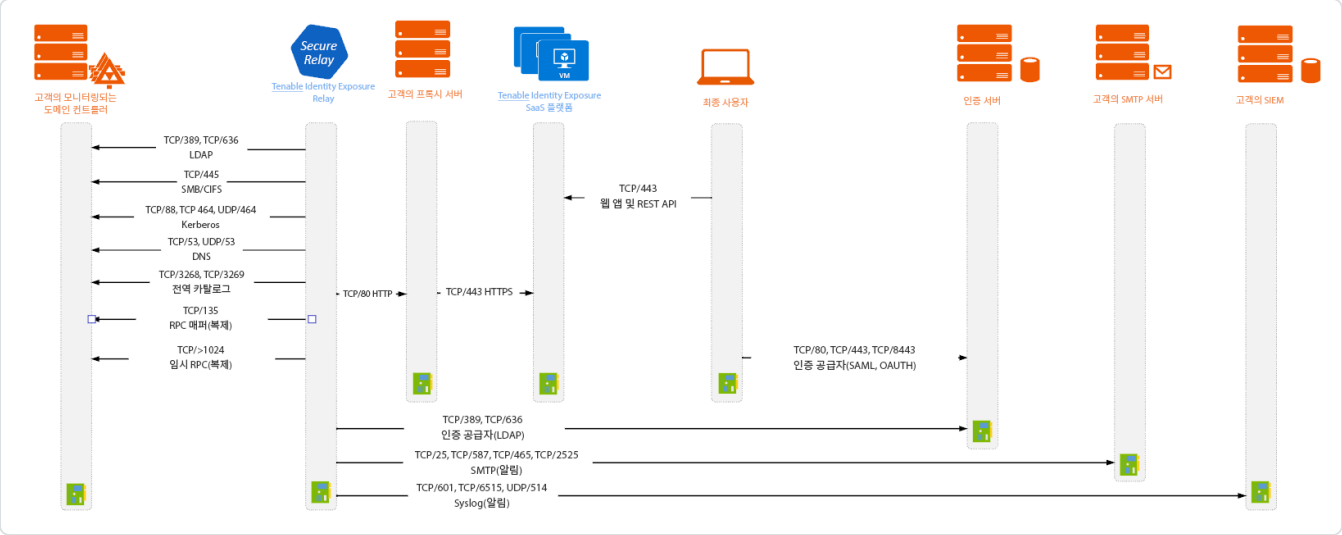
네트워크 흐름

Secure Relay에 필요한 포트

- **프록시 서버가 없는** 일반적 설정의 경우 Relay에 다음 포트가 필요합니다.



- **프록시 서버를 사용하는** 설정의 경우 Relay에 다음 포트가 필요합니다.



TLS 요구 사항

TLS 1.2를 사용하려면 Relay 서버가 2024년 1월 24일 기준으로 다음과 같은 암호 제품군 중 하나 이상을 지원해야 합니다.

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

또한, Windows 구성이 지정된 암호 제품군과 일치하여 Relay 기능과 호환되어야 합니다.

암호 제품군을 검사하는 방법:

1. PowerShell에서 다음의 명령을 실행합니다.

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_
RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. 출력이 다음과 같은지 확인합니다. `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`.

```
PS C:\Users> @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
, "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }


KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 128
BaseCipherSuite       : 49199
CipherSuite           : 49199
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols             : {771, 65277}

KeyType               : 0
Certificate           : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange              : ECDH
HashLength            : 0
Hash                  :
CipherBlockLength     : 16
CipherLength          : 256
BaseCipherSuite       : 49200
CipherSuite           : 49200
Cipher                : AES
Name                  : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols             : {771, 65277}
```

3. 출력이 비어 있는 경우, Relay의 TLS 연결이 작동하기 위해 필요한 암호 제품군 중 사용 설정된 것이 없다는 의미입니다. 적어도 하나의 암호 제품군을 사용 설정하십시오.
4. Relay 서버에서 ECC(Elliptic Curve Cryptography) 곡선을 확인합니다. ECDHE(Elliptic Curve Diffie-Hellman Ephemeral) 암호 제품군을 사용하려면 이 확인이 필수입니다. PowerShell에서 다음의 명령을 실행합니다.

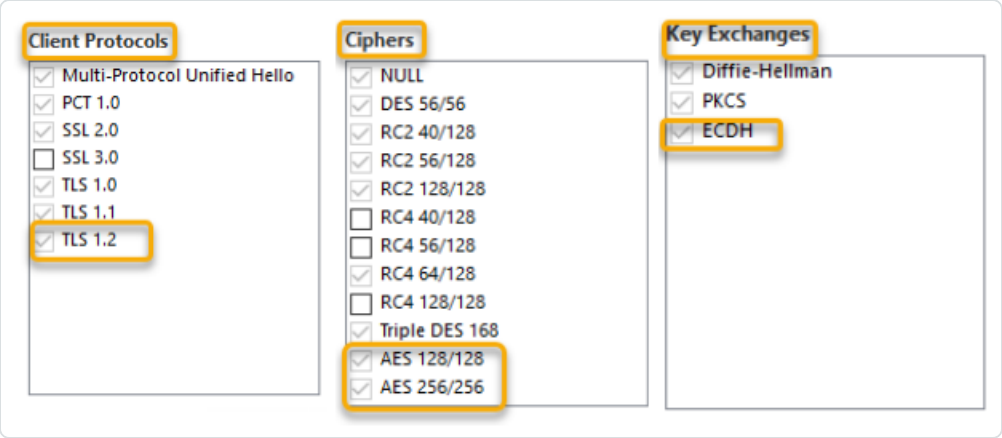
```
Get-TlsEccCurve
```

5. 곡선 **25519**가 있는지 점검합니다. 없는 경우, 사용 설정합니다.

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

Windows 암호 설정을 확인하는 방법:

1. IIS Crypto 도구에서 다음과 같은 옵션이 사용 설정되었는지 확인합니다.
    - 클라이언트 프로토콜: **TLS 1.2**
    - 암호: **AES 128/128** 및 **AES 256/256**
    - 키 교환: **ECDH**



2. 암호 설정을 수정하고 나면 컴퓨터를 다시 시작합니다.

> **참고**: Windows 암호 설정을 수정하면 컴퓨터에서 실행 중이고 Windows TLS 라이브러리, 일명 "Schannel"을 사용 중인 모든 애플리케이션에 영향이 발생합니다. 따라서 조정으로 인한 의도치 않은 부작용을 초래하지 않도록 해야 합니다. 선택한 구성이 조직의 전체 강화 목표 또는 규정 준수 요건과 일치하는지 확인하십시오.

시작하기 전에

필수 조건

가상 머신

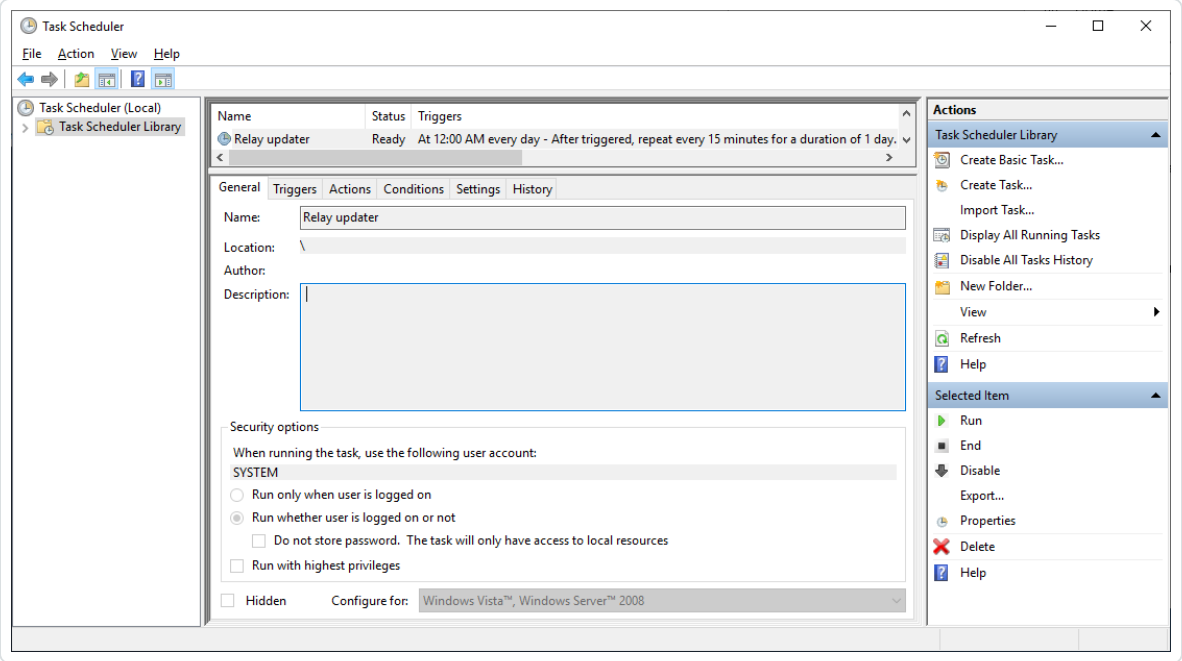
Secure Realy를 호스팅하는 가상 컴퓨터(VM)의 필수 조건은 다음과 같습니다.

고객 규모	Tenable Identity Exposure 서비스	필요한 인스턴스	메모리(인스턴스당)	vCPU(인스턴스당)	디스크 토폴로지	사용 가능한 디스크 공간(인스턴스당)
모든 규모	• `tenable_Relay` • `tenable_envoy`	1	8GB RAM	vCPU 2개	시스템 파티션과 별도의 로그용 파티션	30 GB

VM에는 다음과 같은 요구 사항도 필요합니다.

- Windows Server 2016+ 운영 체제(Linux 아님)
- 최소한 `cloud.tenable.com` 및 `*.tenable.ad`(TLS 1.2)에 대한 인터넷에 연결되어 있는 확인된 DNS 쿼리 및 인터넷 액세스
- 로컬 관리자 권한
- EDR, 바이러스 백신 및 GPO 구성:
    - VM에 CPU가 충분히 남아 있어야 합니다. 예를 들어 Windows Defender Real-Time 기능은 상당한 양의 CPU를 사용하여 성능이 부족할 수 있습니다.
    - 자동 업데이트:
        - `*.tenable.ad`에 대한 호출을 허용하여 자동 업데이트 기능이 Relay 실행 파일을 다운로드할 수 있어야 합니다.
        - 자동 업데이트 기능을 차단하는 그룹 정책 개체(GPO)가 없는지 확인하십시오.

- 'Relay 업데이트 프로그램'의 예약된 작업을 삭제하거나 변경하지 마십시오.



역할 권한

Relay를 구성하려면 역할 기반 권한이 있는 사용자여야 합니다. 필요한 권한은 다음과 같습니다.

- **데이터 엔터티**: 엔터티 릴레이
- **인터페이스 엔터티**:
  - 관리 > 시스템 > 구성 > 애플리케이션 서비스 > Relay
  - 관리 > 시스템 > Relay 관리

자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

허용된 파일 및 프로세스

Relay가 원활하게 작동하려면 바이러스 백신 및/또는 EDR(Endpoint Detection and Response)과 XDR (Extended Detection and Response) 등 타사 보안 도구에 대하여 특정 파일과 프로세스를 허용해야 합니다.

다음과 같은 파일 및 프로세스를 허용하십시오.

참고: C:\ 경로를 Relay 설치 드라이브에 맞춰 조정하십시오.

Windows
파일
C:\Tenable*
C:\tools*
C:\ProgramData\Tenable*
프로세스
nssm.exe --> 경로: C:\tools\nssm.exe
Tenable.Relay.exe --> 경로: C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> 경로: C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> 경로: C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> 경로: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe(OS 버전에 따라 다를 수 있음)
예약된 작업
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay

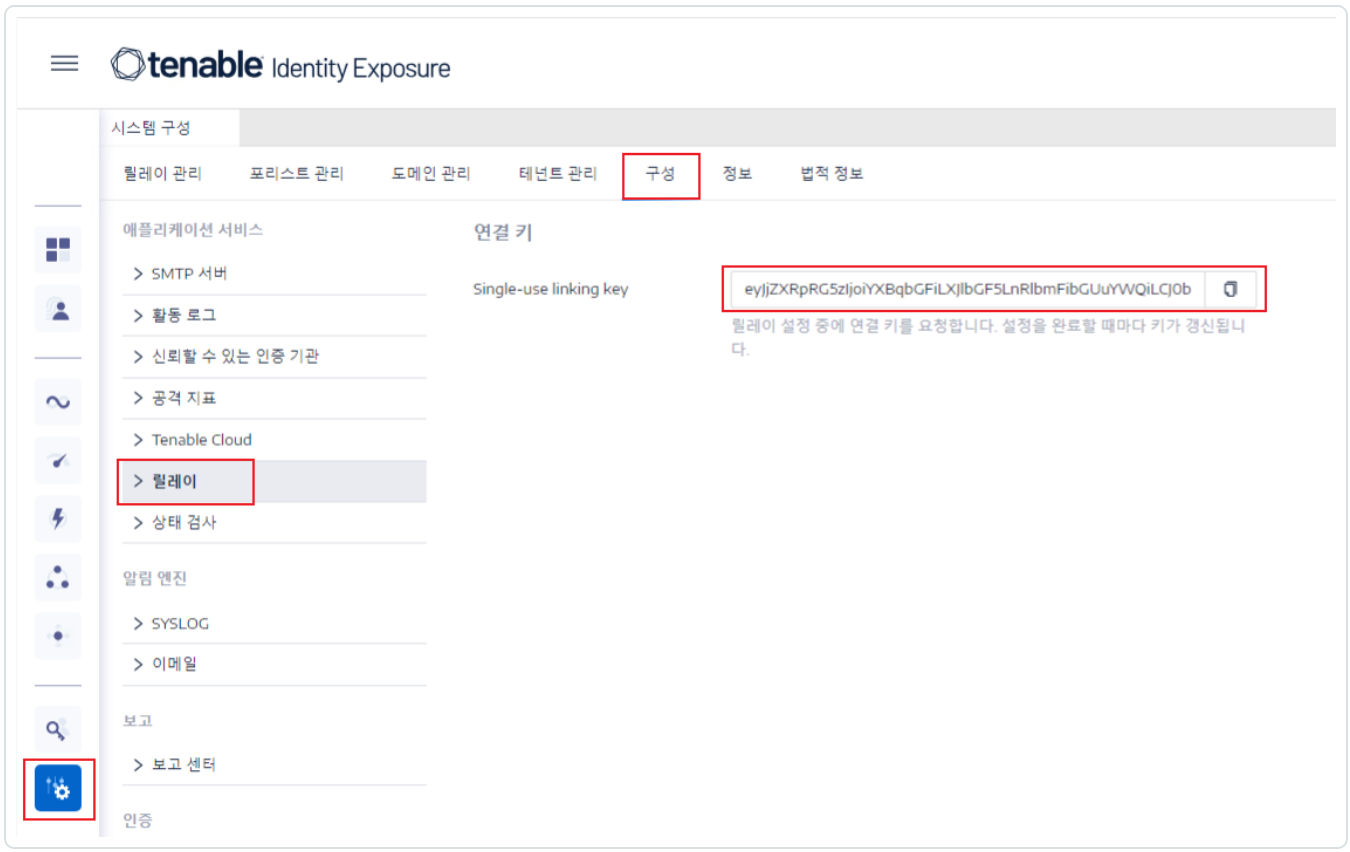
레지스트리 키
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

연결 키

Secure Relay를 설치하려면 네트워크 주소와 인증 토큰을 포함하는 일회용 연결 키가 필요합니다. Secure Realy를 설치할 때마다 Tenable Identity Exposure에서 새 키를 다시 생성합니다.

연결 키를 검색하는 방법:

1. Tenable Identity Exposure에서 왼쪽 메뉴 표시줄의 **시스템**을 클릭하고 **구성** 탭 > **Relay**를 선택합니다.



2. 를 클릭하여 연결 키를 복사합니다.

설치

Secure Relay를 설치하는 방법:

- 설치 방법을 선택합니다.
  - Secure Relay 설치(GUI)
  - Secure Relay(Tenable Nessus Agent) 설치

제거

Secure Relay를 제거하는 방법:

1. Windows에서 **설정** > **앱 및 기능** > **Tenable Identity Exposure Secure Relay**로 이동합니다.
2. **제거**를 클릭합니다.

   제거가 완료되면 Tenable Identity Exposure Secure Relay 서비스 및 환경 변수가 더 이상 시스템에 나타나지 않습니다.
3. Tenable Identity Exposure에서 왼쪽 메뉴 표시줄의 **시스템**을 클릭하고 **Relay 관리** 탭을 선택합니다.
4. 방금 제거한 릴레이를 선택하고  를 클릭하여 이용 가능한 릴레이 목록에서 해당 항목을 제거합니다.

자동 업데이트

Secure Relay를 설치한 후에 Tenable Identity Exposure에서 정기적으로 새 버전이 있는지 확인합니다. 이 프로세스는 완전 자동이며 도메인에 대한 HTTPS 액세스 권한이 필요합니다(TCP/443). 네트워크 트레이의 아이콘이 Tenable Identity Exposure에서 Secure Relay를 업데이트 중인지 표시합니다. 프로세스가 완료되면 Tenable Identity Exposure 서비스가 다시 시작되고 데이터 수집이 다시 시작됩니다.

참고 항목

Secure Relay에 대한 자세한 내용은 Tenable Identity Exposure 관리자 가이드의 Secure Relay를 참조하십시오.

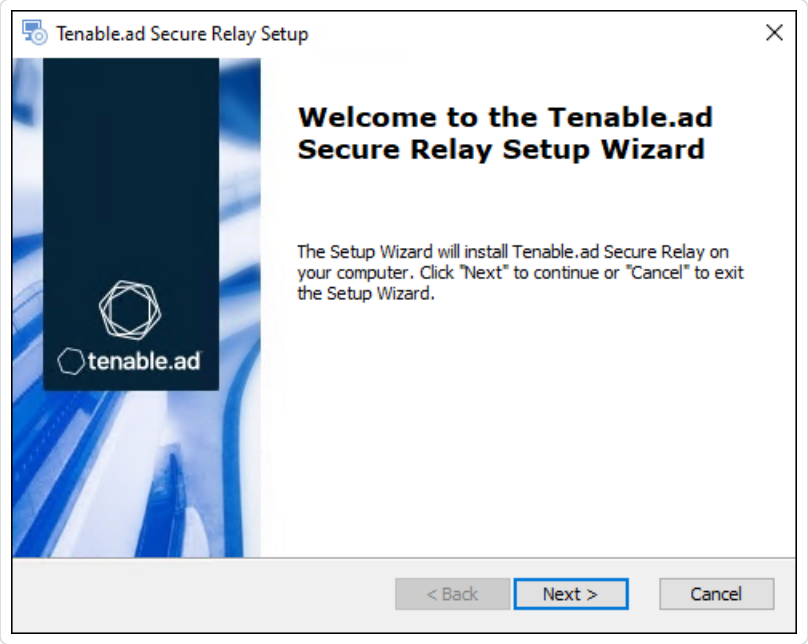
Secure Relay 설치(GUI)

다음 절차에서는 Windows 설치 프로그램으로 Secure Relay를 설치합니다. 시작하기 전에 Secure Relay에 설명된 대로 필수 조건을 충족하고 **필수 연결 키**가 있는지 확인하십시오.

Secure Relay를 설치하는 방법:

1. Tenable Identity Exposure 다운로드 포털에서 설치 프로그램을 VM에 다운로드합니다.
2. `tenable.ad_SecureRelay_v3.xx.x` 파일을 두 번 클릭하여 설치 마법사를 시작합니다.

   시작 화면이 표시됩니다.

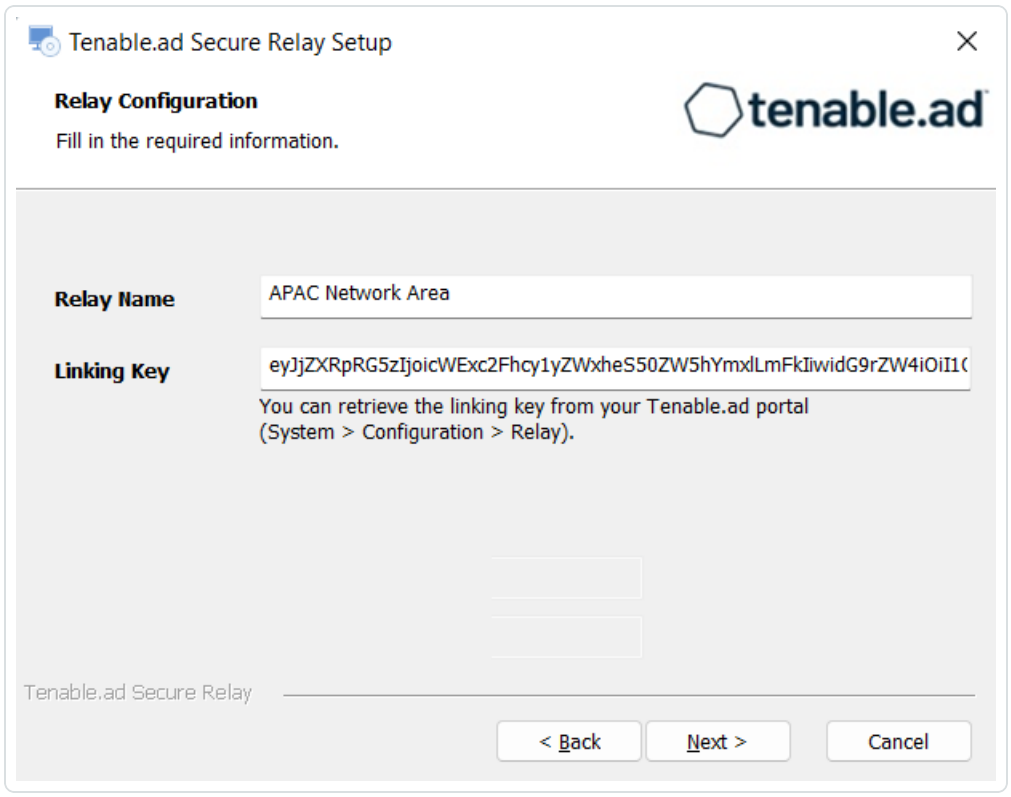


3. **다음**을 클릭합니다.

   사용자 지정 설정 창이 표시됩니다.

4. **찾아보기**를 클릭하여 Secure Relay를 위해 예약한 디스크 파티션(시스템 파티션과 별도)을 선택합니다.
5. **다음**을 클릭합니다.

   Relay 구성 창이 나타납니다.



6. 다음과 같은 정보를 입력합니다.

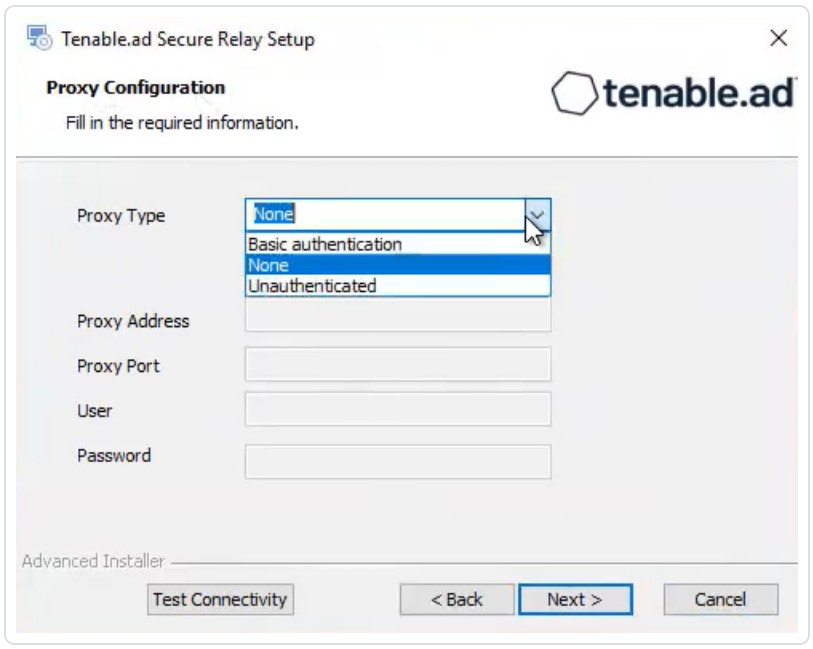
   a. **Relay 이름** 상자에 Secure Relay 이름을 입력합니다.

   b. **연결 키** 상자에 Tenable Identity Exposure 포털에서 검색한 연결 키를 붙여넣습니다.

   c. 프록시 서버를 사용하는 경우, **Relay 호출에 HTTP 프록시 사용** 옵션을 선택하고 프록시 주소와 포트 번호를 제공합니다.

7. **다음**을 클릭합니다.

   프록시 구성 창이 표시됩니다.



8. 다음 옵션 중 하나를 선택합니다.

   a. **없음**: 프록시 서버를 사용하지 않습니다.

   b. **인증되지 않음**: 프록시 서버의 주소와 포트를 입력합니다.

   c. **기본 인증**: 주소와 포트 외에 프록시 서버의 사용자와 비밀번호도 입력합니다.

   주의: "인증되지 않음" 또는 "기본 인증"을 사용하여 프록시를 구성하려면 릴레이는 IPv4 주소(예: `192.168.0.1`) 또는 `http://` 또는 `https://` 없는 프록시 URI(예: `myproxy.mycompany.com`)만 지원합니다. 이 릴레이는 IPv6 주소(예: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`)를 지원하지 않습니다.

9. **연결 테스트**를 클릭합니다. 다음과 같은 결과가 발생할 수 있습니다.

   - **녹색 표시등** - 연결에 성공했습니다.
   - **잘못된 연결 키** - Tenable Identity Exposure 포털에서 연결 키를 검색합니다.
   - **잘못된 Relay 이름** - 이 상자를 비워 둘 수 없습니다. 릴레이 이름을 입력합니다.
   - **연결 실패** - 인터넷 액세스를 확인합니다.

10. **다음**을 클릭합니다.

    설치 준비 완료 창이 표시됩니다.

11. **설치**를 클릭합니다.
12. 설치가 완료되면 **마침**을 클릭합니다.

다음에 할 일

- 설치 후 확인

참고 항목

- Secure Relay
- Secure Relay(Tenable Nessus Agent) 설치
- 설치 후 확인
- Relay 구성

Secure Relay(Tenable Nessus Agent) 설치

다음 절차에서는 Tenable Nessus Agent를 사용해 Secure Relay를 설치합니다.

시작하기 전에

- Tenable Nessus Agent를 다운로드하고 설치해야 합니다.

  참고: Tenable Nessus Agent 설치 프로그램에서 에이전트 키를 요청합니다. 이 키는 Secure Relay 기능에 **필수가 아닙니다**.

- 필요한 필수 조건을 충족하고 Secure Relay에 설명된 대로 **필수 연결 키**가 있어야 합니다.

Secure Relay를 설치하는 방법:

1. Tenable Nessus Agent를 호스팅하며 Relay 역할을 하는 컴퓨터의 Tenable Nessus Agent 디렉터리(`c:\Program Files\Tenable\Nessus Agent`)에서 관리자 명령 프롬프트 창을 열고 다음과 같은 명령을 입력합니다.

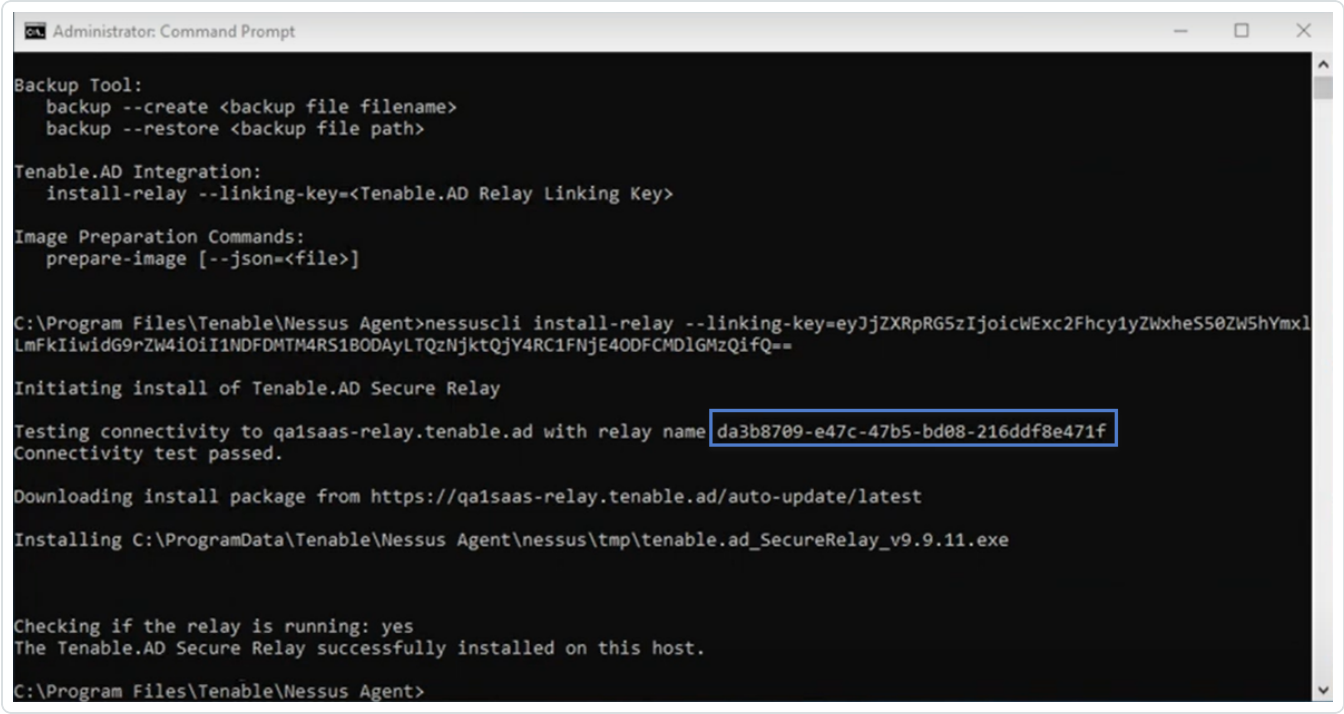
   Secure Relay 설치

   ```
   nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or DNS> --proxy-port=<Customer Proxy Port>
   ```

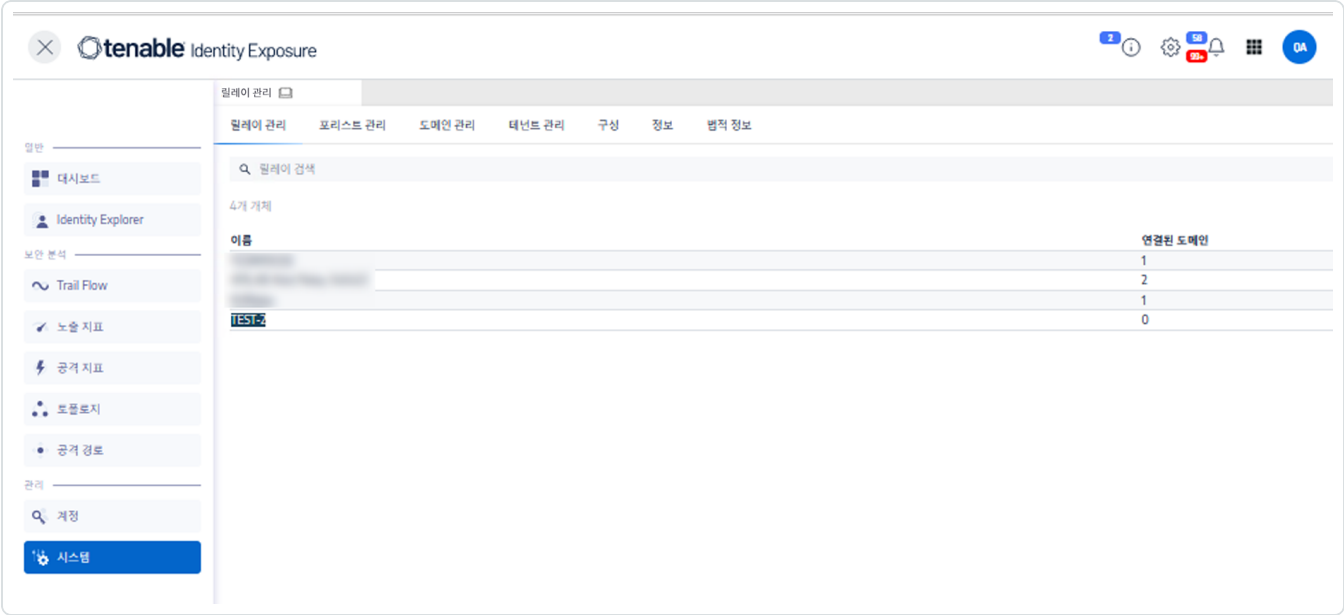
2. <Tenable Identity Exposure Relay 연결 키>를 Tenable Identity Exposure 인스턴스에서 이전에 복사한 값으로 대체하고 프록시 서버를 사용하는 경우 프록시 주소와 포트 번호를 입력합니다.

   설치가 시작됩니다. 연결을 확인하고 설치 프로세스를 실행하는 데 몇 분이 걸립니다.

   설치가 완료되면 Relay가 호스트 컴퓨터에서 실행 중이라는 메시지가 표시됩니다.



3. Tenable Identity Exposure에서 **시스템** > **Relay 관리**를 클릭합니다. 새로 설치된 Relay가 Relay 목록에 표시되며 설치 창에 식별자도 함께 표시됩니다.



다음에 할 일

- 설치 후 확인

참고 항목

- Secure Relay
- Secure Relay 설치(GUI)
- 설치 후 확인
- Relay 구성

설치 후 확인

Secure Relay 설치가 완료되면 다음을 확인하십시오.

Tenable Identity Exposure에 설치된 Relay 목록

설치된 Relay 목록을 확인하는 방법:

- Tenable Identity Exposure에서 왼쪽 메뉴 표시줄의 **시스템**을 클릭하고 **Relay 관리** 탭을 선택합니다.

  창에 Secure Relay 및 연결된 도메인 목록이 표시됩니다.

서비스

설치하면 다음과 같은 서비스가 실행됩니다.

- `Tenable_Relay`
- `tenable_envoy`

  > **참고**: Envoy 라이선스는 **시스템** > **법적 정보** > **Envoy 라이선스**의 Tenable Identity Exposure에서 확인할 수 있습니다 .

환경 변수

또한 설치하면 이름이 "ALSID"로 시작되는 Secure Relay와 관련된 4개의 환경 변수가 추가됩니다. 프록시 서버를 사용하는 경우, 프록시 IP 및 포트와 관련된 추가 변수 2개가 있습니다.

문제 해결을 위한 로그

다음 위치에서 로그를 확인할 수 있습니다.

- **설치 로그**: `C:\Users\<your user>\AppData\Local\Temp`
- **Relay 로그**: Secure Relay를 호스팅하는 VM에서 설치할 때 지정한 폴더

다음에 할 일

- Relay 구성

참고 항목

- Secure Relay
- Secure Relay 설치(GUI)
- Secure Relay(Tenable Nessus Agent) 설치

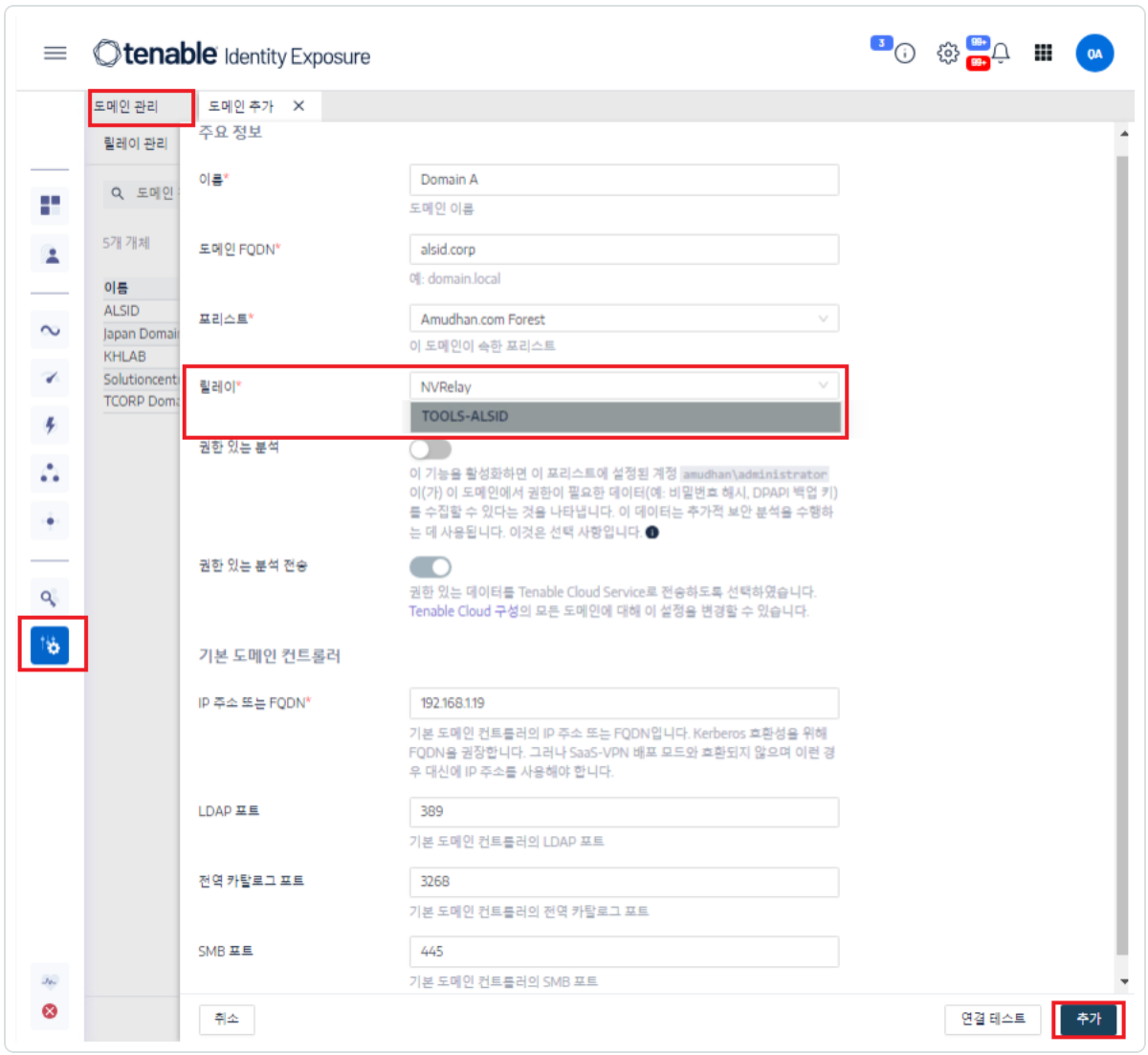
Relay 구성

설치 및 설치 후 확인까지 끝나면 도메인에 연결하고 경고를 설정하도록 Tenable Identity Exposure에서 Relay를 구성합니다.

도메인을 Secure Relay에 연결하는 방법:

1. Tenable Identity Exposure에서 왼쪽 메뉴 표시줄의 **시스템**을 클릭하고 **도메인 관리** 탭을 선택합니다.
2. 도메인 목록에서 연결할 도메인을 선택하고 줄 끝의 ✎를 클릭합니다.

   도메인 편집 창이 열립니다.
3. **Relay** 상자에서 화살표를 클릭하여 설치된 릴레이 드롭다운 목록을 표시하고 해당 도메인에 연결할 릴레이를 선택합니다.



4. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 도메인을 업데이트했다고 확인합니다. Sysvol과 LDAP이 수정 사항을 포함하여 동기화합니다. Trail Flow가 새 이벤트를 수신하기 시작합니다.

참고 항목

- Secure Relay
- Secure Relay 설치(GUI)
- Secure Relay(Tenable Nessus Agent) 설치
- 설치 후 확인

공격 지표 배포

참고: 이 정보는 공격 지표 모듈 혜택이 적용되는 라이선스에만 해당합니다.

Tenable Identity Exposure의 **공격 지표**(IoA)를 이용하면 Active Directory(AD)에서 공격을 탐지할 수 있습니다. IoA마다 설치 스크립트가 자동으로 사용하도록 설정하는 특정 감사 정책이 있어야 합니다. Tenable Identity Exposure IoA 및 구현의 전체 목록은 Tenable 다운로드 포털의 Tenable Identity Exposure 공격 지표 참조 가이드를 참조하십시오.

공격 지표 및 Active Directory

Tenable Identity Exposure에서는 에이전트를 배포하지 않고 환경 구성 변경을 최소화하여 Active Directory 인프라를 모니터링하는 비침해적 솔루션으로 작동합니다.

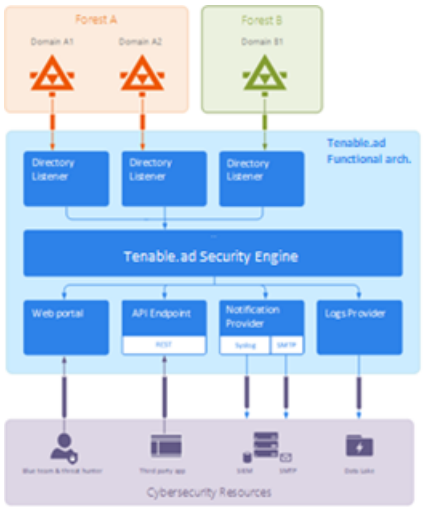
Tenable Identity Exposure에서는 관리자 권한 없는 일반적인 사용자 계정을 사용해 표준 API에 연결하여 보안 모니터링 기능을 이용합니다.

Tenable Identity Exposure에서는 Active Directory 복제 메커니즘을 사용하여 관련 정보를 가져오며 각 도메인의 PDC와 Tenable Identity Exposure의 Directory Listener 사이에서 제한된 대역폭 비용만 발생합니다.

Tenable Identity Exposure에서는 공격 지표를 사용해 효율적으로 보안 인시던트를 탐지하기 위해 ETW(Event Tracing for Windows)와 각 도메인 컨트롤러에서 사용 가능한 복제 메커니즘을 사용합니다. 이러한 정보를 수집하려면 공격 지표 설치에 설명된 것과 같이 Tenable Identity Exposure의 스크립트를 사용해 전용 그룹 정책 개체(GPO)를 배포합니다.

이 GPO는 Windows EvtSubscribe API를 통해 시스템 볼륨(SYSVOL)에 쓰기 작업을 하는 모든 도메인 컨트롤러에 이벤트 로그 리스너를 활성화하여 AD 복제 엔진과 Tenable Identity Exposure의 SYSVOL 이벤트 수신 기능을 유리하게 활용합니다. GPO는 각 도메인 컨트롤러에 SYSVOL 파일을 만들고 그 내용을 정기적으로 플러시합니다.

보안 모니터링을 시작하려면, Tenable Identity Exposure에서는 Microsoft의 표준 디렉터리 API에 연결해야 합니다.



도메인 컨트롤러

Tenable Identity Exposure에서는 네트워크 흐름 매트릭스에 설명된 네트워크 프로토콜을 사용하여 기본 도메인 컨트롤러 에뮬레이터(Primary Domain Controller Emulator, PDCe)와 통신하기만 하면 됩니다.

모니터링하는 도메인 또는 포리스트가 여러 개인 경우, Tenable Identity Exposure에서는 각 도메인의 PDCe에 연결해야 합니다. Tenable은 최상의 성능을 위해 모니터링할 PDCe에 가까운 물리적 네트워크에서 Tenable Identity Exposure를 호스팅하도록 권장하고 있습니다.

사용자 계정

Tenable Identity Exposure에서는 관리자가 아닌 사용자 계정을 사용해 복제 흐름에 액세스하여 모니터링하는 인프라에 인증합니다.

단순한 Tenable Identity Exposure 사용자가 모든 수집한 데이터에 액세스할 수 있습니다. Tenable Identity Exposure에서는 자격 증명, 비밀번호 해시 또는 Kerberos 키와 같은 암호 특성에 액세스하지 않습니다.

Tenable에서는 다음과 같이 "도메인 사용자" 그룹의 멤버인 서비스 계정을 만드는 것을 권장합니다.

- 서비스 계정은 모니터링하는 기본 도메인에 있습니다.
- 서비스 계정은 임의의 조직 단위(OU)에 있으며 다른 보안 서비스 계정을 만든 OU를 선호합니다.

- 서비스 계정에는 일반 사용자 그룹 멤버 자격이 있습니다(예: 도메인 사용자 AD 기본 그룹의 멤버).

시작하기 전에

- IoA 설치의 한계와 잠재적 영향을 검토합니다(기술 변경 사항 및 잠재적 영향의 설명 참조).
- DC에 Active Directory 및 GroupPolicy용 PowerShell 모듈이 설치되어 있고 사용할 수 있는지 확인합니다.
- DC에 분산 파일 시스템 도구 기능 RSAT-DFS-Mgmt-Con이 사용으로 설정되어 배포 스크립트가 복제 상태를 검사할 수 있는지 확인합니다. DC가 복제 중일 때는 GPO를 만들 수 없기 때문입니다.
- Tenable Identity Exposure에서는 플랫폼의 중단을 제한하기 위해 사용량이 적은 시간에 IoA를 설치/업그레이드하도록 권장합니다.
- 권한 확인 - IoA를 설치하려면 다음과 같은 권한을 보유한 사용자 역할이 있어야 합니다.
  - **데이터 엔터티**에서 다음에 대한 "읽기" 액세스:
    - 모든 공격 지표
    - 모든 도메인
  - **인터페이스 엔터티**에서 다음에 대한 액세스:
    - 관리 > 시스템 > 구성
    - 관리 > 시스템 > 구성 > 애플리케이션 서비스 > 공격 지표
    - 관리 > 시스템 > 구성 > 애플리케이션 서비스 > 공격 지표 > 설치 파일 다운로드

  역할 기반 권한에 관한 자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

참고 항목

- 공격 지표 설치
- 공격 지표 설치 스크립트
- 기술 변경 사항 및 잠재적 영향

- Microsoft Sysmon 설치, 일부 Tenable Identity Exposure의 공격 지표가 관련 시스템 데이터를 얻으려면 필요한 Windows 시스템 도구입니다.
- 공격 지표 문제 해결

공격 지표 설치

필수 사용자 역할: Tenable Identity Exposure에서 공격 지표 구성을 수정할 권한이 있는 조직 사용자. 자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

Tenable Identity Exposure의 공격 지표(IoA) 모듈에서는 새 그룹 정책 개체(GPO)를 만들어 조직 단위(OU)에 연결할 수 있는 관리자 계정으로 PowerShell 설치 스크립트를 실행해야 합니다. 이 스크립트는 Tenable Identity Exposure에서 모니터링하고 네트워크를 통해 도메인 컨트롤러에 연결할 수 있는 Active Directory 도메인에 조인된 모든 컴퓨터에서 실행할 수 있습니다.

이 설치 스크립트는 각 AD 도메인에서 한 번씩만 실행하면 됩니다. 생성된 GPO가 기존 및 신규 도메인 컨트롤러(DC)에 모두 이벤트 수신기를 자동으로 배포하기 때문입니다.

또한, "자동 업데이트" 옵션을 사용하면 IoA 구성을 변경하더라도 설치 스크립트를 다시 실행할 필요가 없습니다.

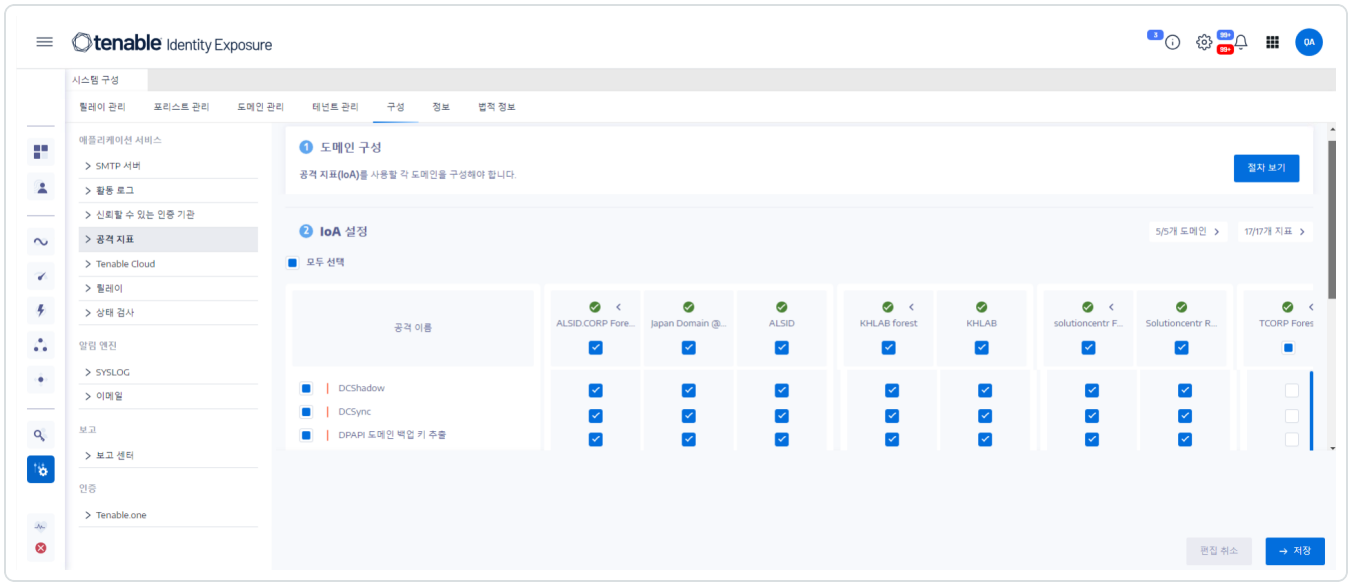
IoA에 대한 도메인을 구성하는 방법:

1. Tenable Identity Exposure에서 왼쪽 메뉴 표시줄의 **시스템**을 클릭하고 **구성** 탭을 클릭합니다.

   구성 창이 표시됩니다.

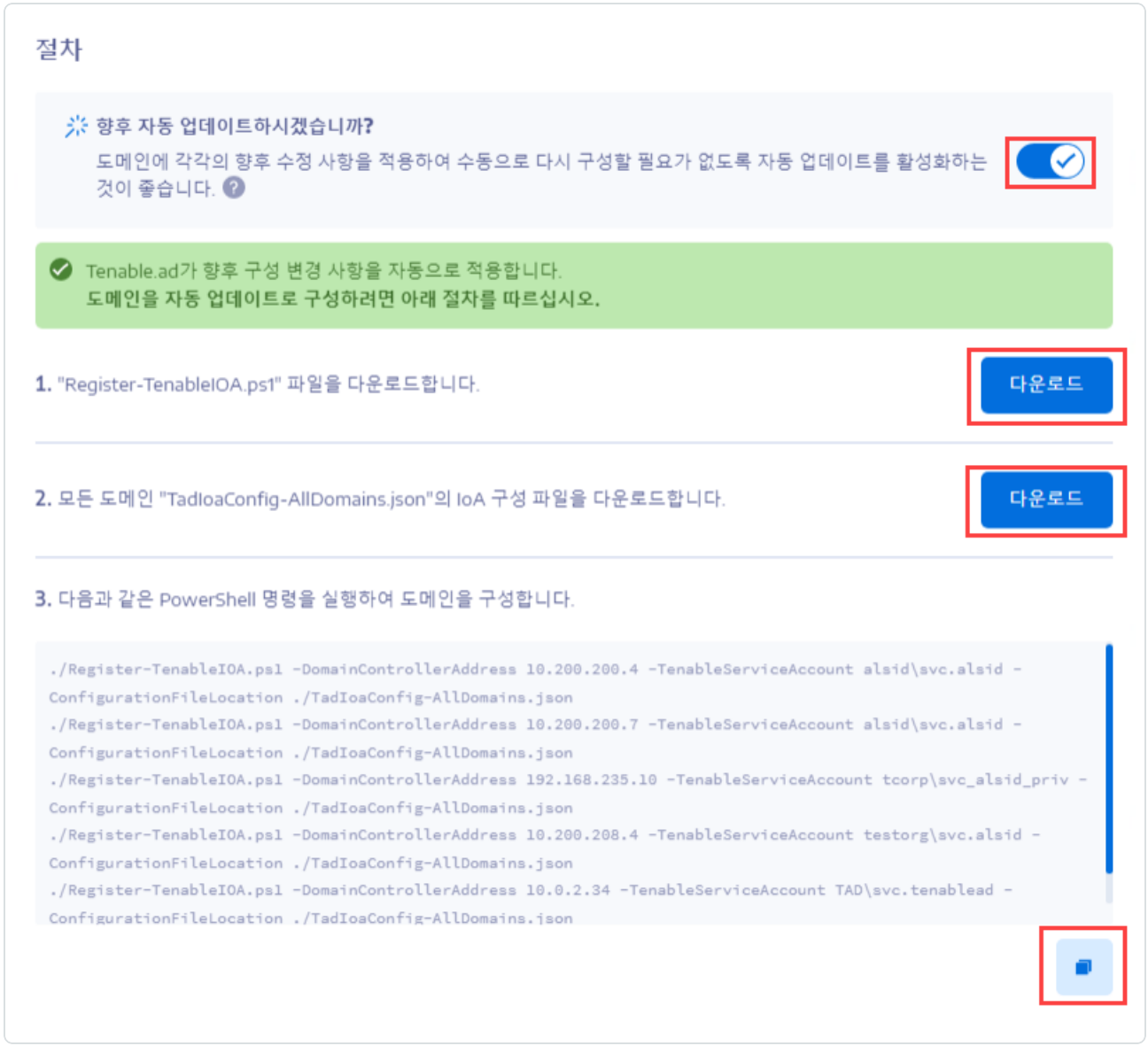
2. **공격 지표**를 클릭합니다.

   IoA 구성 창이 표시됩니다.



3. **(1) 도메인 구성**에서 **절차 보기**를 클릭합니다.

   절차 창이 열립니다.



4. **향후 자동 업데이트** 아래에서:

   - 기본 옵션인 **사용**으로 설정하면 향후 사용자가 Tenable Identity Exposure에서 IoA 구성을 수정할 때마다 Tenable Identity Exposure에서 자동으로 해당 구성을 업데이트합니다. 이렇게 하면 지속적인 보안 분석도 보장됩니다.

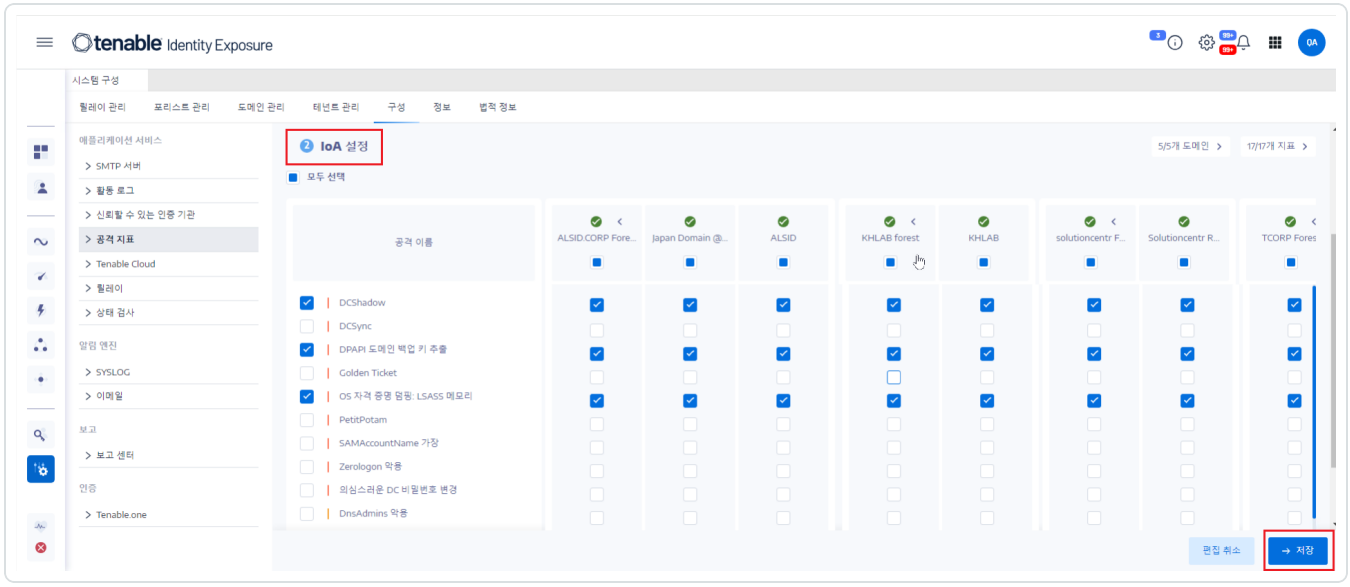
- 이 옵션을 비활성화하면 메시지가 표시되어 향후 자동 업데이트를 받을 것인지 물어봅니다. **절차 보기**를 클릭하고 **사용**으로 설정합니다.

5. **다운로드**를 클릭하여 각 도메인에 대해 실행할 스크립트를 다운로드합니다(`Register-TenableIOA.ps1`).
6. **다운로드**를 클릭하여 도메인에 대한 구성 파일(`TadIoaConfig-AllDomains.json`)을 다운로드합니다.
7. 를 클릭하여 도메인을 구성할 Powershell 명령을 복사합니다.
8. 절차 창 바깥을 클릭하여 창을 닫습니다.
9. 관리자 권한으로 PowerShell 터미널을 열고 명령을 실행하여 IoA에 대한 도메인 컨트롤러를 구성합니다.

> **참고**: IoA를 설치하고 도메인을 쿼리하는 데 사용하는 서비스 계정에 Tenable Identity Exposure(구 Tenable.ad) GPO 폴더의 쓰기 권한이 있어야 합니다. 설치 스크립트가 이 권한을 자동으로 추가합니다. 이 권한을 제거하면 Tenable Identity Exposure에 오류 메시지가 표시되며 자동 업데이트가 더 이상 작동하지 않습니다. 자세한 내용은 공격 지표 설치 스크립트을 참조하십시오.

IoA를 설정하는 방법:

1. IoA 구성 창의 **IoA 설정** 아래에서 구성하려는 IoA를 선택합니다.

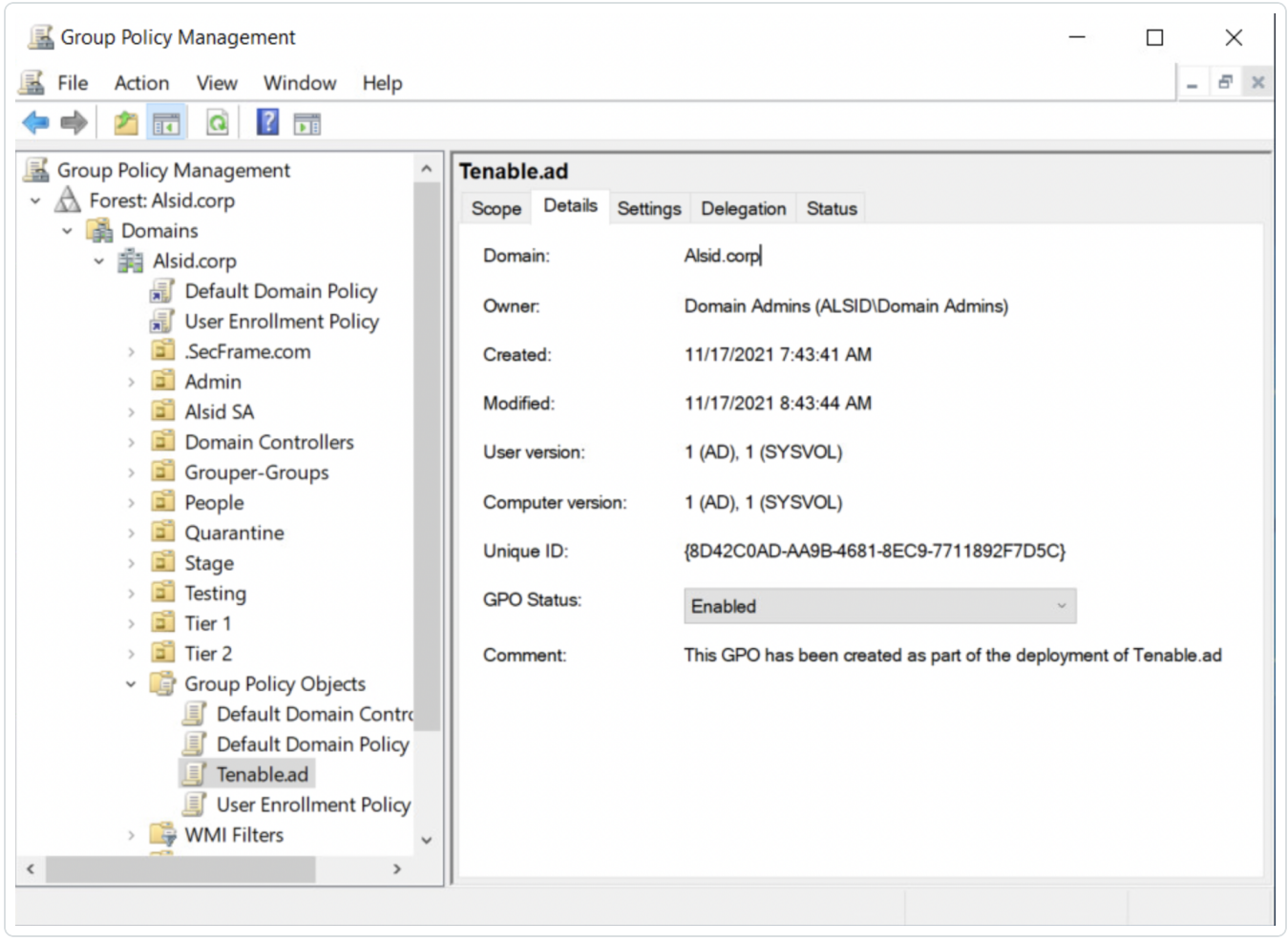


팁: **Zerologon Exploitation** 공격 지표(IoA)는 2020년부터 시작되었습니다. 모든 도메인 컨트롤러(DC)가 최근 3년 이내에 업데이트를 받은 경우, 이 취약성으로부터 보호됩니다. 이 취약성으로부터 DC를 보호하기 위한 필수 패치를 확인하려면 Microsoft의 Netlogon 권한 상승 취약성 정보를 참조하십시오. DC의 보안을 확인하고 나면 이 IoA를 안전하게 비활성화하여 불필요한 알림을 받지 않도록 할 수 있습니다.

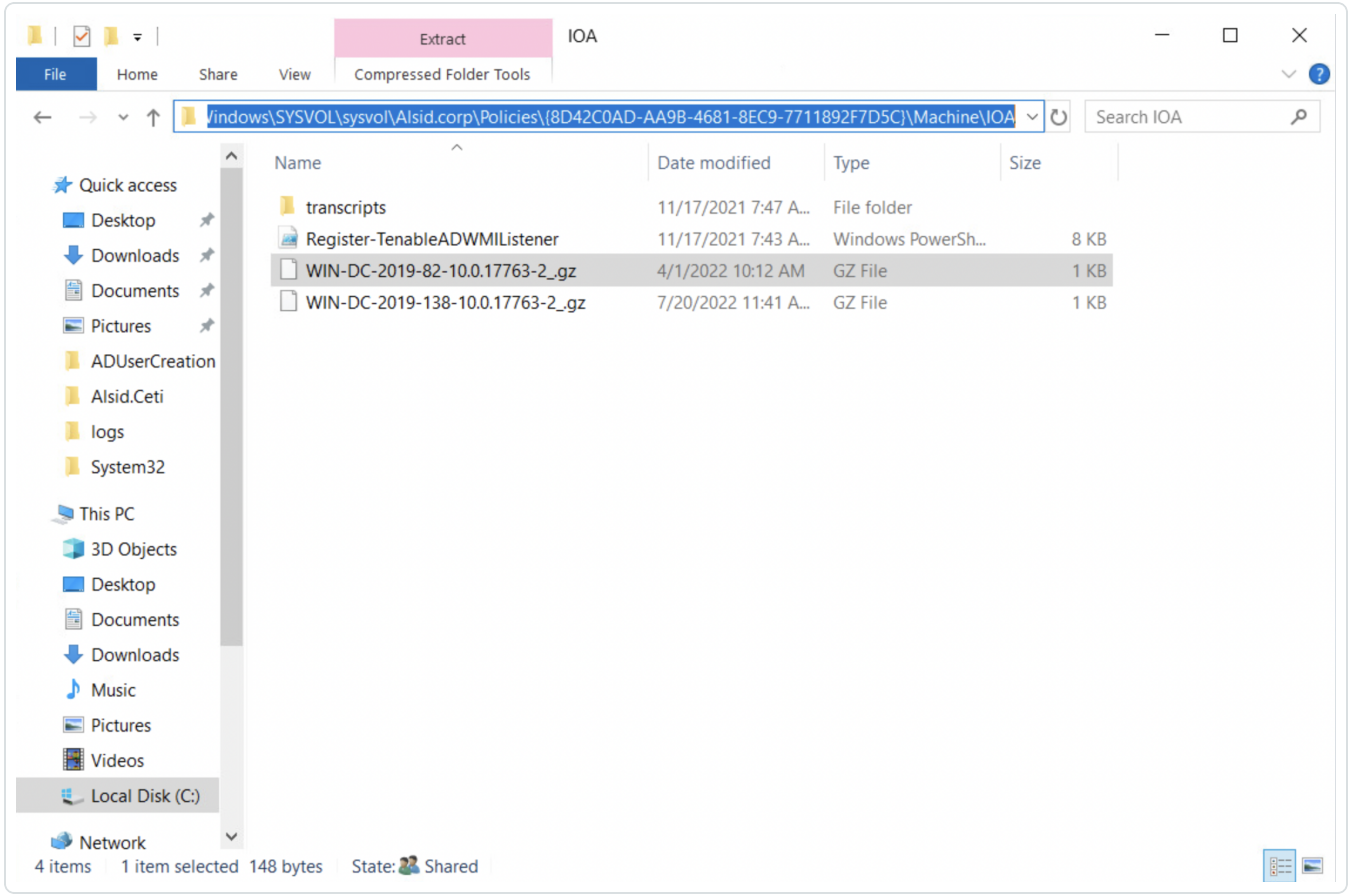
2. **저장**을 클릭합니다.
    - **향후 자동 업데이트**를 사용으로 설정한 경우, Tenable Identity Exposure에서 새 구성을 저장하고 자동으로 업데이트합니다. 이 업데이트가 적용되려면 몇 분 걸립니다.
    - **향후 자동 업데이트**를 사용으로 설정하지 않은 경우, 절차 창이 나타나서 IoA에 대한 도메인을 구성하는 방법:(으)로 안내합니다.

IoA 설치를 확인하는 방법:

1. 그룹 정책 관리에서 새 Tenable Identity Exposure GPO가 생겼으며 도메인 컨트롤러 OU에 연결되는지 확인합니다.



2. `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` 경로로 이동해서 **모든 도메인 컨트롤러**에 대해 `.gz` 파일이 존재하는지 확인한 다음, IoA를 테스트하십시오.



Tenable Identity Exposure 서비스 계정에 대한 "쓰기" 권한 액세스를 확인하는 방법:

1. 파일 관리자에서 `\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\`으로 이동합니다.
2. "IOA" 폴더를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
3. **보안** 탭을 선택하고 **고급**을 클릭합니다.
4. **유효 액세스** 탭을 클릭합니다.
5. **사용자 선택**을 클릭합니다.
6. `<TENABLE-SERVICE-ACCOUNT-NAME>`유형에서 **확인**을 클릭합니다.
7. **유효 액세스 보기**를 클릭합니다.
8. "쓰기" 권한이 활성화되었는지 확인하십시오.

또는 Powershell을 사용할 수도 있습니다.

- 다음 명령을 실행하십시오.

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\IOA\ -
Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

IoA를 보정하는 방법

공격의 오탐 및 미탐을 피하려면 IoA를 환경에 따라 보정해야 합니다. 그러려면 Active Directory의 크기에 따라 이를 맞추거나 알려진 도구를 허용 목록에 추가하는 등의 조처가 필요합니다.

1. 선택하는 옵션 또는 권장하는 값에 관한 자세한 정보는Tenable Identity Exposure공격 지표 참조 가이드를 참조하십시오.
2. 지표 사용자 지정에 설명된 대로 보안 프로필에서 각 IoA에 옵션과 값을 적용합니다.

문제 해결

배포 중에 다음과 같은 오류 메시지가 표시될 수 있습니다.

메시지	수정
"Tenable Identity Exposure에서 구성 파일에 쓸 수 없습니다. 대상 폴더 <targetFolder>가 존재하지 않습니다. 이것은 IoA 모듈 배포가 실패했을 수 있음을 나타냅니다."	스크립트를 제거하고 "절차 보기"를 클릭하여 스크립트를 다시 설치하는 방법을 참조하십시오.
"Tenable Identity Exposure에서 <targetFile>에 있는 구성 파일을 업데이트하기 위해 파일에 쓰지 못했습니다. 다른 프로세스가 파일을 잠갔거나 권한이 변경되었기 때문일 수 있습니다."	• IoA 모듈 외에 다른 프로세스가 구성 파일을 사용하고 있지 않은지 확인하십시오. • 서비스 계정에 파일 내용을 수정할 권한이 있는지 확인하십시오. • 서비스 계정에 권한을 부여하고 싶지 않은 경우, "자동 업데이트" 토글을 사용 안 함으로 설정하고 "절차 보기"를 클릭하여

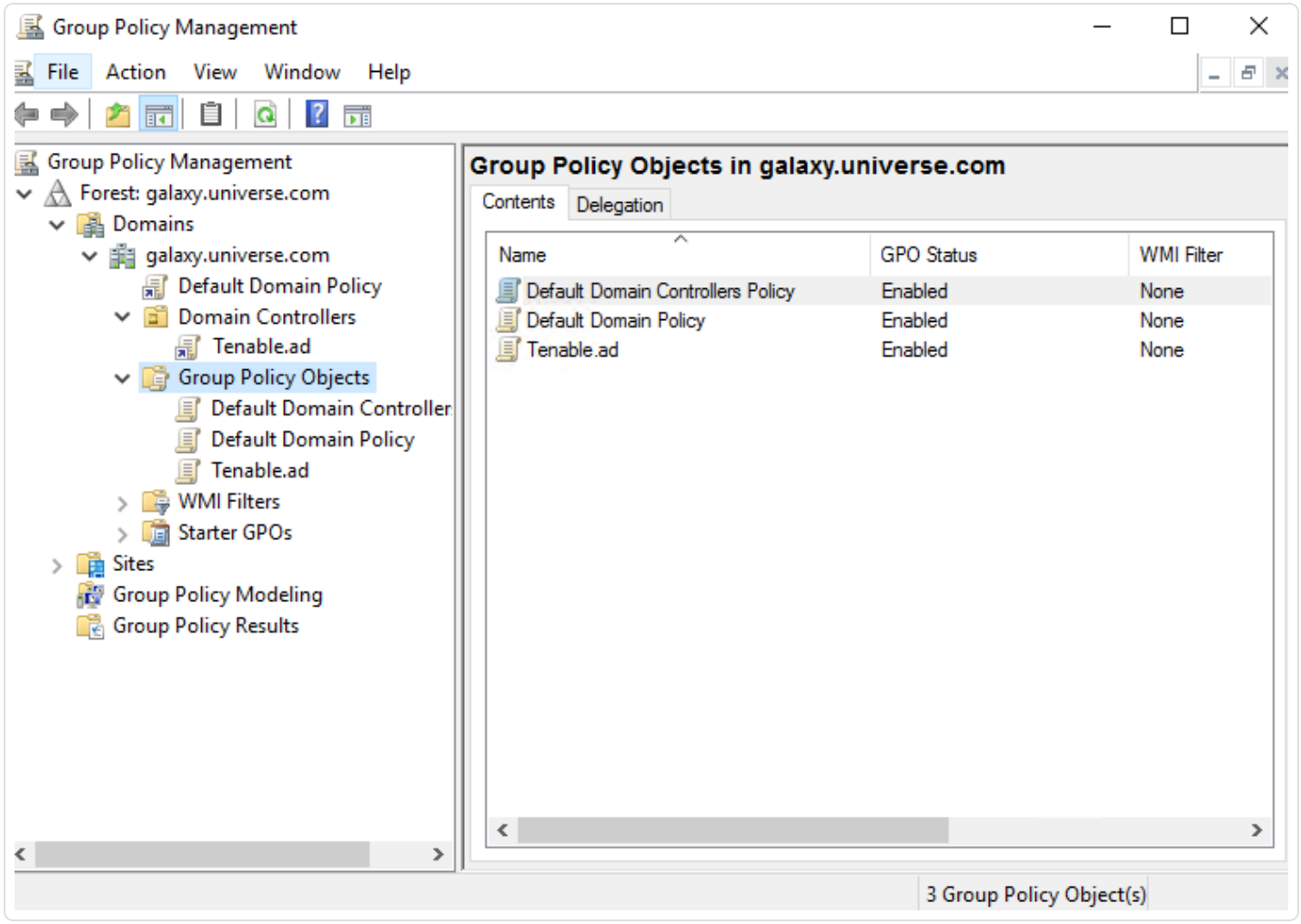
	IoA 구성을 수정할 때마다 수동으로 업데이트하는 방법을 참조하십시오.
"대상 폴더 <targetFolder>에 포함된 Tenable Identity Exposure 버전이 자동 업데이트를 실행할 수 없습니다."	현재 설치된 스크립트는 WMI를 사용하는 오래된 버전입니다. 현재 버전을 제거하고 새 설치 스크립트를 다운로드한 다음 스크립트를 실행합니다.
"구성 파일 배포에 예기치 않은 오류가 발생했습니다."	스크립트를 제거하고 "절차 보기"를 클릭하여 스크립트를 다시 설치하는 방법을 참조하십시오. 그래도 문제가 해결되지 않으면 고객 지원 담당자에게 문의하시기 바랍니다.

자세한 내용은 다음을 참조하십시오.

- 공격 지표 설치 스크립트
- 기술 변경 사항 및 잠재적 영향
- 바이러스 백신 탐지
- 고급 감사 정책 구성 우선 순위

공격 지표 설치 스크립트

공격 지표(IoA) 설치 파일을 다운로드하여 실행하면 IoA 스크립트가 Active Directory(AD) 데이터베이스에서 기본적으로 `Tenable.ad`라는 이름이 지정된 새 그룹 정책 개체(GPO)를 만듭니다. 시스템은 Tenable Identity Exposure GPO를 모든 도메인 컨트롤러(DC)를 포함한 도메인 컨트롤러 조직 단위(OU)에만 연결합니다. 새 정책은 GPO 메커니즘을 사용해 모든 DC 사이에 자동으로 복제됩니다.



설치 스크립트(Tenable Identity Exposure v. 3.29)

GPO에는 다음과 같이 모든 DC가 로컬에서 실행하여 관심 데이터를 수집하는 PowerShell 스크립트가 포함되어 있습니다.

- 이 스크립트는 Windows EvtSubscribe API를 사용하여 각 도메인 컨트롤러에서 이벤트 로그 수신기를 구성합니다. 스크립트는 `TenableADEventsListenerConfiguration.json` 구성 파일

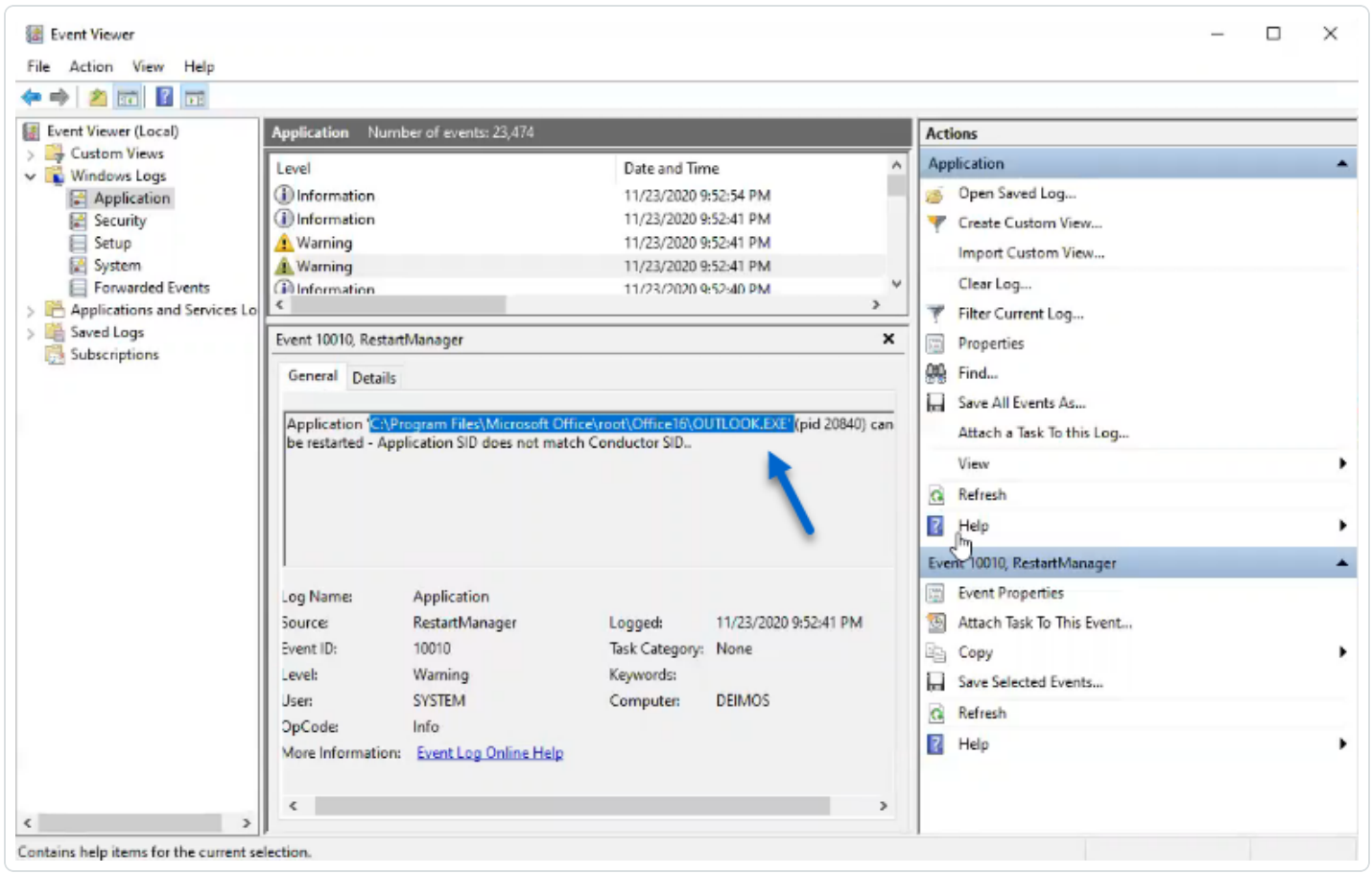
에 지정된 대로 일치하는 각 이벤트 로그에 대해 EvtSubscribe에 의해 트리거되는 콜백 및 요청을 제출하여 필요한 각 이벤트 로그 채널을 구독합니다.

- 이벤트 수신기는 이벤트 로그를 수신하고 Sysvol이라는 네트워크 공유에 저장된 파일로 주기적으로 플러시하기 전에 이벤트 로그를 버퍼링합니다. 각 DC는 수집된 이벤트를 저장하는 Sysvol 파일 하나에 플러시하고 다른 도메인 컨트롤러에 복제합니다.
- 또한 이 스크립트는 DC가 다시 시작될 때 이벤트 구독자를 다시 등록하여 이 메커니즘이 지속되도록 WMI 소비자를 만듭니다. WMI는 소비자가 이벤트 수신기를 다시 등록할 수 있도록 DC가 다시 시작될 때마다 소비자에게 알립니다.
- 이 시점에 분산 파일 시스템(DFS) 복제가 발생하여 여러 도메인 컨트롤러 간에 파일을 자동으로 동기화합니다. Tenable Identity Exposure의 플랫폼은 유입되는 DFS 복제 트래픽을 수신 대기하고 이 데이터를 사용하여 이벤트를 수집하고 보안 분석을 실행한 다음 IoA 알림을 생성합니다.

로컬 데이터 가져오기

Windows 이벤트 로그는 운영 체제와 애플리케이션에서 발생하는 모든 이벤트를 기록합니다. 이벤트 로그는 Windows에 통합된 구성 요소의 프레임워크에 의존합니다.

Tenable Identity Exposure IoA 이벤트 로그 수신기는 EvtSubscribe API를 사용하여 이벤트 로그에서 추출하는 삽입 문자열 형식으로 유용한 이벤트 로그 데이터 세그먼트만 수집합니다. Tenable Identity Exposure에서는 이러한 삽입 문자열을 Sysvol 폴더에 저장된 파일에 쓰고 DFS 엔진을 통해 복제합니다. 그러면 Tenable Identity Exposure에서 이벤트 로그로부터 보안 분석을 실행하고 공격을 탐지하기에 적절한 양의 데이터만 수집할 수 있습니다.



IoA 스크립트 요약

다음 표는 Tenable Identity Exposure 스크립트 배포에 관한 개요입니다.

단계	설명	관련된 구성 요소	기술적 조치
1	Tenable Identity Exposure의 IoA 배포 등록	GPO 관리	`Tenable.ad`(기본 이름) GPO를 만들고 도메인 컨트롤러 OU에 연결합니다.
2	DC에서	DC 로컬	AD 복제 및 그룹 정책 새로 고침 간격에 따라 각 DC가 적용할 새

	Tenable Identity Exposure의 IoA 배포 시작	시스템	GPO를 탐지합니다.
3	고급 로깅 정책 상태 제어	DC 로컬 시스템	시스템이 레지스트리 키 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`를 설정하여 고급 로깅 정책을 활성화합니다.
4	로컬 로깅 정책 업데이트	DC 로컬 시스템	탐지하려는 IoA에 따라 Tenable Identity Exposure에서는 특정 감사 정책을 동적으로 생성하고 활성화합니다. 이 정책은 기존 로깅 정책을 비활성화하지 않으며 필요한 경우 보강하기만 합니다. 충돌이 탐지되면 GPO 설치 스크립트가 중단되고 "Tenable Identity Exposure에 감사 정책이 필요 '...' 하지만 현재 AD 구성이 그 사용을 방지합니다."와 같은 메시지가 표시됩니다.
5	이벤트 수신기 및 WMI 생산자 등록	DC 로컬 시스템	시스템은 GPO에 포함된 스크립트를 등록하고 실행합니다. 이 스크립트는 PowerShell 프로세스를 실행하여 EvtSubscribe API를 사용하는 이벤트 로그를 구독하고 지속성을 위해 `ActiveScriptEventConsumer` 인스턴스를 만듭니다. Tenable Identity Exposure에서 이러한 개체를 사용해 이벤트 로그 콘텐츠를 수신하고 저장합니다.
6	이벤트 로그 메시지 수집	DC 로컬 시스템	Tenable Identity Exposure에서 관련 이벤트 로그 메시지를 캡처하고 주기적으로 버퍼링한 다음 Tenable Identity ExposureGPO(`...{GPO_GUID}\Machine\IOA<DC_name>`)에 연결된 Sysvol 폴더에 저장된 파일(DC당 한 개)에 저장합니다.
7	선언된 DC SYSVOL 폴더에 파일 복	Active Directory	AD는 DFS를 사용해 도메인 전체(특히 선언된 DC)에 파일을 복제합니다. Tenable Identity Exposure 플랫폼은 각 파일에 대한 알림을 받고 해당 내용을 읽습니다.

	제		
8	이러한 파일 덮어쓰기	Active Directory	각각의 DC가 같은 파일에서 주기적으로 버퍼링된 이벤트를 자동으로 지속적으로 씁니다.

설치 스크립트(Tenable Identity Exposure v. 3.19.11 이하)

GPO에는 다음과 같이 모든 DC가 로컬에서 실행하여 관심 데이터를 수집하는 PowerShell 스크립트가 포함되어 있습니다.

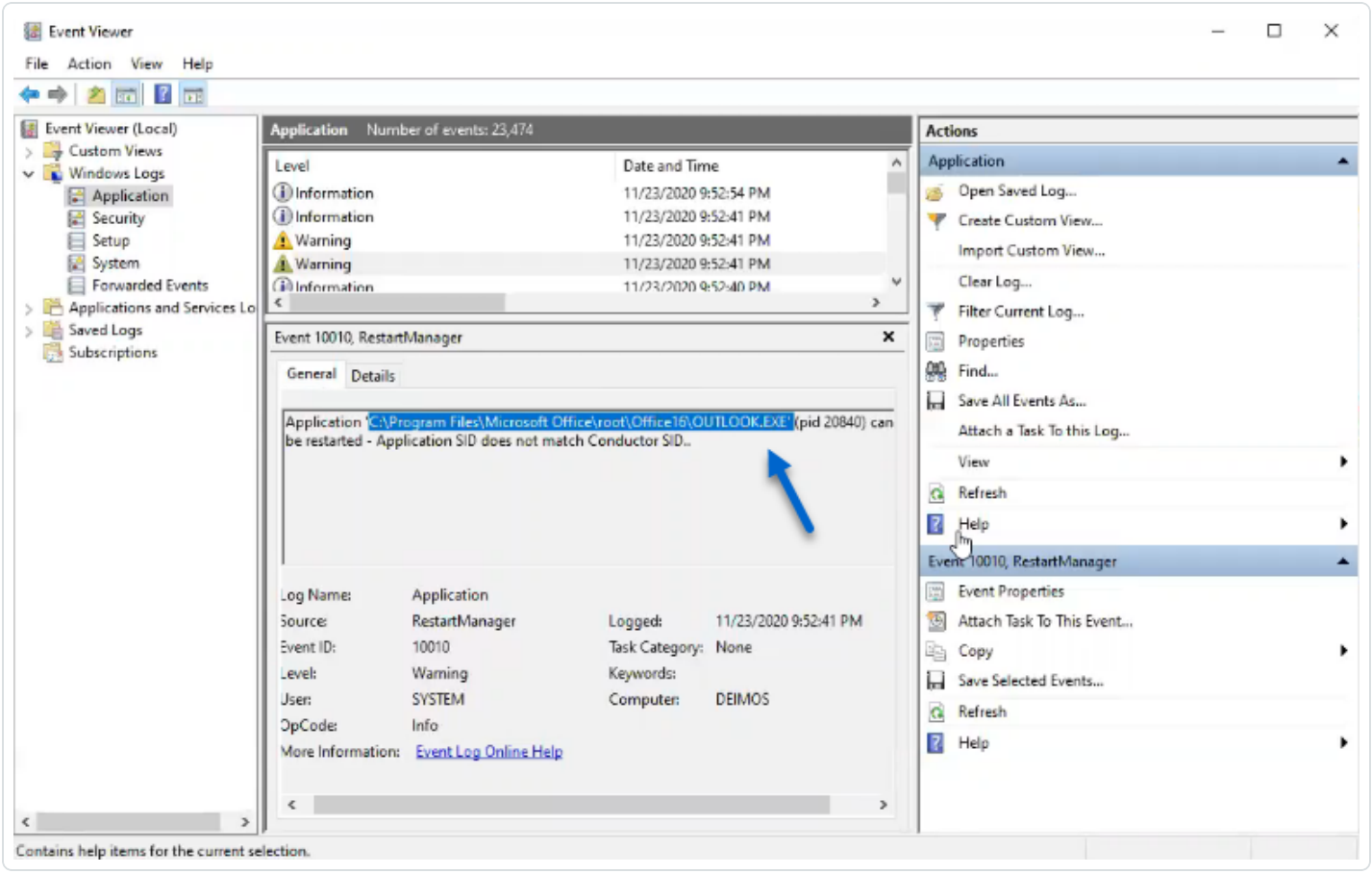
- 이 스크립트는 시스템 메모리에 이벤트 감시자와 WMI(Windows Management Instrumentation) 생산자/소비자를 구성합니다. WMI는 로컬 또는 원격 컴퓨터 시스템의 상태에 관한 정보를 제공하는 Windows 구성 요소입니다.
- 이벤트 감시자는 이벤트 로그를 수신하고 Sysvol이라는 네트워크 공유에 저장된 파일로 플러시하기 전에 이벤트 로그를 주기적으로 버퍼링합니다. 각 DC는 수집된 이벤트를 저장하는 Sysvol 파일 하나에 플러시하고 다른 도메인 컨트롤러에 복제합니다.
- WMI 소비자는 DC가 다시 시작되면 이벤트 감시자를 다시 등록하여 이 메커니즘을 지속합니다. DC가 다시 시작될 때마다 생산자가 다시 작동하여 소비자에게 이를 알립니다. 결과적으로 소비자가 이벤트 감시자를 다시 등록합니다.
- 이 시점에 분산 파일 시스템 또는 DFS 복제가 발생하며 여러 도메인 컨트롤러 간에 파일을 자동으로 동기화합니다. Tenable Identity Exposure의 플랫폼은 유입되는 DFS 복제 트래픽을 수신 대기하고 이 데이터를 사용하여 이벤트를 수집하고 보안 분석을 실행한 다음 IoA 알림을 생성합니다.

로컬 데이터 가져오기

Windows 이벤트 로그는 운영 체제와 애플리케이션에서 발생하는 모든 이벤트를 기록합니다. ETW(Event Tracing for Windows)라는 이벤트 로그는 Windows에 통합된 구성 요소 프레임워크에 의존합니다. ETW는 커널에 있으며 DC에 로컬로 저장되고 AD 프로토콜이 복제하지 않은 데이터를 생산합니다.

Tenable Identity Exposure에서는 WMI 엔진을 사용하여 유용한 ETW 데이터 세그먼트만, 이벤트 로그에서 추출하는 삽입 문자열 형식으로 수집합니다. Tenable Identity Exposure에서는 이러한 삽입 문자열을 Sysvol 폴더에 저장된 파일에 쓰고 DFS 엔진을 통해 복제합니다. 이렇게 하면 Tenable

Identity Exposure에서 ETW로부터 보안 분석을 실행하고 공격을 감지하는 데 적절한 양의 데이터만 수집할 수 있습니다.



IoA 스크립트 요약

다음 표는 Tenable Identity Exposure 스크립트 배포에 관한 개요입니다.

단계	설명	관련된 구성 요소	기술적 조치
1	Tenable Identity Exposure의 IoA 배포 등	GPO 관리	`Tenable.ad`(기본 이름) GPO를 만들고 도메인 컨트롤러 OU에 연결합니다.

	록		
2	DC에서 Tenable Identity Exposure의 IoA 배포 시작	DC 로컬 시스템	AD 복제 및 그룹 정책 새로 고침 간격에 따라 각 DC가 적용할 새 GPO를 탐지합니다.
3	이벤트 감시자 및 WMI 생산자/소비자 등록	DC 로컬 시스템	시스템이 즉시 실행 작업을 등록하여 실행합니다. 이 작업이 PowerShell 프로세스를 실행하여 `ManagementEventWatcher` 및 `ActiveScriptEventConsumer` 클래스의 인스턴스를 만듭니다. Tenable Identity Exposure에서 이러한 개체를 사용해 ETW 메시지를 수신하고 저장합니다.
4	고급 로깅 정책 상태 제어	DC 로컬 시스템	시스템이 레지스트리 키 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`를 설정하여 고급 로깅 정책을 활성화합니다.
5	로컬 로깅 정책 업데이트	DC 로컬 시스템	탐지하려는 IoA에 따라 Tenable Identity Exposure에서는 고급 로깅 정책을 동적으로 생성하고 활성화합니다. 이 정책은 기존 로깅 정책을 비활성화하지 않으며 필요한 경우 보강하기만 합니다. 충돌이 탐지되면 GPO 설치 스크립트가 중단되고 "Tenable Identity Exposure에 감사 정책이 필요 '...' 하지만 현재 AD 구성이 그 사용을 방지합니다."와 같은 메시지가 표시됩니다.
6	ETW 메시지 수집	DC 로컬 시스템	Tenable Identity Exposure에서 관련 ETW 메시지를 캡처하고 주기적으로 버퍼링한 다음 Tenable Identity ExposureGPO(`...{GPO_GUID}\Machine\IOA<DC_name>`)에 연결된 Sysvol 폴더에 저장된 파일(DC당 한 개)에 저장합니다.
7	Tenable Identity Exposu	Active Directory	AD는 DFS를 사용해 도메인 전체에 파일을 복제합니다. Tenable Identity Exposure 플랫폼은 파일도 수신합니다.

	re 플랫폼에 파일 복제		
8	이러한 파일 덮어쓰기	Active Directory	각각의 DC가 같은 파일에서 주기적으로 버퍼링된 이벤트를 자동으로 지속적으로 씁니다.

참고 항목

- Indicators of Attack and the Active Directory
- 공격 지표 설치
- 기술 변경 사항 및 잠재적 영향

기술 변경 사항 및 잠재적 영향

공격 지표(IoA) 모듈의 설치 스크립트를 실행하면 GPO를 만들어 모니터링되는 DC에 다음과 같은 변경 사항을 투명하게 적용합니다.

- 기본 이름이 "Tenable.ad"인 새 GPO가 기본적으로 도메인 컨트롤러의 조직 단위(OU)에 연결됩니다.
- Microsoft 고급 로깅 정책을 활성화하기 위한 레지스트리 키 수정.
- 새 이벤트 로그 정책을 활성화하여 IoA에 필요한 ETW 정보를 생성하도록 도메인 컨트롤러를 적용.

  참고: 이벤트 로그 정책은 ETW 엔진이 Tenable Identity Exposure에 필요한 삽입 문자열을 생성하려면 필수입니다. 이 정책은 기존 로깅 정책을 사용 중지하지 않고 정책에 추가합니다. 충돌이 있는 경우, 배포 스크립트가 중단되고 오류 메시지가 표시됩니다.

- Tenable Identity Exposure 서비스 계정에 쓰기 권한을 추가하여 GPO 폴더에 저장된 IoA 구성의 "자동 업데이트"를 허용합니다.

한계 및 잠재적 영향

공격 지표(IoA) 모듈에는 다음과 같은 한계가 있을 수 있습니다.

- IoA 모듈은 ETW 데이터를 사용하고 Microsoft가 정의한 제한 내에서 작동합니다.
- 설치된 GPO는 전체 도메인에 복제되어야 하며 설치 프로세스가 완료되려면 GPO 새로 고침 간격이 경과해야 합니다. Tenable Identity Exposure에서 즉시 공격 지표 엔진에서 검사를 시작하지 않아 이 효과를 최소화하더라도, 이 복제 기간에는 오탐과 미탐이 발생할 수 있습니다.
- Tenable은 SYSVOL 파일 공유를 사용하여 도메인 컨트롤러에서 ETW 정보를 검색합니다. SYSVOL이 도메인 내 모든 도메인 컨트롤러에 복제되므로, Active Directory 활동량이 가장 많을 때 복제 활동이 크게 증가합니다.
- 여러 도메인 컨트롤러와 Tenable Identity Exposure 사이에서 파일을 복제할 경우 일부 네트워크 대역폭도 사용됩니다. Tenable Identity Exposure에서는 수집하는 파일을 자동으로 제거하여 이러한 영향을 조절하고 이러한 파일의 크기도 제한합니다(기본적으로 최대 500MB).
- 분산 파일 시스템(DFS) 복제가 느리거나 끊긴 것으로 인한 문제입니다. 자세한 내용은 DFS 복제 문제 완화을 참조하십시오.

참고 항목

- Indicators of Attack and the Active Directory
- 공격 지표 설치
- 공격 지표 설치 스크립트
- 공격 지표 문제 해결

공격 시나리오(< v. 3.36)

주의: 공격 지표에 대한 이 구성 업데이트 기능은 3.36 이후 Tenable Identity Exposure 버전에는 더 이상 적용되지 않습니다.

필수 사용자 역할: 공격 지표 구성을 수정할 권한이 있는 조직 사용자.

공격 시나리오를 정의하려면 특정 도메인에서 Tenable Identity Exposure에서 모니터링할 공격 유형을 선택해야 합니다.

시작하기 전에

공격 시나리오를 수정하려면 다음과 같은 권한이 있는 사용자 역할이 있어야 합니다.

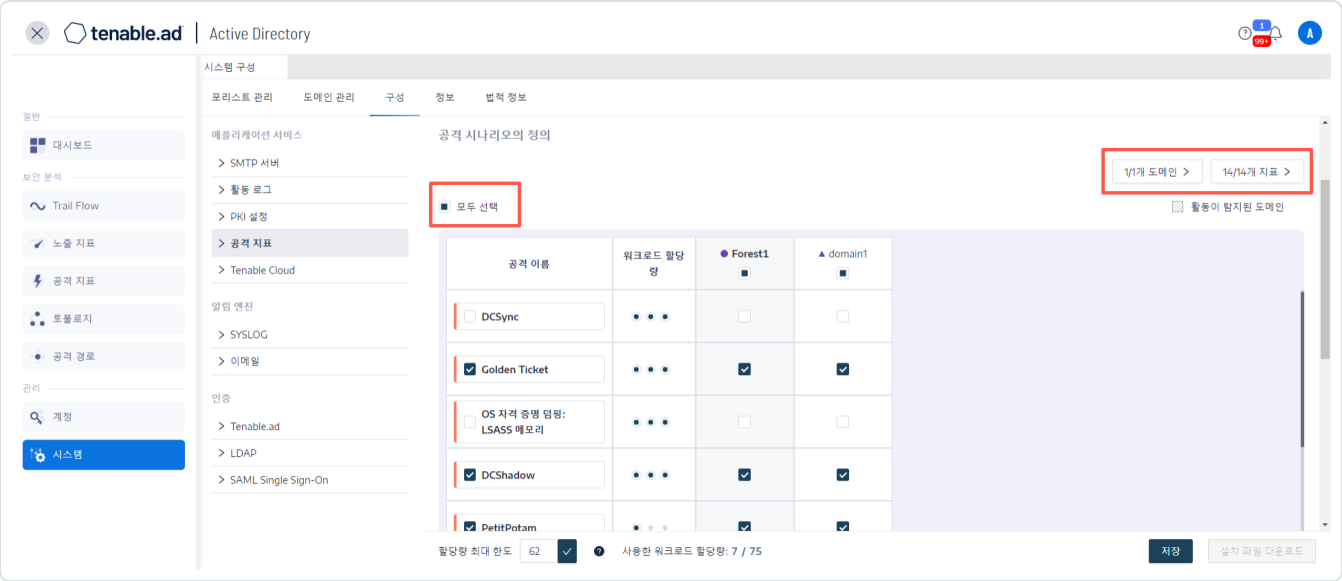
- **데이터 엔터티**에서 다음에 대한 "읽기" 액세스:
  - 모든 공격 지표
  - 모든 도메인
- **인터페이스 엔터티**에서 다음에 대한 액세스:
  - 관리 > 시스템 > 구성
  - 관리 > 시스템 > 구성 > 애플리케이션 서비스 > 공격 지표
  - 관리 > 시스템 > 구성 > 애플리케이션 서비스 > 공격 지표 > 설치 파일 다운로드

역할 기반 권한에 관한 자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

공격 시나리오를 정의하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **공격 지표**를 클릭합니다.

   공격 지표의 정의 창이 열립니다.

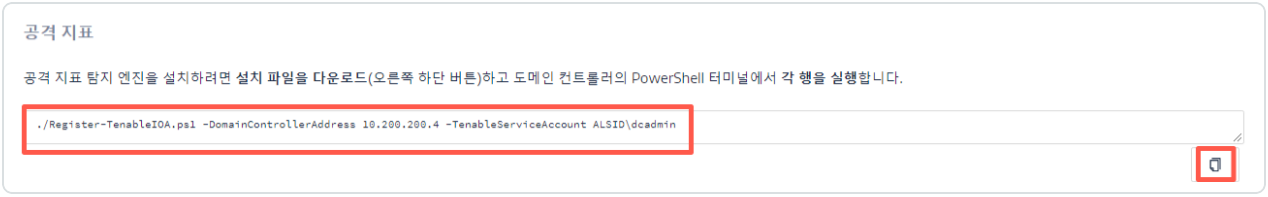


2. **공격 이름** 아래에서 모니터링하려는 공격을 선택합니다.
3. 선택한 공격을 모니터링하려는 도메인을 선택합니다.
4. 원하는 경우, 다음 중 하나를 수행할 수 있습니다.
    - **모두 선택**을 클릭하여 모든 도메인에서 모든 공격을 모니터링합니다.
    - **n/n 도메인** 또는 **n/n 지표**를 클릭하여 특정 공격을 모니터링할 특정 도메일을 필터링합니다.
5. **저장**을 클릭합니다.

    구성을 저장한 후에 확인 메시지가 표시되어 Tenable Identity Exposure에서 각 공격의 활동 상태를 지우는 것을 알려줍니다.
6. **확인**을 클릭합니다.

    메시지가 표시되어 Tenable Identity Exposure에서 공격 지표 구성을 업데이트했다고 확인합니다.
7. **설치 파일 다운로드**를 클릭합니다.
8. 새 공격 구성을 적용하려면 설치 파일을 실행합니다.
    a. 다운로드한 설치 파일을 모니터링하는 도메인의 DC에 복사하여 붙여 넣습니다.
    b. 관리자 권한으로 PowerShell 터미널을 엽니다.

c. Tenable Identity Exposure에서 창 아래에 있는 공격 지표 섹션 아래의 명령을 복사합니다.



d. PowerShell 창에 명령을 붙여 넣어 스크립트를 실행합니다.

워크로드 할당량

주의: 워크로드 할당량 기능만은 3.36 이후 Tenable Identity Exposure 버전에는 더 이상 적용되지 않습니다.

필수 사용자 역할: 워크로드 할당량을 편집할 권한이 있는 조직 사용자.

Tenable Identity Exposure의 각 공격 지표에는 공격에서 입수한 데이터를 분석하는 데 필요한 리소스를 감안한 워크로드 할당량이 연결되어 있습니다.

Tenable Identity Exposure에서 워크로드 할당량을 계산하여 동시에 실행되는 공격 지표(IoA) 수를 제한합니다. 이것은 도메인 컨트롤러에 이벤트 생성에 대한 대역폭과 CPU 사용량에 영향을 미칩니다.

워크로드 할당량 제한을 수정한 후에 다음과 같은 작업을 수행하십시오.

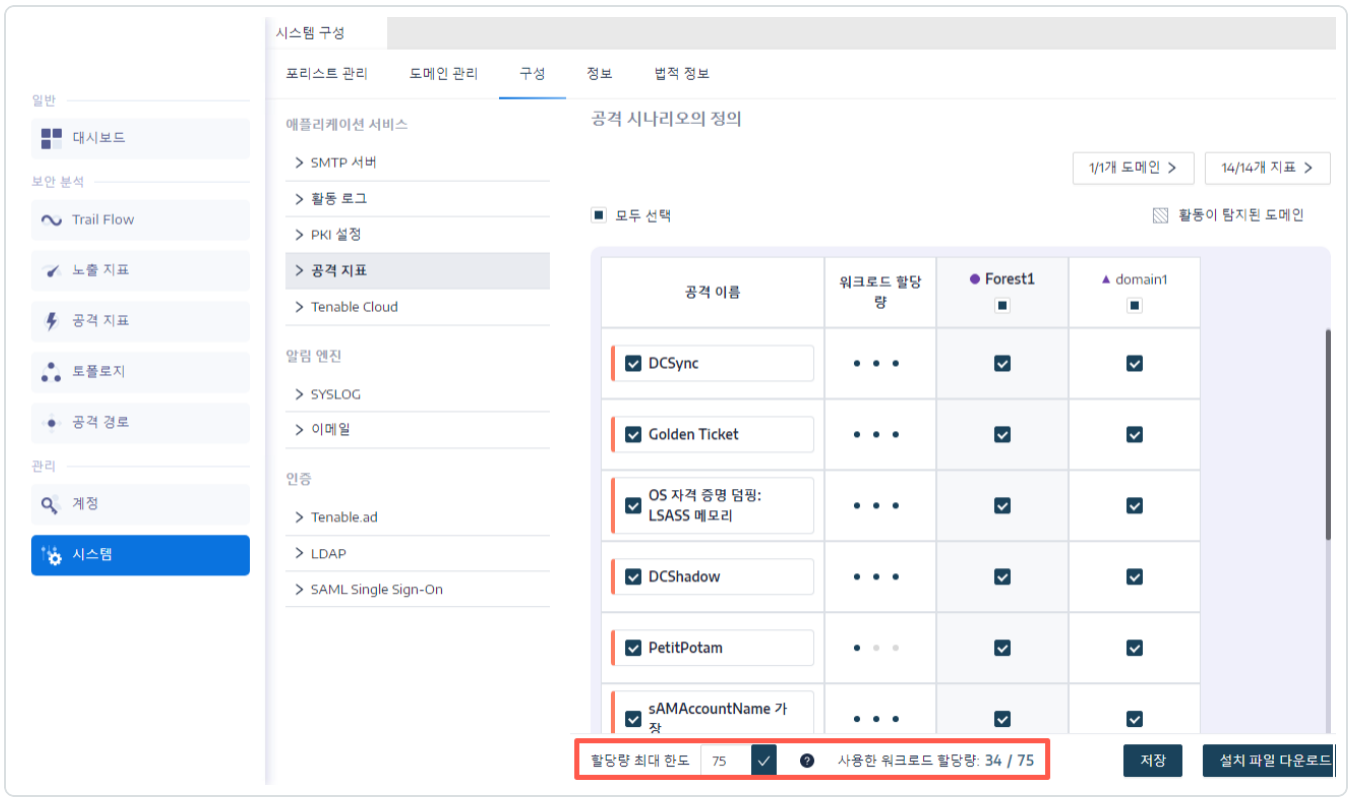
- 증가: 증가 이후의 통계를 모니터링하여 마진이 적절한지 확인합니다.
- 감소: 몇몇 IoA를 비활성화하여 이 할당량 미만을 유지하도록 합니다. 이렇게 하면 공격에 대한 보안 범위가 줄어듭니다.

워크로드 할당량 한도를 수정하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **공격 지표**를 클릭합니다.

   IoA 구성 창이 열립니다.

2. 구성하려는 IoA를 선택합니다.
3. **공격 지표** 아래의 **할당량 최대 한도** 상자에 워크로드 할당량 한도 값을 입력합니다.



4. 입력한 값 옆에 있는 체크 표시를 클릭합니다.

   메시지가 표시되어 이 수정 사항이 Tenable Identity Exposure에 어떤 영향을 미치는지 알려줍니다.

   > **참고**: 현재 공격 구성에 필요한 것보다 작은 할당량 최대 한도를 입력하는 경우, 활성 공격 지표의 수를 조정하거나 한도를 높여야 합니다.

5. **확인**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 할당량 최대 한도를 업데이트했음을 확인합니다.

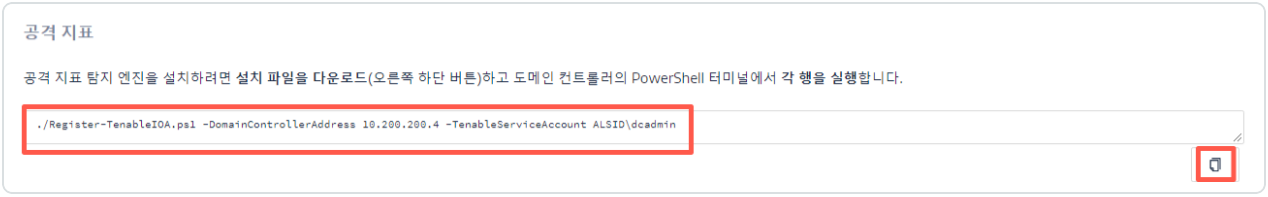
6. **저장**을 클릭합니다.

   구성을 저장한 후에 확인 메시지가 표시되어 Tenable Identity Exposure에서 각 공격의 활동 상태를 지우는 것을 알려줍니다.

7. **확인**을 클릭합니다.

메시지가 표시되어 Tenable Identity Exposure에서 공격 지표 구성을 업데이트했다고 확인합니다.

8. **설치 파일 다운로드**를 클릭합니다.
9. 새 공격 구성을 적용하려면 설치 파일을 실행합니다.
    a. 다운로드한 설치 파일을 모니터링하는 도메인의 DC에 복사하여 붙여 넣습니다.
    b. 관리자 권한으로 PowerShell 터미널을 엽니다.
    c. Tenable Identity Exposure에서 창 아래에 있는 공격 지표 섹션 아래의 명령을 복사합니다.



    d. PowerShell 창에 명령을 붙여 넣어 스크립트를 실행합니다.

Microsoft Sysmon 설치

일부 Tenable Identity Exposure의 공격 지표(IoA)를 활성화하려면 Microsoft 시스템 모니터(Sysmon) 서비스가 필요합니다.

Sysmon은 시스템 활동을 모니터링하고 Windows 이벤트 로그에 기록하여 ETW(Event Tracing for Windows) 인프라에 좀 더 보안 중심적인 정보를 제공합니다.

추가로 Windows 서비스와 드라이버를 설치하면 Active Directory 인프라를 호스팅하는 도메인 컨트롤러의 성능에 영향을 미칠 수 있기 때문입니다. Tenable은 Microsoft Sysmon을 자동으로 배포하지 않습니다. 수동으로 설치하거나 전용 GPO를 사용해야 합니다.

다음 IoA에는 Microsoft Sysmon이 필요합니다.

이름	이유
OS 자격 증명 덤핑: LSASS 메모리	프로세스 삽입 탐지

참고: Sysmon을 설치하기로 선택한 경우 필요한 모든 이벤트를 수집하려면 PDC만 아니라 모든 도메인 컨트롤러에 Sysmon을 설치해야 합니다.

참고: Sysmon 설치를 테스트하여 호환성 문제가 없는지 확인한 다음에 Tenable Identity Exposure를 완전히 배포해야 합니다.

팁: 설치 후에는 정기적으로 Sysmon을 업데이트해야 가능한 취약성을 해결하는 각종 패치를 활용할 수 있습니다. Tenable Identity Exposure와 호환되는 가장 오래된 버전은 Sysmon 12.0입니다.

Sysmon을 설치하는 방법:

1. Microsoft 웹 사이트에서 Sysmon을 다운로드합니다.
2. 명령줄 인터페이스에서 다음과 같은 명령을 실행하여 로컬 컴퓨터에 Microsoft Sysmon을 설치합니다.

```
.\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

참고: 구성 설명은 주석이 추가된 Sysmon 구성 파일을 참조하십시오.

3. 다음 명령을 실행하여 WMI 필터에 Sysmon이 설치되었음을 나타내는 레지스트리 키를 추가합니다.

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Sysmon을 제거하는 방법:

1. PowerShell 터미널을 엽니다.
2. `Sysmon64.exe`를 포함하는 폴더를 찾습니다.
3. 다음과 같은 명령을 입력합니다.

```
PS C:\> .\Sysmon64.exe -u
```

레지스트리 키를 삭제하는 방법:

- Sysmon을 실행 중인 모든 컴퓨터의 명령줄 인터페이스에 다음과 같은 명령을 입력합니다.

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Sysmon 구성 파일

참고:
- Sysmon 설정 파일을 XML 파일로 복사하여 저장한 후 사용하십시오. 오류가 발생하는 경우 여기에서 구성 파일을 직접 다운로드할 수도 있습니다.
- 파일 속성에서 파일을 차단 해제한 다음에 사용하십시오.

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
```

```
[FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>

    <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>

    <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </CreateRemoteThread>
    </RuleGroup>

    <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RawAccessRead>
    </RuleGroup>

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
        <ProcessAccess onmatch="include">
          <!-- Detect Access to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
```

```
            <GrantedAccess>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>

          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </ProcessAccess>
    </RuleGroup>

    <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
    <RuleGroup name="" groupRelation="or">
      <RegistryEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RegistryEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
```

```
    <RuleGroup name="" groupRelation="or">
      <FileCreateStreamHash onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateStreamHash>
    </RuleGroup>

    <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    <RuleGroup name="" groupRelation="or">
      <PipeEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </PipeEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
    <RuleGroup name="" groupRelation="or">
      <WmiEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </WmiEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
    <RuleGroup name="" groupRelation="or">
      <DnsQuery onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DnsQuery>
    </RuleGroup>

    <!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileDelete>
    </RuleGroup>

  </EventFiltering>
</Sysmon>
```

공격 지표 제거

필수 역할: 로컬 시스템의 관리자.

공격 지표(IoA) 모듈을 제거하려면 명령을 실행하여 Tenable Identity Exposure 정리라는 새 그룹 정책 개체(GPO)를 만듭니다.

제거 프로세스는 기본적으로 이 새 GPO를 사용하여 이전에 설치한 GPO와 그 SYSVOL 파일, 레지스트리 설정, 고급 로깅 정책과 WMI 필터를 정리합니다.

참고: 처음 GPO 이름을 변경한 경우, 제거 프로그램에서 어느 GPO를 제거해야 하는지 알 수 있도록 이름을 전달해야 합니다. 새 GPO 이름을 전달하려면 `-GpoDisplayName` 매개 변수를 사용하십시오.

IoA 모듈을 제거하는 방법:

1. 명령줄 인터페이스에서 다음과 같은 명령을 실행하여 IoA 모듈을 제거합니다.

   ```
   Register-TenableIOA.ps1 -Uninstall
   ```

2. 이 새 GPO를 도메인 전체에 복제합니다. 스크립트는 복제 완료를 위해 4시간의 지연을 적용합니다.

3. 다음과 같은 명령을 실행하여 정리 GPO를 삭제합니다.

   ```
   Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
   ```

4. 선택 사항: 다음과 같은 명령을 실행하여 GPO가 더 이상 존재하지 않는지 확인합니다.

   ```
   (Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}
   | Select Displayname| measure
   ```

공격 지표 문제 해결

- 고급 감사 정책 구성 우선 순위
- 바이러스 백신 탐지
- Tenable Identity Exposure 로그 파일
- 이벤트 로그 수신기 유효성 검사
- DFS 복제 문제 완화

바이러스 백신 탐지

Tenable과 Microsoft는 도메인 컨트롤러에 바이러스 백신, 엔드포인트 보호 플랫폼(EPP) 또는 엔드포인트 탐지 및 대응(EDR) 소프트웨어(또는 중앙 관리 콘솔이 있는 기타 모든 도구) 설치를 권장하지 않습니다. 설치하기로 선택하는 경우, 바이러스 백신/EPP/EDR이 도메인 컨트롤러에서 공격 지표(IoA) 이벤트를 수집하는 데 필요한 항목을 탐지하고 심하면 차단하거나 삭제할 수도 있습니다.

Tenable Identity Exposure의 공격 지표 배포 스크립트는 악성 코드를 포함하지 않으며 난독 처리도 하지 않습니다. 하지만 PowerShell과 WMI를 사용하기도 하며 구현의 에이전트리스 특성으로 인해 때때로 탐지되는 것은 정상입니다.

다음과 같은 문제가 발생하는 경우:

- 설치 중 오류 메시지
- 탐지 중에 오탐 또는 미탐

설치 스크립트 바이러스 백신 탐지 문제 해결하는 방법:

1. 바이러스 백신/EPP/EDR 보안 로그를 검토하여 Tenable Identity Exposure 구성 요소 탐지, 차단 또는 삭제 기록이 있는지 확인합니다. 바이러스 백신/EPP/EDR은 다음과 같은 구성 요소에 영향을 줄 수 있습니다.
    - 도메인 컨트롤러에 적용된 Tenable Identity Exposure GPO의 `ScheduledTasks.xml` 파일.
    - PowerShell.exe를 실행하는 도메인 컨트롤러의 Tenable Identity Exposure 예약 작업.
    - 도메인 컨트롤러에서 시작된 Tenable Identity Exposure `Register-TenableADEventsListener.exe` 프로세스.
2. 도구에 이러한 영향을 받는 구성 요소에 대하여 보안 예외 사항을 추가합니다.
    - 특히 Symantec 엔드포인트 보호의 경우 IoA 설치 프로세스 중에 `CL.Downloader!gen27` 탐지를 보고할 수 있습니다. 이 알려진 위험을 예외 정책에 추가할 수 있습니다.
    - 작업 스케줄러를 설정했으면 PowerShell을 실행하여 `Register-TenableADEventsListener.exe` 프로세스를 시작합니다. 바이러스 백신/EPP/EDR 소프트웨어가 이 PowerShell 스크립트를 방해하여 공격 지표가 적절히 실행되지 못하게 할 수 있습니다. 이 프로세스를 긴밀히 추적하고 모든 모니터링 대상 도메인 컨트롤러에서

한 번만 실행되도록 하십시오.

바이러스 백신/EPP/EDR 파일 경로 제외의 예:

```
Register-TenableADEventsListener.exe process
 "\\"domain"\sysvol\"domain"\Policies\{"GUID_Tenable.ad}\Machine\IOA\Register-
TenableADEventsListener.exe"
```

```
ScheduledTasks.xml file
    C:\Users\<User Name>\AppData\Local\Temp\4\Tenable.ad\
{GUID}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    C:\Windows\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    \\[DOMAIN.FQDN]\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
```

고급 감사 정책 구성 우선 순위

Tenable Identity Exposure에서 필수 이벤트 로깅을 사용하기 위해 만드는 그룹 정책 개체(GPO)는 적용 모드를 사용으로 설정하여 조직 단위(OU) 도메인 컨트롤러에 연결됩니다.

이렇게 하면 해당 GPO에 높은 우선 순위를 부여하지만, 더 높은 수준(예: 도메인 또는 사이트)에서 구성되어 적용된 GPO가 있으면 이보다 높은 우선 순위를 차지하게 됩니다.

고급 감사 정책 구성 설정을 정의하며 우선 순위가 더 높은 GPO가 Tenable Identity Exposure의 요구 사항과 충돌하는 경우, 이것이 우선 순위를 차지하며 Tenable Identity Exposure에서는 공격 탐지에 필요한 이벤트를 놓칩니다.

Windows는 GPO가 정의한 고급 감사 정책 구성 설정을 병합하기 때문에, 여러 GPO가 각기 다른 설정을 정의할 수 있습니다.

그러나 각 설정 수준에서는 우선 순위가 더 높은 GPO 정의 값만 사용합니다. 예를 들어 Tenable Identity Exposure에는 감사 자격 증명 유효성 검사 설정에 대해 성공 및 실패 값이 필요합니다. 그러나 우선 순위가 더 높은 GPO가 감사 자격 증명 유효성 검사에 성공만 정의하는 경우, Windows는 성공 이벤트만 수집하며 Tenable Identity Exposure에서는 필수적인 실패 이벤트를 놓치게 됩니다.

GPO 우선 순위를 검사하는 방법:

1. 도메인 컨트롤러의 명령줄 인터페이스에서 다음과 같은 명령을 실행합니다.

   이것은 모든 GPO와 우선 순위를 고려한 다음 효과적인 고급 감사 정책 구성을 출력합니다.

   ```
   auditpol.exe /get /category:*
   ```

2. 이 출력을 Tenable Identity Exposure 고급 감사 정책 요구 사항과 비교합니다. Tenable Identity Exposure에 필요한 각 설정에 대하여, 이 효과적인 정책이 이 설정에도 적용되는지 확인합니다.

   - 효과적인 정책이 더 철저한 경우에는 문제가 되지 않습니다. 예를 들어 Tenable Identity Exposure에 "성공" 또는 "실패"가 필요하고, 설정은 "성공과 실패"인 경우가 이에 해당합니다.
   - 효과적인 정책이 충분하지 않은 경우, 우선 순위가 더 높은 GPO가 상충하는 설정을 정의한다는 의미입니다.

GPO 우선 순위를 수정하는 방법:

1. 고급 감사 정책 구성을 정의하는 "적용됨" 모드에서 더 높은 수준(도메인 또는 사이트)에 연결된 GPO를 찾습니다.
2. 명령줄 인터페이스에서, 도메인 컨트롤러에서 다음과 같은 명령을 실행하여 최우선 GPO를 정확히 찾습니다.

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. GPO에서 상응하는 고급 감사 정책 구성 설정을 Tenable Identity Exposure의 최소 요구 사항에 맞춰 수정합니다. 예:
   - Tenable Identity Exposure에 "성공"이 필요하고 우선 순위가 더 높은 GPO에서는 "실패"가 정의된 경우, 설정을 "성공 및 실패"로 수정합니다.
   - Tenable Identity Exposure에 "성공 및 실패"가 필요하고 우선 순위가 더 높은 GPO에서는 "성공"이 정의된 경우, 설정을 "성공 및 실패"로 수정합니다.
4. 설정을 수정한 뒤에는 업데이트된 GPO가 적용될 때까지 기다리거나 `gpupdate` 명령을 사용해 강제 적용할 수 있습니다.
5. GPO 우선 순위를 검사하는 방법: 절차를 반복하여 새로운 효과적인 정책을 확인합니다.

이벤트 로그 수신기 유효성 검사

공격 지표 설치 스크립트가 시스템의 메모리에 이벤트 감시자와 WMI(Windows Management Instrumentation) 생산자/소비자를 구성합니다. WMI는 로컬 또는 원격 컴퓨터 시스템의 상태에 관한 정보를 제공하는 Windows 구성 요소입니다.

WMI 등록이 올바른지 검사하는 방법:

- PowerShell에서 다음의 명령을 실행합니다.

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- 소비자가 하나 이상 있는 경우, 이런 유형의 출력을 얻게 됩니다.

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter
"Filter = ""__EventFilter.name='AlsidForAD-Launcher'"""


__GENUS                 : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS            : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : __
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsidForAD-Launcher\"",F
                          ilter="__EventFilter.Name=\"AlsidForAD-Launcher\""
__PROPERTY_COUNT        : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER                : DC-999
__NAMESPACE             : ROOT\subscription
__PATH                  : \\DC-999\ROOT\subscription:__
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
                          =\"AlsidForAD-Launcher\"",Filter="__EventFilter.Name=\"AlsidForAD-
Launcher\""
Consumer                : ActiveScriptEventConsumer.Name="AlsidForAD-Launcher"
CreatorSID              : {1, 1, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             :
Filter                  : __EventFilter.Name="AlsidForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders       : False
PSComputerName          : DC-999
```

  - 등록된 WMI 소비자가 없는 경우, 명령이 아무것도 반환하지 않습니다.
  - 이것은 WMI에 대하여 DC에서 프로세스를 실행하기 위한 전제 조건입니다.

WMI 프로세스를 검색하는 방법(3.19 버전 이하):

- PowerShell에서 다음의 명령을 실행합니다.

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- 유효한 결과의 예:

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}

ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472
```

이벤트 로그 수신기를 검색하는 방법(3.29 버전 이상):

- PowerShell에서 다음의 명령을 실행합니다.

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- 유효한 결과의 예:

```
PS C:\IOAInstall> gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}

ProcessId Name                                HandleCount WorkingSetSize VirtualSize

5748      Register-TenableADEventsListener.exe 152         4096000        4384534528
```

Tenable Identity Exposure 로그 파일

GPO와 WMI 사용자의 유효성을 검사한 뒤에도 여전히 공격 지표 알림이 표시되지 않는 경우, Tenable Identity Exposure의 내부 로그를 검토할 수 있습니다.

Ceti 로그

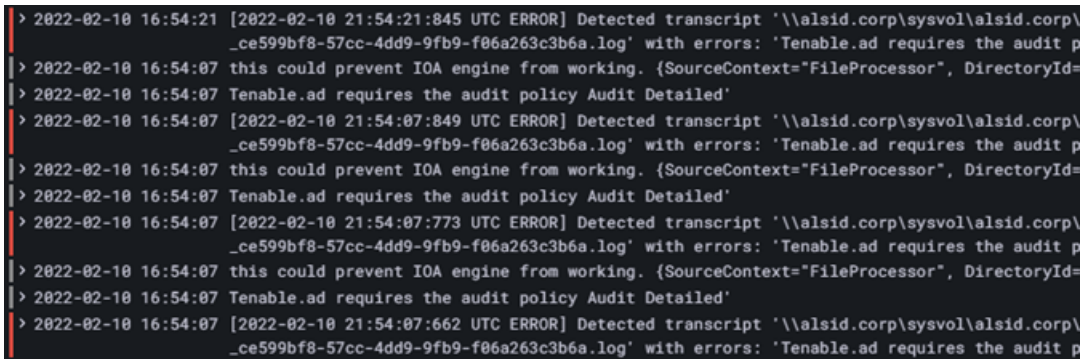
- CETI 로그에 다음과 같은 오류 메시지가 있는지 확인합니다.

```
[2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA
events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper",
DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
```

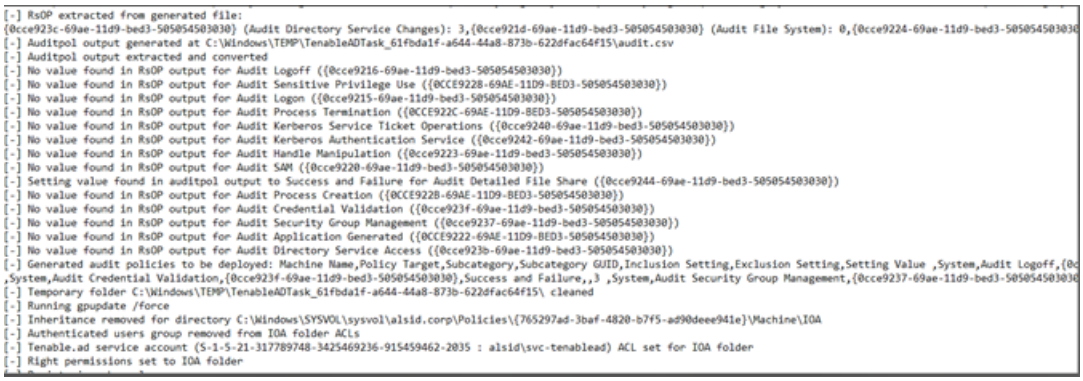
- 이 메시지가 표시되는 경우, GPO 설정과 WMI 사용자가 위의 오류 메시지에 목록으로 기재된 도메인 컨트롤러(DC)에서 실행 중인지 확인합니다.

감사 설정

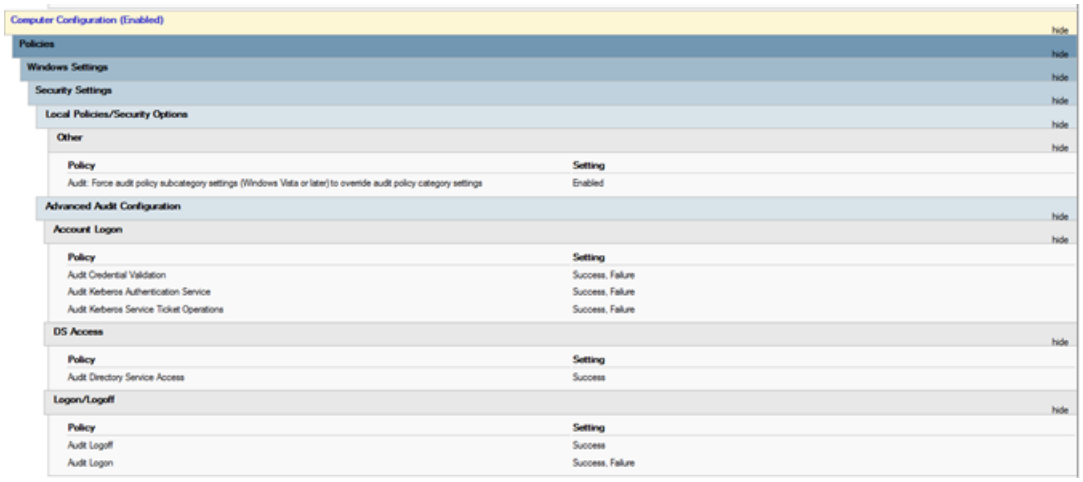
- "Tenable Identity Exposure에 감사 정책 필요..."와 비슷한 오류가 표시되는 경우, 기존 GPO를 확인하여 필수 감사 정책을 "감사 안 함"으로 설정한 것이 아닌지 확인합니다.



- "RSOP..."라고 명시된 오류가 발생하는 경우:



- 감사 정책을 확인하고 Sysvol 폴더의 기록 파일을 찾아 설치 중에 문제가 발생했는지 확인합니다.



Cygni 로그

Cygni는 공격을 기록하고 Tenable Identity Exposure에서 알림을 생성하기 위해 호출한 `.gz` 파일을 목록으로 표시합니다.

I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-GoldenTicket

```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-
GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket",
ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ProcessInjectionLsass

```
022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-
ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-
ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-DCShadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for
Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce",
ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-
AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for
Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-
PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-PetitPotam

```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Cephei 로그

다음 로그 항목은 Cephei가 공격을 쓰는 것을 확인합니다. 키 값은 **attackTypeID**이며 이것이 Cygni 항목과 상관관계를 정립하는 데 사용할 수 있는 공격 유형을 지정합니다.

I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
```

```
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-GoldenTicket attackTypeID:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ProcessInjectionLsass attackTypeID:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-DCShadow attackTypeID:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-BruteForce attackTypeID:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PasswordSpraying attackTypeID:6

```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PetitPotam attackTypeID:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ReconAdminsEnum attackTypeID:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-Kerberoasting attackTypeID:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-NtdsExtraction attackTypeID:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

Electra 로그

다음과 같은 항목이 표시될 것입니다.

[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)

```
[2022-03-15T14:04:39.151Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-
alert (namespace=electra)
[2022-03-15T14:04:39.168Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners.
alertIoA (namespace=electra)
```

Eridanis 로그

다음과 같은 항목이 표시될 것입니다.

```
022-03-15T14:04:39.150Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200
122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation
success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200
122 - 6ms (namespace=hapi)
```

DFS 복제 문제 완화

공격 지표 배포 스크립트에 있는 추가적인 매개 변수인 `-EventLogsFileWriteFrequency X`를 사용하면 분산 파일 시스템(DFS) 복제가 느려지거나 끊기는 등 발생 가능한 잠재적인 문제를 해결할 수 있습니다.

이 매개 변수는 선택 사항이며 Tenable에서는 DFS 복제 문제가 발생했거나 IoA 스크립트 배포 이후 이것이 발견된 경우에만 사용하도록 권장합니다. 일반적인 상황에서는 이 매개 변수가 기본값으로 유지되며 스크립트를 실행할 때 명령줄에 포함하지 않아도 됩니다.

매개 변수를 수정해야 하는 경우

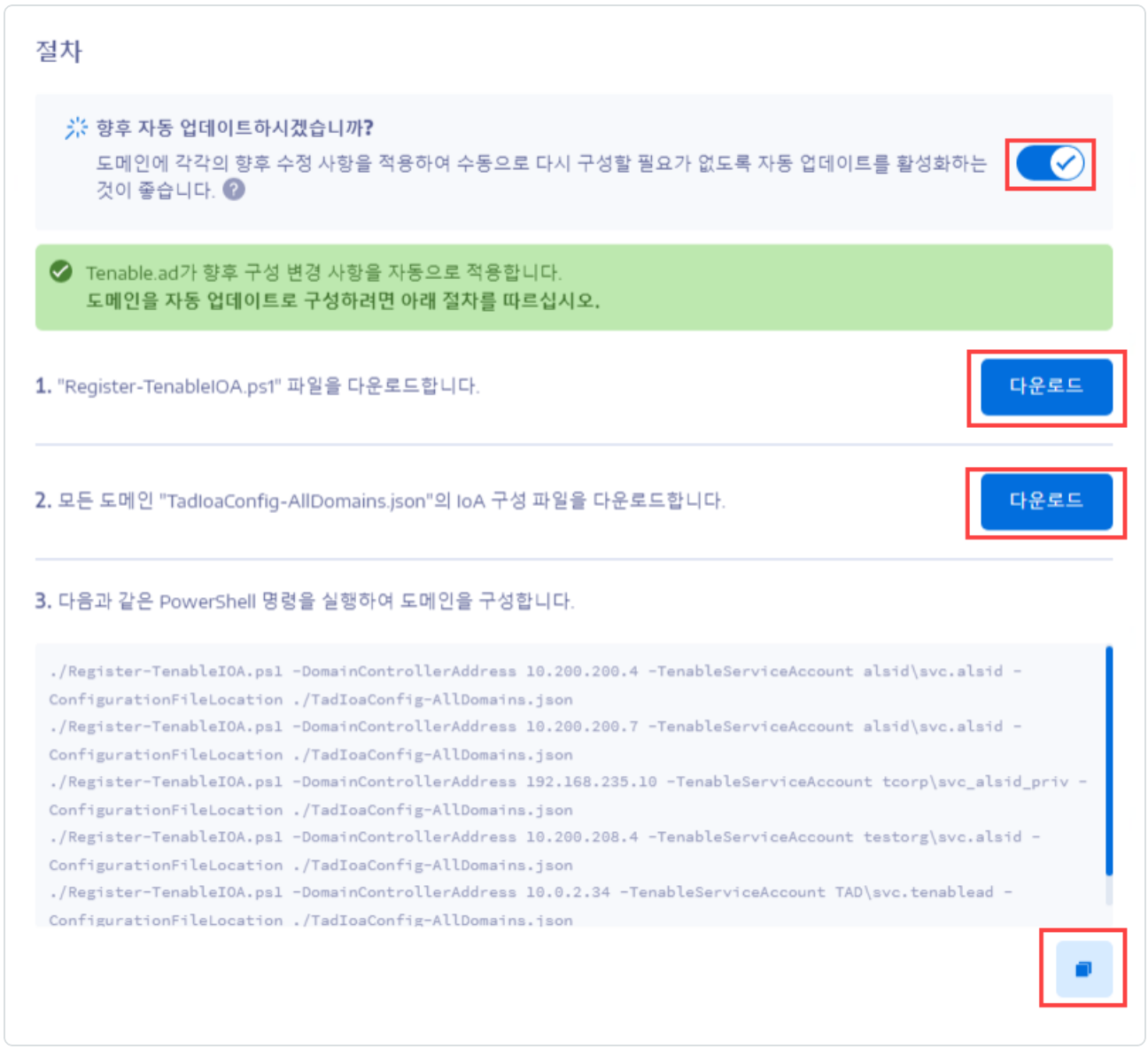
매개 변수 `-EventLogsFileWriteFrequency X`의 값 [X]는 Tenable Identity Exposure 수신기가 PDCe가 아닌 도메인 컨트롤러(DC)에서 이벤트 로그 파일을 생성하는 빈도입니다. Tenable Identity Exposure 수신기가 사용하는 기본값이며 권장하는 값은 15초입니다. 그러나 사용자 지정 값은 PDCe DC에는 적용되지 않으며 기본값인 15초로 유지되어 공격 탐지 기능의 온전한 작동을 보장합니다. Tenable에서는 이 매개 변수를 사용하고 이 값을 기본값인 15초를 넘어 최고 300초(5분)까지 늘리는 것은 인프라에 DFS 복제 문제가 발생했거나 그러한 문제가 발생할 가능성이 큰 경우만으로 한정할 것을 권장합니다.

권장 사항

이벤트 로그 파일 쓰기 빈도를 높이면 파일이 덜 자주 생성되므로, 공격 탐지 지연이 늘어나게 됩니다(예를 들어 파일을 PDCe가 아닌 DC에서 기본값인 15초 대신 30초 마다 생성하는 경우). 또한 지연을 늘리면 기술 변경 사항 및 잠재적 영향에 정의된 설정 한도 내에서 생성된 이벤트 로그 파일의 크기가 늘어납니다. 따라서, 이 매개 변수는 완화 전략으로만 사용해야 하며 DFS 복제 문제에 대한 적절한 조사를 대신할 수는 없습니다.

매개 변수를 적용하는 방법:

1. 절차에 설명된 대로 IoA의 도메인을 구성합니다. 자세한 내용은 공격 지표 설치을 참조하십시오.



2. 관리자 권한으로 PowerShell 터미널을 엽니다.
3. 스크립트를 실행하여 IoA에 대한 도메인 컨트롤러를 구성하고 - `EventLogsFileWriteFrequency X` 매개 변수를 추가합니다. 여기에서 [X]는 이벤트 로그 파일 빈도로 설정하고자 하는 빈도입니다.

인증

Tenable Identity Exposure 사용자를 인증하는 여러 방법이 있습니다.

- Tenable Identity Exposure 계정을 사용한 인증
- LDAP를 사용하여 인증
- SAML을 사용한 인증

Tenable One을 사용한 인증

필요한 라이선스: Tenable One

참고: Tenable One 라이선스를 사용하는 경우, 모든 인증 설정을 Tenable Vulnerability Management에서 관리합니다. 자세한 내용은 *Tenable Vulnerability Management 사용자 가이드*의 액세스 제어를 참조하십시오.

Tenable One을 사용하여 인증을 구성하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 클릭합니다.

   구성 창이 표시됩니다.

2. **인증** 섹션 아래에서 **Tenable One**을 클릭합니다.

3. **기본 프로필** 드롭다운 상자에서 해당 사용자의 프로필을 선택합니다.

4. **기본 역할** 상자에서 해당 사용자의 역할을 선택합니다.

   팁: 이전에 Tenable Identity Exposure에 연결한 적이 없는 Tenable One의 인증된 사용자는 Tenable Identity Exposure에 로그인하면 자동으로 계정이 생깁니다. 기본적으로 사용자에게 기본 프로필 및 기본 역할이 적용됩니다. **예외**: Tenable Vulnerability Management에서 "관리자" 역할을 가진 사용자는 Tenable Identity Exposure에서 "전역 관리자" 역할도 갖게 됩니다.

5. **저장**을 클릭합니다.

Tenable Identity Exposure 계정을 사용한 인증

가장 간단한 인증 방법은 사용자 이름과 비밀번호가 필요한 Tenable Identity Exposure 계정을 통한 인증입니다.

이 인증 방법은 기본 잠금 정책, 인증 메커니즘에 대한 무차별 대입 공격을 완화하도록 고안된 보안 제어를 제공합니다. 이 방법은 로그인 시도에 너무 많이 실패하면 사용자 계정을 잠급니다. 계정이 잠기면 사용자는 Tenable Identity Exposure API에 액세스할 수 없습니다

Tenable Identity Exposure 계정을 사용해 인증을 구성하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 클릭합니다.

   구성 창이 표시됩니다.

2. **인증** 섹션 아래에서 **Tenable Identity Exposure**를 클릭합니다.
3. **기본 프로필** 드롭다운 상자에서 해당 사용자의 프로필을 선택합니다.
4. **기본 역할** 상자에서 해당 사용자의 역할을 선택합니다.

5. 잠금 정책 설정 구성:

설정	설명	기본값
사용	• **사용** - 로그인 시도가 정해진 횟수만큼 실패하고 나면 Tenable Identity Exposure에서 해당 계정을 잠급니다. • **사용 안 함** - 로그인 시도가 실패한 뒤에도 Tenable Identity Exposure에서 해당 계정을 잠그지 않습니다.	사용
잠금 기간	Tenable Identity Exposure에서 계정의 로그인 시도를 잠그는 기간입니다. Tenable Identity Exposure에서는 이 시간이 지나면 계정을 자동으로 잠금 해제하여 사용자가 다시 로그인을 시도할 수 있게 합니다. 잠금 기간을 구성하는 방법: 1. 슬라이더를 클릭하여 잠금 기간을 설정합니다. 2. 정해진 기간이 지난 뒤에 계정을 자동으로 잠금 해제하지 않으려면 **무한**을 선택합니다. **참고**: '전역 관리자' 그룹 내 모든 계정이 잠기면 Tenable Identity Exposure에서 10초 후 기본 관리자 계정을 잠금 해제합니다.	300초
잠금까지 로그인 시도 횟수	Tenable Identity Exposure에서 계정을 잠그기까지 실패한 로그인 시도 횟수입니다.	3
만회 기간	Tenable Identity Exposure에서 실패한 로그인 시도 횟수를 세는 시간 간격입니다. 정해진 횟수만큼 로그인 시도가 실패하면 Tenable Identity Exposure에서 계정을 잠급니다. 만회 기간을 설정하는 방법: 1. 슬라이더를 클릭하여 시간 간격을 설정합니다.	900초

	2. Tenable Identity Exposure에서 계정을 잠그기 전에 실패한 로그인 시도 횟수를 셀 시간 간격을 설정하지 않으려면, "무한"을 선택합니다.	

6. **저장**을 클릭합니다.

잠금 정책을 사용 중지하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 클릭합니다.

   구성 창이 표시됩니다.

2. **사용** 토글을 클릭하여 잠금 정책을 해제합니다.

참고: 잠금 정책을 사용 중지하면 잠긴 사용자 계정으로 다시 연결을 시도할 수 있습니다.

잠긴 계정 목록을 조회하는 방법:

- Tenable Identity Exposure에서 **계정** > **사용자 계정 관리**로 이동합니다.

  Tenable Identity Exposure에서 사용자 목록에 잠긴 계정을 빨간색 자물쇠 아이콘과 함께 표시합니다. Tenable Identity Exposure에서는 잠긴 계정 사용자에게 다음과 같은 메시지를 표시합니다. "인증 시도가 너무 많이 실패하여 사용자의 계정이 잠겼습니다. 관리자에게 문의해야 합니다."

계정을 잠금 해제하는 방법:

계정 잠금을 해제하려면 사용자를 편집할 수 있는 권한이 있어야 합니다.

1. Tenable Identity Exposure에서 **계정** > **사용자 계정 관리**를 클릭합니다.

   사용자 계정 관리 창이 표시됩니다.

2. 사용자 목록에서 잠긴 계정을 찾습니다.
3. 연필 아이콘을 클릭하여 잠긴 사용자 계정을 편집합니다.

   해당 사용자의 정보 창이 표시됩니다.

4. **잠금 제거** 버튼을 클릭합니다.

사용자 역할에 잠금 정책을 구성할 권한을 부여하는 방법:

1. Tenable Identity Exposure에서 **계정** > **역할 관리**를 클릭합니다.

   역할 관리 창이 표시됩니다.

2. 역할 이름 옆에 있는 연필 아이콘을 클릭하여 역할을 편집합니다.

   역할 편집 창이 표시됩니다.

3. **시스템 구성 엔터티** 탭을 클릭합니다.

4. **권한 관리** 섹션 아래에서 **계정 잠금 정책** 확인란을 선택합니다.

5. 토글을 클릭하여 **권한 없음** 또는 **허가됨**으로 설정합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 해당 사용자의 권한을 업데이트했다고 확인합니다.

   > **참고**: Tenable Identity Exposure에서는 이 창에서 읽기 권한만 있는 사용자의 잠금 정책 설정을 사용 중지합니다.

LDAP를 사용하여 인증

Tenable Identity Exposure에서는 LDAP(Lightweight Directory Access Protocol)를 사용한 인증을 허용합니다.

LDAP 인증을 사용하려면 다음과 같은 항목이 있어야 합니다.

- Active Directory에 액세스하는 사용자 및 비밀번호가 있는 미리 구성한 서비스 계정.
- 미리 구성한 Active Directory 그룹.

LDAP 인증을 설정하면 로그인 페이지에 LDAP 옵션이 탭으로 표시됩니다.

LDAP 인증을 구성하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 클릭합니다.

   구성 창이 표시됩니다.

2. **인증** 섹션 아래에서 **LDAP**를 클릭합니다.
3. **LDAP 인증 사용** 토글을 클릭하여 사용으로 설정합니다.

   LDAP 정보 양식이 표시됩니다.

4. 다음과 같은 정보를 입력합니다.

   - **LDAP 서버 주소** 상자에 `ldap://`로 시작하고 도메인 이름 및 포트 번호로 끝나는 LDAP 서버 IP 주소를 입력합니다.

     > **참고**: LDAPS 서버를 사용하는 경우, `ldaps://`로 시작하고 도메인 이름 및 포트 번호로 끝나는 그 서버의 주소를 입력합니다. LDAPS 구성 완료 방법은 LDAPS에 사용자 지정된 신뢰할 수 있는 인증 기관(CA) 인증서를 추가하는 방법: 절차를 참조하십시오.

   - **LDAP 서버에 쿼리하는 데 사용하는 서비스 계정** 상자에 LDAP 서버에 액세스하는 데 사용하는 고유 이름(DN), SamAccountName 또는 UserPrincipalName을 입력합니다.
   - **서비스 계정 비밀번호** 상자에 이 서비스 계정의 비밀번호를 입력합니다.
   - **LDAP 검색 기준** 상자에 Tenable Identity Exposure에서 연결을 시도하는 사용자를 검색하는 데 사용하는 LDAP 디렉터리를 입력합니다(`DC=` 또는 `OU=`으로 시작). 이것은 루트 디렉터리일 수도 있고, 특정 조직 단위일 수도 있습니다.

- **LDAP 검색 필터** 상자에 Tenable Identity Exposure에서 사용자를 필터링하는 데 사용하는 특성을 입력합니다. Active Directory의 인증용 표준 특성은 `sAMAccountname={{login}}`입니다. 로그인의 값은 사용자가 인증하는 동안 제공하는 값입니다.

5. **SASL 바인딩 사용**의 경우, 다음 중 한 가지 작업을 수행합니다.
   - 서비스 계정에 SamAccountName을 사용하는 경우, **SASL 바인딩 사용** 토글을 클릭하여 사용으로 설정합니다.
   - 서비스 계정에 고유 이름 또는 UserPrincipalName을 사용하는 경우, **SASL 바인딩 사용**을 사용 안 함 설정에 둡니다.
6. **기본 프로필 및 역할** 섹션 아래에서 **LDAP 그룹 추가**를 클릭하여 인증이 허용된 그룹을 지정합니다.

   LDAP 그룹 정보 양식이 표시됩니다.
   - **LDAP 그룹 이름** 상자에 해당 그룹의 고유 이름을 입력합니다(예: `CN=TAD_User,OU=Groups,DC=Tenable,DC=ad`).
   - **기본 프로필** 드롭다운 상자에서 허용된 그룹의 프로필을 선택합니다.
   - **기본 역할** 상자에서 허용된 그룹의 역할을 선택합니다.
7. 필요한 경우 ⊕ 아이콘을 클릭하면 새 허용된 그룹을 추가할 수 있습니다.
8. **저장**을 클릭합니다.

LDAPS에 사용자 지정된 신뢰할 수 있는 인증 기관(CA) 인증서를 추가하는 방법:

1. Tenable Identity Exposure에서 **시스템**을 클릭합니다.
2. **구성** 탭을 클릭하여 구성 창을 표시합니다.
3. **애플리케이션 서비스** 섹션에서 **신뢰할 수 있는 인증 기관**을 클릭합니다.
4. **추가 CA 인증서** 상자에 Tenable Identity Exposure에서 사용할 회사의 PEM 인코딩된 신뢰할 수 있는 CA 인증서를 붙여 넣습니다.
5. **저장**을 클릭합니다.

보안 프로필과 역할에 대한 자세한 정보는 다음을 참조하십시오.

- 보안 프로필
- 사용자 역할

SAML을 사용한 인증

Tenable Identity Exposure 사용자가 Tenable Identity Exposure에 로그인할 때 ID 공급자가 시작한 SSO(Single Sing-On)를 사용할 수 있도록 SAML 인증을 구성할 수 있습니다.

시작하기 전에:

- Tenable Identity Exposure와 함께 사용하기 위해 SAML을 구성하는 방법에 대한 단계별 가이드는 Tenable SAML 구성 빠른 참조 가이드를 참조하십시오.
- ID 공급자(IDP)에 다음과 같은 항목이 있는지 확인합니다.
  - SAML v2 전용입니다.
  - "어설션 암호화"를 사용합니다.
  - Tenable Identity Exposure가 Tenable Identity Exposure 웹 포털에서 액세스 권한을 부여하기 위해 사용하는 사용하는 IDP 그룹입니다.
  - SAML 서버의 URL입니다.
  - SAML 서버 인증서에 PEM 인코딩된 형식으로 서명한 신뢰할 수 있는 인증 기관(CA)이며, `-----BEGIN CERTIFICATE -----`으로 시작하고 `-----END CERTIFICATE -----`으로 끝납니다.

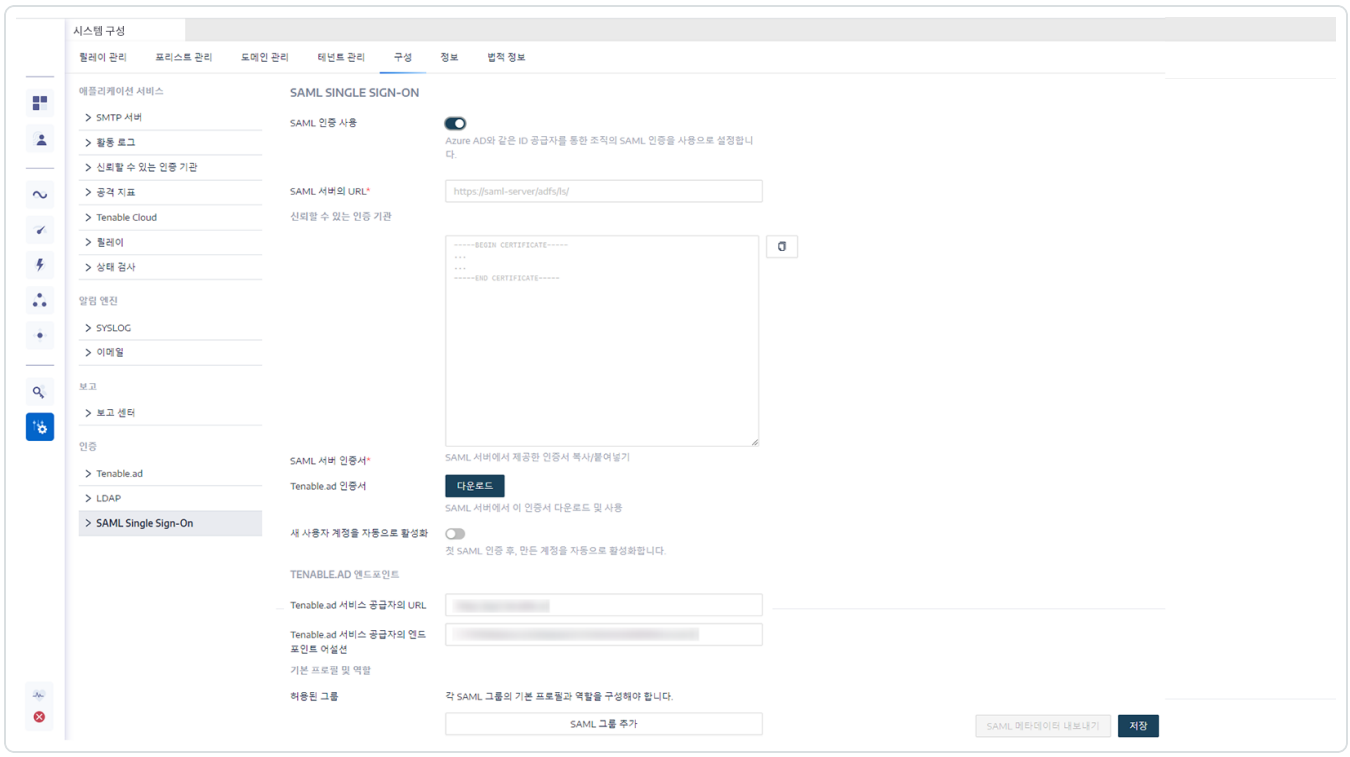
SAML 인증을 구성하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 클릭합니다.

   구성 창이 표시됩니다.

2. **인증** 섹션 아래에서 **SAML Single Sign-on**을 클릭합니다.
3. **SAML 인증 사용** 토글을 클릭합니다.

   SAML 정보 양식이 표시됩니다.



4. 다음과 같은 정보를 입력합니다.

    - **SAML 서버의 URL** 상자에 Tenable Identity Exposure가 연결해야 하는 IDP의 SAML 서버 URL 전체를 입력합니다.
    - **신뢰할 수 있는 인증 기관** 상자에 SAML 서버의 인증서에 서명한 CA를 붙여 넣습니다.

5. **Tenable Identity Exposure 인증서** 상자에서 **생성 및 다운로드**를 클릭합니다. 자체 서명한 새 인증서가 생성되고 데이터베이스의 SAML 구성이 업데이트되며 다운로드할 새 인증서를 반환합니다.

    주의: 이 버튼을 클릭하면 SAML 구성이 중단됩니다. Tenable Identity Exposure에서 IDP가 이전 인증서(존재하는 경우)를 계속 사용하는 동안 IDP가 가장 최근에 생성된 인증서로 즉시 인증할 것으로 예상하기 때문입니다. 새 Tenable Identity Exposure 인증서를 생성하는 경우, 새 인증서를 사용하도록 IDP를 다시 구성해야 합니다.

6. **새 사용자 계정을 자동으로 활성화** 토글을 클릭하여 SAML에 처음 로그인한 다음 새 사용자 계정을 활성화합니다.

7. **Tenable Identity Exposure 엔드포인트**에서 다음 정보를 입력합니다.

- Tenable Identity Exposure 서비스 공급자의 URL
- Tenable Identity Exposure 서비스 공급자의 엔드포인트 어설션

8. **기본 프로필 및 역할** 섹션 아래에서 **SAML 그룹 추가**를 클릭하여 인증이 허용된 그룹을 지정합니다.

   SAML 그룹 정보 양식이 표시됩니다.

9. 다음과 같은 정보를 입력합니다.
   - **SAML 그룹 이름** 상자에 허용된 그룹 이름을 SAML 서버에 표시되는 것과 같이 입력합니다.
   - **기본 프로필** 드롭다운 상자에서 허용된 그룹의 프로필을 선택합니다.
   - **기본 역할** 상자에서 허용된 그룹의 역할을 선택합니다.
10. 필요한 경우 ⊕ 아이콘을 클릭하면 새 허용된 그룹을 추가할 수 있습니다.
11. **저장**을 클릭합니다.

    SAML 인증을 설정하고 나면 로그인 페이지에 SAML 옵션이 탭으로 표시됩니다.

보안 프로필과 역할에 관한 자세한 정보는 다음을 참조하십시오.

- 보안 프로필
- 사용자 역할

사용자 계정

사용자 계정 관리 페이지에서 Tenable Identity Exposure 사용자 계정의 세부 정보를 추가, 편집, 삭제 또는 조회할 수 있습니다.

사용자는 두 개 범주에 속합니다.

- 전역 관리자 - 모든 권한을 포함하는 관리자 역할입니다.
- 사용자 - 비즈니스 데이터에 대한 읽기 전용 권한만 있는 단순한 사용자 역할입니다.

자세한 내용은 다음을 참조하십시오.

- 사용자 만들기
- 사용자 편집
- 사용자 비활성화
- 사용자 삭제

사용자 만들기

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

참고: 다음 지침은 Tenable Identity Exposure의 독립 실행형 인스턴스에 해당합니다. Tenable Vulnerability Management에 연결된 인스턴스의 경우, Tenable Vulnerability Management에서 사용자를 만들면 이것이 이후 Tenable Identity Exposure으로 전달됩니다.

사용자를 만드는 방법:

1. Tenable Identity Exposure에서 **계정** > **사용자 계정 관리**를 클릭합니다.

   사용자 계정 관리 창이 표시됩니다.

2. 오른쪽에 있는 **사용자 만들기** 버튼을 클릭합니다.

   사용자 만들기 창이 표시됩니다.

3. **기본 정보** 섹션 아래에 다음과 같은 사용자 관련 정보를 입력합니다.
   - 이름
   - 성
   - 이메일
   - 비밀번호: 적어도 12자(최소 소문자 1개, 대문자 1개, 숫자 1개, 특수 문자 1개 포함)
   - 비밀번호 확인
   - 부서
   - 약력
4. **인증 허용** 토글을 클릭하여 사용자를 활성화합니다.
5. **역할 관리** 섹션 아래에서 해당 사용자에게 적용할 역할을 선택합니다.
6. **만들기**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 선택한 역할의 사용자를 만들었다고 확인합니다.

참고 항목

- 사용자 편집
- 사용자 비활성화
- 사용자 삭제

사용자 편집

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

사용자를 편집하는 방법:

1. Tenable Identity Exposure에서 **계정** > **사용자 계정 관리**를 클릭합니다.

   사용자 계정 관리 창이 표시됩니다.

2. 사용자 목록에서 사용자의 이름이 표시되는 줄을 가리킨 다음 줄 끝의 ✎ 아이콘을 클릭합니다.

   사용자 편집 창이 표시됩니다.

3. **기본 정보** 섹션 아래에서 사용자에 관한 정보를 수정합니다(필요에 따라).
   - 이름
   - 성
   - 이메일
   - 비밀번호: 8자 이상 필수
   - 비밀번호 확인
   - 부서
   - 약력

4. **역할 관리** 섹션 아래에서 필요에 따라 사용자의 역할을 수정합니다.

5. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 선택한 역할의 사용자를 업데이트했다고 확인합니다.

참고 항목

- 사용자 만들기
- 사용자 비활성화
- 사용자 삭제

사용자 비활성화

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

사용자를 비활성화하는 방법:

1. Tenable Identity Exposure에서 **계정** > **사용자 계정 관리**를 클릭합니다.

   사용자 계정 관리 창이 표시됩니다.

2. 사용자 목록에서 사용자의 이름이 표시되는 줄을 가리킨 다음 줄 끝의 ✎ 아이콘을 클릭합니다.

   사용자 편집 창이 표시됩니다.

3. **인증 허용** 토글을 클릭하여 사용자를 비활성화합니다.

4. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 사용자를 업데이트했다고 확인합니다.

참고 항목

- 사용자 만들기
- 사용자 편집
- 사용자 삭제

사용자 삭제

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

사용자를 삭제하는 방법:

1. Tenable Identity Exposure에서 **계정** > **사용자 계정 관리**를 클릭합니다.

   사용자 계정 관리 창이 표시됩니다.

2. 사용자 목록에서 삭제하려는 사용자의 이름이 표시되는 줄을 가리킨 다음 줄 끝의 아이콘을 클릭합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.

3. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 사용자를 삭제했다고 확인합니다.

참고 항목

- 사용자 만들기
- 사용자 편집
- 사용자 비활성화

보안 프로필

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

프로필을 사용하면 Active Directory에 영향을 미치는 위험 보기를 만들고 사용자 지정할 수 있습니다.

각각의 프로필에 해당 프로필의 사용자에 대하여 구성된 노출 및 공격 시나리오가 표시됩니다. 예를 들어 IT 관리자의 데이터 분석의 일반 보기는 보안 팀의 일반 보기와 다를 수 있으며 AD 인프라에서 직면하는 모든 위험의 포괄적 보기를 표시합니다.

보안 프로필을 적용하면 다양한 유형의 사용자가 해당 보안 프로필의 지표에서 정의한 다양한 보고 관점에서 제공된 데이터 분석을 검토할 수 있습니다.

보안 프로필 관리 창을 사용하면 다양한 보고 관점의 보안 분석을 검토할 수 있는 다양한 사용자 유형을 유지할 수 있습니다. 보안 프로필을 사용하면 위험 노출 지표와 공격 지표의 동작을 사용자 지정할 수도 있습니다.

참고: Tenable Identity Exposure에서는 "Tenable"이라는 이름의 기본 보안 프로필을 제공합니다. **Tenable 프로필은 수정하거나 삭제할 수 없지만**, 이 프로필을 템플릿으로 사용해 각자 필요에 맞게 조정된 설정으로 다른 보안 프로필을 생성할 수 있습니다.

새 보안 프로필을 만드는 방법은 다음과 같습니다.

1. Tenable Identity Exposure에서 **계정** > **보안 프로필 관리**를 클릭합니다.

   보안 프로필 관리 창이 표시됩니다.

2. 오른쪽에 있는 **프로필 만들기** 버튼을 클릭합니다.

   프로필 만들기 창이 표시됩니다.

3. 작업 드롭다운 상자에서 다음 중 한 가지 조치를 취할 수 있습니다.

   - **새 프로필을 만듭니다**.
   - 기존 보안 프로필을 **복사**하여 이것을 바탕으로 새 프로필을 만듭니다(예: "Tenable" 프로필).

4. **새 프로필의 이름** 상자에 새 프로필의 이름을 입력합니다.

참고: Tenable Identity Exposure에서는 영숫자 글자와 밑줄만 허용합니다.

5. 오른쪽 하단에 있는 **만들기** 버튼을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 프로필을 만들었다고 표시합니다. **프로필 구성** 창이 표시됩니다.

보안 프로필을 삭제하는 방법:

1. Tenable Identity Exposure에서 **계정** > **보안 프로필 관리**를 클릭합니다.

   보안 프로필 관리 창이 표시됩니다.

2. 보안 프로필 목록에서 삭제하려는 보안 프로필을 가리키고 줄 끝의 🗑 아이콘을 클릭합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.

3. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 프로필을 삭제했다고 확인합니다.

다음에 할 일

프로필 만들기를 완료하려면 지표 사용자 지정에서 자세한 내용을 참조하십시오.

자세한 내용은 다음을 참조하십시오.

- 지표 사용자 지정
- 지표의 사용자 지정 미세 조정

지표 사용자 지정

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

보안 프로필의 위험 노출 지표와 공격 지표를 사용자 지정할 수 있습니다.

각 보안 프로필은 하나의 프로필이 다른 프로필의 결과에 영향을 미치지 않도록 독립적으로 작동합니다. "Tenable" 프로필은 사용자 지정하거나 일탈을 허용 목록에 추가하는 데 사용할 수 없으므로 참조용으로만 사용해야 합니다. 특정 요구 사항을 충족하려면 사용자 지정 프로필을 만들어야 합니다.

지표 사용자 지정 창에서 "전역 사용자 지정"이라는 용어는 모든 프로필이 아니라 **모든 도메인과 관련이 있습니다**. 결과적으로 하나의 보안 프로필에 대해 "전역 사용자 지정"에 적용하는 설정은 "Tenable" 프로필이나 다른 프로필에 영향을 미치지 않습니다.

팁: "Tenable" 보안 프로필의 설정을 확인하려면 줄 끝에 있는 👁 아이콘을 클릭합니다.

지표를 사용자 지정하는 방법:

1. Tenable Identity Exposure에서 **계정** > **보안 프로필 관리**를 클릭합니다.

   보안 프로필 관리 창이 표시됩니다.

2. 보안 프로필 목록에서 사용자 지정하려는 지표를 포함한 보안 프로필을 가리킵니다. 보안 프로필 이름이 표시되는 줄 끝의 ✎ 아이콘을 클릭합니다.

   프로필 구성 창이 표시됩니다.

3. **위험 노출 지표** 또는 **공격 지표** 탭을 선택합니다.

4. (선택 사항) **지표 검색** 상자에 지표 이름을 입력합니다.

5. 사용자 지정할 지표 이름을 클릭합니다.

   지표 사용자 지정 창이 표시됩니다.

6. 지표에 필요한 사용자 지정을 적용합니다.

   참고: 일부 지표 옵션의 경우 정규식(regex)을 사용해야 합니다. 정규식은 '같은(equal)' 일치가 아니라 '포함(contain)' 일치 방식입니다. 예: 입력 옵션으로 "admin"을 제공하는 경우, "samAccountName=admin"의 사용자와 "samAccountName=admintoto"의 사용자를 허용 목록에 추가할 수 있습니다.
   - 정확한 일치 결과를 얻으려면 정규식 특수 문자("^...$") 구문을 사용해야 합니다.

- 또한 정규식을 사용할 때는 백슬래시를 사용해 특수 문자를 이스케이프해야 합니다. 예: `"domain\user"` 및 `"CN=Vincent C (Test),DC=tenable,DC=corp"`를 선언하려면 `"domain\\user"` 및 `"CN=Vincent C. \(Test\),DC=tenable,DC=corp"`를 입력합니다.

7. **초안 저장**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 사용자 지정 옵션을 저장했다고 확인합니다.

사용자 지정을 적용하는 방법:

1. 다음 중 한 가지 조치를 취할 수 있습니다.
   - **프로필 구성** 창에서 오른쪽 하단에 있는 **보류 중인 사용자 지정 적용**을 클릭하거나
   - **보안 프로필 관리** 창에서 보안 프로필 이름이 표시되는 줄 끝의 ✓ 아이콘을 클릭합니다.

   메시지가 표시되어 사용자 지정을 적용하면 데이터가 모두 지워지고 시간이 소요되는 모니터링되는 Active Directory의 전체 분석이 필요하다고 경고합니다.
2. **확인**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 사용자 지정 옵션을 적용했다고 확인합니다. **보안 프로필 관리** 표의 *보안 분석* 열에 **대기 중**이라고 표시되면 보안 프로필에 따른 분석이 실행 대기 중이라는 뜻입니다.

사용자 지정을 취소하는 방법:

- 다음 중 한 가지 조치를 취할 수 있습니다.
  - **프로필 구성** 창에서 왼쪽 하단에 있는 **보류 중인 사용자 지정 되돌리기**를 클릭하거나
  - **보안 프로필 관리** 창에서 보안 프로필 이름이 표시되는 줄 끝의 ↶ 아이콘을 클릭합니다.

  메시지가 표시되어 Tenable Identity Exposure에서 사용자 지정 옵션을 취소했다고 확인합니다.

참고 항목

- 지표의 사용자 지정 미세 조정

지표의 사용자 지정 미세 조정

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

보안 프로필의 지표에 추가로 사용자 지정을 적용하면 특정 도메인에 대한 지표 옵션을 선택할 수 있습니다. 기본적으로, 전역 사용자 지정은 모든 도메인에 적용됩니다.

지표의 사용자 지정을 미세 조정하는 방법:

1. Tenable Identity Exposure에서 **계정** > **보안 프로필 관리**를 클릭합니다.

   보안 프로필 관리 창이 표시됩니다.

2. 보안 프로필 목록에서 사용자 지정하려는 지표를 포함한 보안 프로필을 가리킵니다. 보안 프로필 이름이 표시되는 줄 끝의 ✎ 아이콘을 클릭합니다.

   프로필 구성 창이 표시됩니다.

3. **위험 노출 지표** 또는 **공격 지표** 탭을 선택합니다.
4. (선택 사항) **지표 검색** 상자에 지표 이름을 입력합니다.
5. 사용자 지정할 지표의 이름을 클릭합니다.

   지표 사용자 지정 창이 표시됩니다.

6. **전역 사용자 지정** 탭 옆에 있는 ✚ 아이콘을 클릭합니다.

   사용자 지정 번호 1 탭이 표시됩니다.

7. **적용** 상자를 클릭합니다.

   포리스트 및 도메인 창이 표시됩니다.

8. (선택 사항) 검색 상자에 포리스트 또는 도메인 이름을 입력합니다.
9. 도메인을 선택합니다.
10. **선택 항목 필터링**을 클릭합니다.
11. 선택한 도메인의 지표에 필요에 따라 추가로 사용자 지정을 적용합니다.
12. **초안 저장**을 클릭합니다.

미세 조정한 사용자 지정을 취소하는 방법:

1. 사용자 지정 탭을 클릭합니다.
2. 창 아래에 있는 **이 구성 제거**를 클릭합니다.

참고 항목

- 지표 사용자 지정

사용자 역할

Tenable Identity Exposure에서는 사용자 역할 기반 액세스 제어(RBAC)를 사용하여 조직 내 데이터 및 기능에 대한 액세스 보안을 유지합니다. 역할은 사용자가 맡은 역할에 따라 자신의 계정에서 액세스할 수 있는 정보의 유형을 결정합니다.

적절한 권한이 있는 사용자는 다른 사용자에게 각자의 역할에 따라 권한을 할당하여 다음과 같은 작업을 수행하도록 할 수 있습니다.

- 콘텐츠와 메뉴, 시스템 및 위험 노출 지표 구성을 읽습니다.
- 콘텐츠와 메뉴, 시스템 및 공격 지표 구성을 편집합니다.
- 계정, 보안 프로필과 역할을 만듭니다.

참고 항목

- 역할 관리
- 역할에 대한 권한 설정
- 사용자 인터페이스 엔터티에 대한 권한 설정(예)

역할 관리

새 역할을 만드는 방법:

1. Tenable Identity Exposure에서 **계정** > **역할 관리**로 이동합니다.
2. 오른쪽 상단에 있는 **역할 만들기** 버튼을 클릭합니다.

   역할 만들기 창이 표시됩니다.
3. 이름 상자에 역할의 이름을 입력합니다.
4. 설명 상자에 해당 역할에 대한 몇 가지 정보를 입력합니다.
5. 오른쪽 하단에 있는 **추가**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 역할을 만들었다고 확인합니다. 역할을 설정할 수 있는 **역할 편집** 창이 표시됩니다.

참고: Tenable Identity Exposure 관리자 역할(전역 관리자라고 함)은 수정할 수 없습니다. 아이콘을 클릭하면 Tenable Identity Exposure 역할 설정이 표시됩니다.

역할을 삭제하는 방법:

1. Tenable Identity Exposure에서 **계정** > **역할 관리**로 이동합니다.
2. 역할 목록에서 삭제하려는 역할을 가리키고 오른쪽에 있는 아이콘을 클릭합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.
3. 삭제를 클릭합니다.

   메시지가 표시되어 역할을 삭제했다고 확인합니다.

참고 항목

- 역할에 대한 권한 설정

역할에 대한 권한 설정

필수 사용자 역할: 관리자 또는 적절한 권한이 있는 조직 사용자.

Tenable Identity Exposure에서는 역할 기반 액세스 제어(RBAC)를 사용해 데이터에 대한 액세스 보안을 유지합니다. 역할은 사용자가 조직 내에서 맡은 기능적인 역할에 따라 액세스할 수 있는 정보의 유형을 결정합니다. Tenable Identity Exposure에서 새 사용자를 만들면 해당 사용자에게 특정 역할과 그에 연결된 권한을 할당하게 됩니다.

역할에 대한 권한을 설정하는 방법:

1. Tenable Identity Exposure에서 **계정** > **역할 관리**를 클릭합니다.
2. 권한을 설정하려는 역할을 가리키고 오른쪽의 아이콘을 클릭합니다.

   역할 편집 창이 표시됩니다.
3. **권한 관리** 아래에서 엔터티 유형을 선택합니다.
   - 데이터 엔터티
   - 사용자 엔터티
   - 시스템 구성 엔터티
   - 인터페이스 엔터티
4. 엔터티 이름 목록에서 권한을 설정할 엔터티를 선택합니다.
5. **읽기**, **편집** 또는 **만들기** 열 아래에서 토글을 클릭하여 허가됨 또는 권한 없음으로 설정합니다.
6. 다음 중 한 가지 조치를 취할 수 있습니다.
   - 적용을 클릭하여 해당 권한을 적용하고 **역할 편집** 창은 추가 수정을 위해 열어둡니다.
   - 적용을 클릭하고 닫아 권한을 적용하고 **역할 편집** 창을 닫습니다.

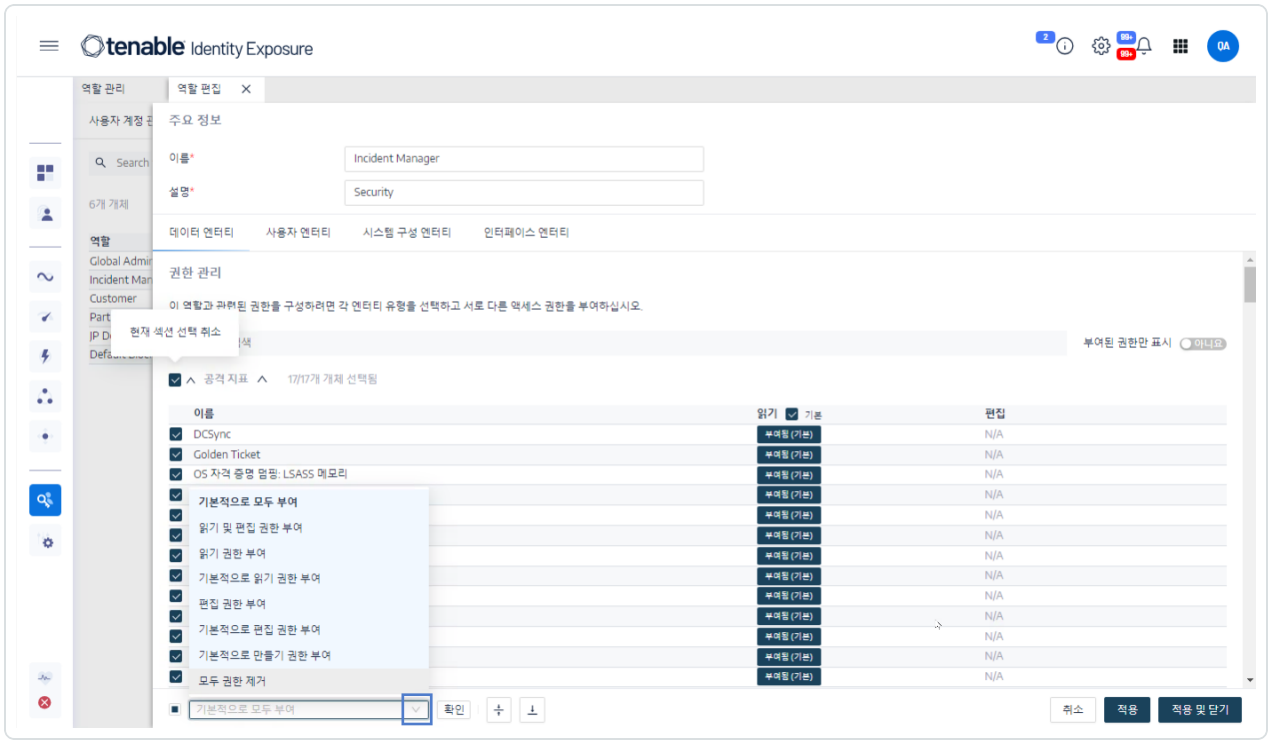
   메시지가 표시되어 Tenable Identity Exposure에서 역할을 업데이트했다고 확인합니다.

역할에 대하여 권한을 일괄 설정하는 방법:

1. Tenable Identity Exposure에서 **계정** > **역할 관리**를 클릭합니다.
2. 권한을 설정하려는 역할을 가리키고 오른쪽의 ✎ 아이콘을 클릭합니다.

   역할 편집 창이 표시됩니다.
3. **권한 관리** 아래에서 엔터티 유형을 선택합니다.
4. 권한을 설정할 엔터티 또는 엔터티의 섹션(예: 위험 노출 지표)을 선택합니다.
5. 페이지 아래에서 드롭다운 상자의 화살표를 클릭하여 권한 목록를 표시합니다.
6. 역할의 권한을 선택합니다.
7. **확인**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 엔터티에 권한을 설정했다고 확인합니다.



권한 유형

권한	설명
읽기	개체 또는 구성을 볼 수 있는 권한입니다.
편집	개체 또는 구성을 수정하는 권한입니다. 수정 사항을 적용하려면 읽기 권한이 필요합

	니다.
만들기	개체 또는 구성을 만드는 권한입니다. **만들기** 권한에는 **읽기** 및 **편집** 권한이 있어야 허용된 리소스에서 허용된 작업을 수행할 수 있습니다.

엔터티 유형

Tenable Identity Exposure에는 네 가지 유형의 엔터티가 있어 액세스하려면 권한이 필요하며 이러한 권한은 조직 내 각 사용자 역할에 따라 조정할 수 있습니다.

엔터티 유형	포함	권한
데이터 엔터티		
이 엔터티는 모니터링되는 Active Directory를 설정하고 Tenable Identity Exposure에서 데이터 분석을 구성하는 데 필요한 권한을 제어합니다.	• 공격 지표 • 위험 노출 지표 • 포리스트 • 도메인 • 프로필 • 사용자 • 이메일 알림 • Syslog 알림 • 역할 • 엔터티 릴레이 • 보고서	읽기, 편집, 만들기
사용자 엔터티		
이 엔터티는 Tenable Identity Exposure에서 데이터 분석을 위해 표시하는 정보를 사용자가 구성하는 능력과 개인 정보 및 기본 설정을 수정하는 능력을 제어합니	• 기본 설정 • 대시보드 • 위젯	편집, 만들기

다.	• API 키 • 개인 정보	
시스템 구성 엔터티		
이 엔터티는 Tenable Identity Exposure 플랫폼 및 서비스에 대한 액세스를 제어합니다.	• 애플리케이션 서비스(SMTP, 로그, 인증 Tenable Identity Exposure, 공격 지표, 신뢰할 수 있는 인증 기관) • 공개 API를 통한 점수 • 라이선스 • LDAP 인증 • SAML 인증 **참고**: Tenable Vulnerability Management 라이선스가 있는 경우 LDAP 및 SAML 인증에 대한 권한을 사용할 수 없습니다. • 토폴로지 • 계정 잠금 정책 • 도메인 다시 크롤링 • 활동 로그 • Tenable Cloud Service(Tenable Cloud 데이터 수집) • Microsoft Entra ID 지원 • 상태 검사 • 사용자의 자체 추적만 표시	읽기, 편집
인터페이스 엔터티		
이 엔터티는 Tenable Identity Exposure 사용자 인터페이스와 기능의 특정 부분에	특정 Tenable Identity Exposure 기능에 대한 액세스 경로입니다. 자세한 내용은	허가됨, 권

액세스하는 권한을 정의합니다.	사용자 인터페이스 엔터티에 대한 권한 설정(예)를 참조하십시오.	한 없음

참고 항목

- 사용자 계정
- 사용자 역할

사용자 인터페이스 엔터티에 대한 권한 설정(예)

Tenable Identity Exposure에서는 특정 사용자 인터페이스 기능에 액세스하는 데 사용되는 경로를 따라 권한을 적용합니다. 다음 예는 Syslog 구성을 허용하기 위해 권한을 설정하는 방법을 보여줍니다.

Syslog 매개 변수에 도달하려면 사용자에게는 Tenable Identity Exposure의 **시스템** > **구성** > **SYSLOG** 경로를 따라 권한이 필요합니다.

- 시스템 구성: **관리** > **시스템**
- 구성 매개 변수: **관리** > **시스템** > **구성**
- Syslog 알림: **관리** > **시스템** > **구성** > **알림 엔진** > **SYSLOG**

Syslog 구성에 대한 권한을 설정하는 방법:

1. Tenable Identity Exposure에서 **계정** > **역할 관리**를 클릭합니다.
2. 권한을 설정하려는 역할을 가리키고 오른쪽의 아이콘을 클릭합니다.

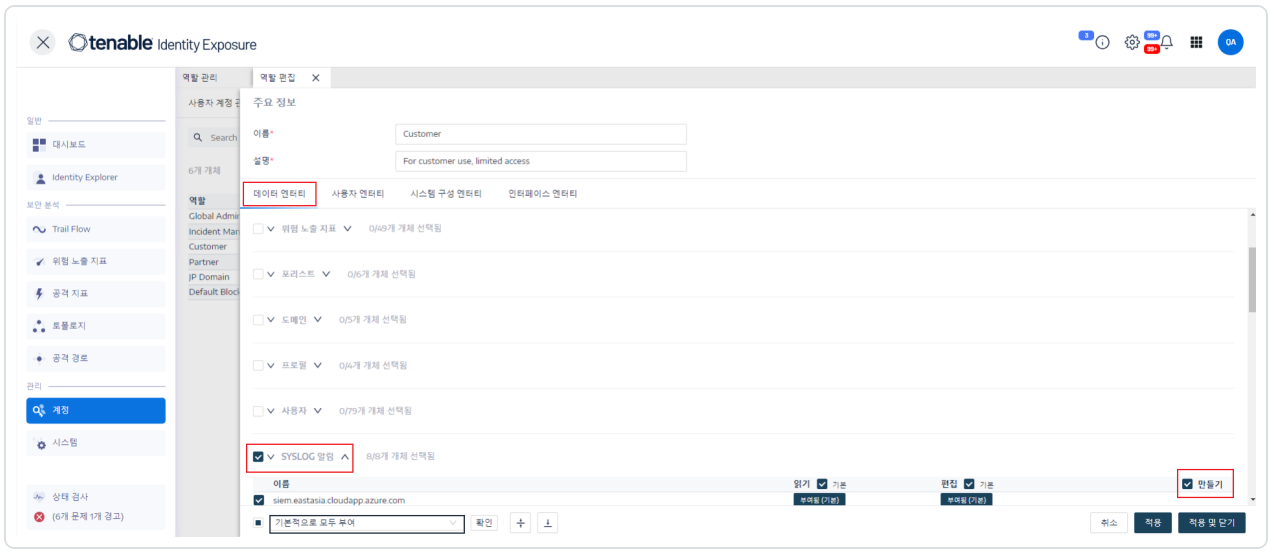
   역할 편집 창이 표시됩니다.
3. **권한 관리** 아래에서 **인터페이스 엔터티**를 선택합니다.
4. 엔터티 목록에서 다음과 같은 작업을 수행합니다.
   - **관리** > **시스템**을 선택하고 액세스 토글을 클릭하여 **허가됨**으로 설정합니다.
   - **관리** > **시스템** > **구성**을 선택하고 액세스 토글을 클릭하여 **허가됨**으로 설정합니다.
   - **관리** > **시스템 구성** > **알림 엔진** > **SYSLOG**를 선택하고 액세스 토글을 클릭하여 **허가됨**으로 설정합니다.
5. **적용**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 엔터티에 대한 권한을 업데이트했음을 확인합니다.

6. **권한 관리** 아래에서 **데이터 엔터티**를 선택합니다.
7. 엔터티 섹션 목록에서 **Syslog 알림**을 선택합니다.
8. **만들기** 권한을 선택합니다.

   Tenable Identity Exposure에서 암시적으로 읽기 및 편집 권한을 부여합니다.
9. **적용 및 닫기**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 엔터티에 대한 권한을 업데이트했음을 확인합니다.


tenable Identity Exposure
역할 관리
역할 편집
주요 정보
이름*
Customer
설명*
For customer use, limited access
데이터 엔터티
사용자 엔터티
시스템 구성 엔터티
인터페이스 엔터티
위험 노출 지표
포리스트
도메인
프로필
사용자
SYSLOG 알림
이름
읽기
편집
만들기
siem.eastasia.cloudapp.azure.com
기본적으로 모두 부여
확인
취소
적용
적용 및 닫기
대시보드
Identity Explorer
Trail Flow
공격 지표
토폴로지
공격 경로
계정
시스템
상태 검사

포리스트

Active Directory(AD) 포리스트는 공통 스키마, 구성 및 트러스트 관계를 공유하는 도메인의 모음입니다. 리소스를 관리 및 구성하기 위한 계층 구조를 제공하여 중앙 집중형 관리를 지원하며 한 조직 내 여러 도메인 전체에서 보안 인증을 지원합니다.

포리스트 관리

포리스트를 추가하는 방법:

1. Tenable Identity Exposure에서 **시스템**> **포리스트 관리**를 클릭합니다.
2. 오른쪽에 있는 **포리스트 추가**를 클릭합니다.

   포리스트 추가 창이 표시됩니다.
3. **이름** 상자에 포리스트 이름을 입력합니다.
4. **계정** 섹션에 Tenable Identity Exposure에서 사용하는 계정에 대해 다음과 같은 정보를 입력합니다.
   - **로그인**: 서비스 계정의 이름을 입력합니다.
     형식: 사용자 주체 이름, 예를 들어 "`tenablead@domain.example.com`"(Kerberos 인증과의 호환성을 위해 권장) 또는 NetBIOS(예: "`DomainNetBIOSName\SamAccountName`").
   - **비밀번호**: 서비스 계정의 비밀번호를 입력합니다.

   참고: Tenable Identity Exposure의 AD 서비스 계정을 보호된 사용자 그룹 구성원으로 설정해야 하는 경우, Tenable Identity Exposure 구성이 Kerberos 인증을 지원해야 합니다. 보호되는 사용자는 NTLM 인증을 사용할 수 없기 때문입니다.
5. **추가**를 클릭합니다.

   메시지가 표시되어 새 포리스트가 추가되었다고 확인합니다.

포리스트를 편집하는 방법:

1. Tenable Identity Exposure에서 **시스템**> **포리스트 관리**를 클릭합니다.
2. 포리스트 목록에서 수정하려는 포리스트를 가리키고 오른쪽에 있는 ✎ 아이콘을 클릭합니다.

   포리스트 편집 창이 표시됩니다.
3. 필요에 따라 수정합니다.
4. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 포리스트를 업데이트했다고 확인합니다.

서비스 계정 보호

Tenable에서는 사용자 계정 제어(UAC) 특성을 올바로 설정하여 보안을 유지하기 위해 서비스 계정을 보호하도록 권장합니다. 이렇게 해야 위임을 방지하고 사전 인증을 필수로 설정하며 더 강력한 암호화를 사용하고 비밀번호 만료 및 요구 사항을 적용하고 승인된 비밀번호 변경만 허용할 수 있습니다. 이러한 조치를 취하면 무단 액세스와 잠재적인 보안 침해 위험을 완화하고 조직 시스템과 데이터의 무결성을 보장할 수 있습니다.

Windows 정책 편집기를 사용하여 설정을 수정하는 방법:

사용자 계정 제어 설정은 Windows의 로컬 보안 정책 편집기나 그룹 정책 편집기(적절한 관리자 권한이 있어야 함)를 사용해 수정하면 됩니다.

- 편집기에서 **로컬 정책** > **보안 옵션**으로 이동하여 다음과 같은 설정을 찾아 구성합니다(이 내용은 Windows 버전에 따라 다를 수 있음).
  - "*네트워크 액세스: 네트워크 인증을 위한 비밀번호 및 자격 증명 저장 허용 안 함*": **사용**으로 설정합니다.
  - "*계정: Kerberos 사전 인증 필수 아님*": **사용 중지**로 설정합니다.
  - "*네트워크 보안: Kerberos에 대해 허용된 암호화 유형 구성*": "*이 계정에 Kerberos DES 암호화 유형 사용*" 옵션을 선택하면 **안 됩니다.**
  - "*계정: 최대 비밀번호 기간*": 비밀번호 만료 기간을 설정합니다(예: `PasswordNeverExpires = FALSE`가 되도록 30일, 60일, 90일 등이어야 함).
  - "*계정: 로컬 계정의 빈 비밀번호 사용을 콘솔 로그온으로만 제한*": **사용 중지**로 설정합니다.
  - "*대화형 로그온: 캐시할 이전 로그온 수(도메인 컨트롤러를 사용할 수 없는 경우)*": 원하는 값(예: "10")으로 설정해 사용자가 자신의 비밀번호를 변경하도록 허용합니다.

Powershell을 사용하여 설정을 수정하는 방법:

- AD를 호스팅하는 컴퓨터에서 적절한 관리 권한으로 PowerShell을 열고 다음과 같은 명령을 실행합니다.

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
```

```
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

여기에서 <AD_ACCOUNT>는 수정하려는 Active Directory 계정의 이름입니다.

도메인

Tenable Identity Exposure에서는 중앙 집중식 관리를 위해 논리적 방식으로 공통의 설정을 공유하는 개체를 그룹화하는 도메인을 모니터링합니다.

도메인을 추가하는 방법:

1. Tenable Identity Exposure에서 **시스템**을 클릭합니다.
2. **도메인 관리** 탭을 클릭합니다.

   도메인 관리 창이 표시됩니다.
3. 오른쪽 상단에 있는 **도메인 추가**를 클릭합니다.

   도메인 추가 창이 표시됩니다.

4. **기본 정보** 섹션에 다음과 같은 정보를 입력합니다.

    - **이름** 상자에 도메인 이름을 입력합니다.
    - **도메인 FQDN** 상자에 도메인의 FQDN(정규화된 도메인 이름)을 입력합니다.
    - **포리스트** 드롭다운 상자에서 도메인이 속한 포리스트를 선택합니다.

5. **권한 있는 분석**(선택 사항): 토글을 사용으로 설정하면 이 포리스트의 "dcadmin" 계정이 고급 보안 분석을 수행하기 위해 이 도메인에서 권한 있는 데이터를 수집하도록 허용하게 됩니다.

6. **권한이 있는 분석 전송**: 이 옵션에 대한 자세한 내용은 Tenable Cloud 데이터 수집를 참조하십시오.

7. **기본 도메인 컨트롤러** 섹션에 다음과 같은 정보를 입력합니다.

   - **IP 주소 또는 호스트 이름** 상자에 기본 도메인 컨트롤러의 호스트 이름(Kerberos 인증과의 호환성을 위해 필요하지만 SaaS-VPN 배포 모드와 호환되지 않음) 또는 IP 주소를 입력합니다.

     > Tenable Identity Exposure에서는 로드 밸런서를 지원하지 않습니다.

   - **LDAP 포트** 상자에 기본 도메인 컨트롤러의 LDAP 포트를 입력합니다.

     > **참고**: TCP/636(LDAPS) 포트를 사용하여 도메인에 연결하는 경우, Tenable Identity Exposure에서 연결을 수행하려면 AD 인증서를 유효성 검사하기 위해 Active Directory의 인증 기관(CA) 인증서에 액세스할 수 있어야 합니다. Secure Relay 환경에서는 Relay 시스템에 CA 인증서를 설치할 수 있습니다. VPN 환경에서는 이 구성이 불가능합니다.

   - **전역 카탈로그 포트** 상자에 기본 도메인 컨트롤러의 전역 카탈로그 포트를 입력합니다.
   - **SMB 포트** 상자에 기본 도메인 컨트롤러의 SMB 포트를 입력합니다.

8. **추가**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 도메인을 추가했다고 확인합니다.

도메인을 편집하는 방법:

1. Tenable Identity Exposure에서 **시스템**을 클릭합니다.
2. **도메인 관리** 탭을 클릭합니다.

   도메인 관리 창이 표시됩니다.

3. 편집하려는 도메인 이름을 가리키면 오른쪽에 ✎ 아이콘이 표시됩니다.
4. ✎ 아이콘을 클릭합니다.

   도메인 편집 창이 표시됩니다.

5. 도메인의 정보를 편집합니다.
6. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 도메인을 업데이트했다고 확인합니다.

도메인을 삭제하는 방법:

1. Tenable Identity Exposure에서 **시스템**을 클릭합니다.
2. **도메인 관리** 탭을 클릭합니다.

   도메인 관리 창이 표시됩니다.
3. 삭제하려는 도메인 이름을 가리키면 🗑 아이콘이 표시됩니다.
4. 🗑 아이콘을 클릭합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.
5. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 도메인을 삭제했다고 확인합니다.

참고 항목

- 도메인에서 데이터 강제로 새로 고침
- 허니팟 계정
- Kerberos 인증

도메인에서 데이터 강제로 새로 고침

도메인에서 데이터를 강제로 새로 고치는 방법:

1. Tenable Identity Exposure에서 **시스템**을 클릭합니다.
2. **도메인 관리** 탭을 클릭합니다.

   도메인 관리 창이 표시됩니다.
3. 데이터를 강제로 새로 고치려는 도메인 이름을 가리키면 오른쪽에 ↻ 아이콘이 표시됩니다.
4. ↻ 아이콘을 클릭합니다.

   데이터 새로 고침 작업에 관한 정보가 포함된 메시지가 표시됩니다.
5. **확인**을 클릭합니다.

참고 항목

- 허니팟 계정

허니팟 계정

필수 사용자 역할: 로컬 시스템의 관리자

허니팟 계정은 미끼 계정이며 Active Directory를 통해 네트워크를 침해하려 하는 공격자를 탐지하는 것이 이 계정의 유일한 목적입니다.

Tenable Identity Exposure의 공격 지표가 Kerberoasting 악용 시도를 탐지하려면 이 계정이 전제 조건입니다. 이 공격은 서비스 티켓을 요청 및 탈취한 다음 해당 서비스 계정의 자격 증명을 오프라인으로 크래킹하여 서비스 계정에 대한 액세스를 얻으려고 합니다. Kerberoasting 공격 지표는 허니팟 계정에 로그인 시도 또는 티켓 요청이 수신되면 알림을 보냅니다.

도메인당 하나의 허니팟 계정을 연결합니다. 허니팟 계정은 보안 프로필과 관련이 없습니다.

허니팟 계정을 추가하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **도메인 관리**를 클릭합니다.

   도메인 관리 창이 표시됩니다.

2. 허니팟 계정을 추가하려는 도메인을 가리킵니다.

3. **허니팟 계정 구성 상태** 아래에서 **+**를 클릭합니다.

   허니팟 계정 추가 창이 표시됩니다.

4. **이름** 상자에 허니팟 계정으로 사용할 사용자 계정의 고유 이름(DN)을 입력합니다.

   팁: 임의의 문자열을 입력하면 Tenable Identity Exposure에서 검색을 실시하여 해당 사용자 계정이 Active Directory에 있는 경우 일치하는 사용자 계정 이름을 드롭다운 상자에 표시합니다.

5. **배포** 섹션에 Tenable Identity Exposure에서 허니팟 계정을 배포하기 위해 실행할 적절한 설정을 포함한 스크립트를 생성합니다. 를 클릭하여 이 스크립트를 복사합니다.

6. **추가**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 허니팟 계정을 추가했다고 확인합니다. 도메인 관리 창에서 선택한 도메인의 **허니팟 계정 구성 상태**가 주황색( )으로 표시되어 활성화하려면 허니팟 계정 배포 스크립트를 실행해야 한다고 알려줍니다.

참고: **허니팟 계정 구성 상태**가 빨간색(🔴)으로 표시되는 경우, Tenable Identity Exposure에서 Active Directory에서 이 사용자 계정을 찾을 수 없음을 나타냅니다. 이 사용자 계정부터 만들고 다음 단계로 계속 진행해야 합니다.

7. Active Directory 모듈을 포함한 시스템의 Windows PowerShell에서 복사한 허니팟 계정 배포 스크립트를 실행합니다.

   도메인 관리 창에 선택한 **허니팟 계정 구성 상태**가 녹색 상태(🟢)로 표시되어 활성 상태임을 나타냅니다.

   참고: Tenable Identity Exposure에서 허니팟 계정을 처리하고 활성화하는 데 시간이 걸릴 수 있습니다.

허니팟 계정을 편집하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **도메인 관리**를 클릭합니다.

   도메인 관리 창이 표시됩니다.

2. 허니팟 계정을 추가하려는 도메인을 가리킵니다.
3. **허니팟 계정 구성 상태** 아래에서 오른쪽에 있는 아이콘을 클릭합니다.

   허니팟 계정 편집 창이 표시됩니다.

4. **이름** 상자에서 필요에 따라 사용자 계정을 수정합니다.
5. **배포** 섹션에서 를 클릭하여 허니팟 계정 배포 스크립트를 복사합니다.
6. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 허니팟 계정을 업데이트했다고 확인합니다. 도메인 관리 창에서 선택한 도메인의 **허니팟 계정 구성 상태**가 주황색(🟠)으로 표시되어 활성화하려면 허니팟 계정 배포 스크립트를 실행해야 한다고 알려줍니다.

   참고: **허니팟 계정 구성 상태**가 빨간색(🔴)으로 표시되는 경우, Tenable Identity Exposure에서 Active Directory에서 이 사용자 계정을 찾을 수 없음을 나타냅니다. 이 사용자 계정부터 만들고 다음 단계로 계속 진행해야 합니다.

7. Active Directory 모듈을 포함한 시스템의 Windows PowerShell에서 복사한 허니팟 계정 배포 스크립트를 실행합니다.

도메인 관리 창에 선택한 **허니팟 계정 구성 상태**가 녹색 상태(●)로 표시되어 구성된 상태임을 나타냅니다.

> **참고**: Tenable Identity Exposure에서 허니팟 계정을 처리하고 활성화하는 데 시간이 걸릴 수 있습니다.

허니팟 계정을 삭제하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **도메인 관리**를 클릭합니다.

   도메인 관리 창이 표시됩니다.

2. 허니팟 계정을 추가하려는 도메인을 가리킵니다.

3. **허니팟 계정 구성 상태** 아래에서 오른쪽에 있는 아이콘을 클릭합니다.

   허니팟 계정 편집 창이 표시됩니다.

4. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 허니팟 계정을 삭제했다고 확인합니다.

참고 항목

- 도메인에서 데이터 강제로 새로 고침

Kerberos 인증

Tenable Identity Exposure에서는 제공된 자격 증명을 사용하여 구성된 도메인 컨트롤러를 인증합니다. 이러한 DC는 NTLM 또는 Kerberos 인증을 수락합니다. NTLM은 문서화된 보안 문제가 있는 기존 프로토콜이며 Microsoft 및 모든 사이버 보안 표준에서는 이제 사용을 권장하지 않습니다. 대신에 Kerberos가 더욱 강력한 프로토콜이므로 이를 고려해야 합니다. Windows는 항상 Kerberos를 먼저 시도하고 Kerberos를 사용할 수 없는 경우에만 NTLM을 시도합니다.

Tenable Identity Exposure는 몇 가지 예외를 제외하고는 NTLM 및 Kerberos와 모두 호환됩니다. Tenable Identity Exposure는 모든 필수 조건을 충족하는 경우 Kerberos를 기본 프로토콜로 우선 지정합니다. 이 섹션에서는 요구 사항을 설명하고 Kerberos를 사용할 수 있도록 Tenable Identity Exposure를 구성하는 방법을 보여줍니다.

Kerberos 대신 NTLM을 사용하는 것도 SYSVOL 강화가 Tenable Identity Exposure를 방해하는 원인이 됩니다. 자세한 내용은 Tenable Identity Exposure와 SYSVOL 강화 간섭을 참조하십시오.

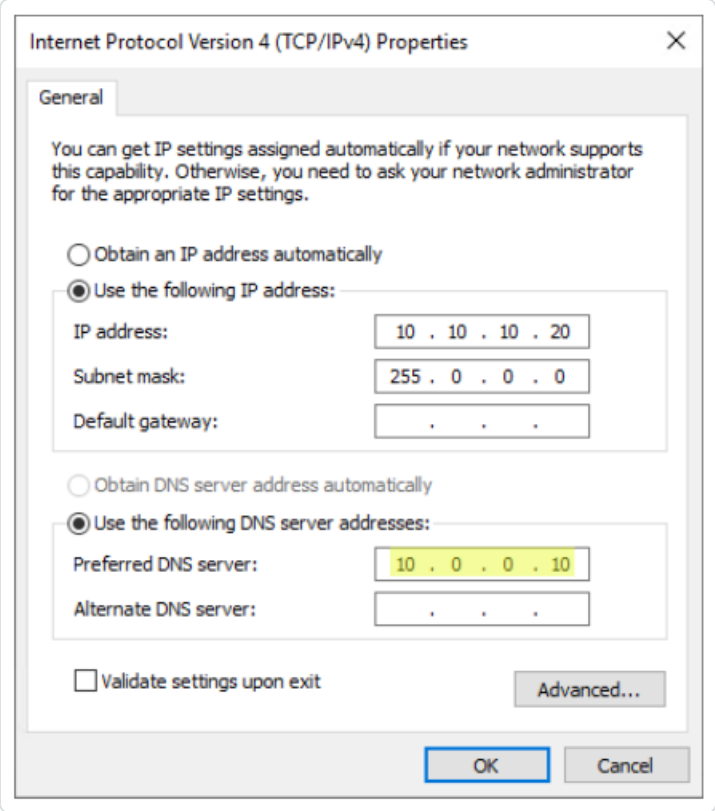
Tenable Identity Exposure 배포 모드와의 호환성

배포 모드	Kerberos 지원
온프레미스	예
SaaS-TLS(기존)	예
Secure Relay를 사용하는 SaaS	예
VPN을 사용하는 SaaS	아니요 - 설치를 Secure Relay 배포 모드로 전환해야 합니다.

기술 요구 사항

- **Tenable Identity Exposure에 구성된 AD 서비스 계정에는 UPN(UserPrincipalName)이 있어야 합니다**. 서비스 계정 및 도메인 구성의 설명을 참조하십시오.
- **DNS 구성 및 DNS 서버에서는 모든 필수적인 DNS 항목 확인을 허용해야 함** - 도메인 컨트롤러를 알고 있는 DNS 서버를 사용하도록 Directory Listener 또는 Relay 시스템을 구성해야 합니다. Directory Listener 또는 Relay 시스템이 도메인에 가입한 경우(Tenable Identity Exposure에서 권장하지 않음), 이 요구 사항을 이미 충족한 상태일 것입니다. 일반적으로 도메인 컨트롤러도 DNS를 실행하므로 가장 쉬운 방법은 도메인 컨트롤러 자체를 기본 설정 DNS 서버로 사용하는

것입니다. 예:



참고: Directory Listener 또는 Relay 시스템이 여러 도메인에 연결되고 여러 포리스트에 있을 가능성이 있는 경우, 구성된 DNS 서버가 모든 도메인에 필수적인 모든 DNS 항목을 확인할 수 있는지 확인하십시오. 그렇지 않으면 여러 Directory Listener 또는 Relay 시스템을 설정해야 합니다.

- **Kerberos "서버"(KDC)에 도달 가능성** - TCP/88 포트를 통해 Directory Listener 또는 Relay에서 도메인 컨트롤러에 네트워크 연결이 필요합니다. Directory Listener 또는 Relay가 도메인에 연결된 경우(Tenable에서 권장하지 않음), 이 요구 사항을 이미 충족한 상태일 것입니다. 구성된 각 Tenable Identity Exposure 포리스트는 Kerberos를 통해 서비스 계정이 있는 각 도메인에서 하나 이상의 도메인 컨트롤러와 네트워크 연결이 필요하며 각각의 연결된 도메인에서 하나 이상의 도메인 컨트롤러와 네트워크 연결이 필요합니다.

  요구 사항에 대한 자세한 내용은 네트워크 흐름 행렬 및 TLS 네트워크 행렬을 참조하십시오.

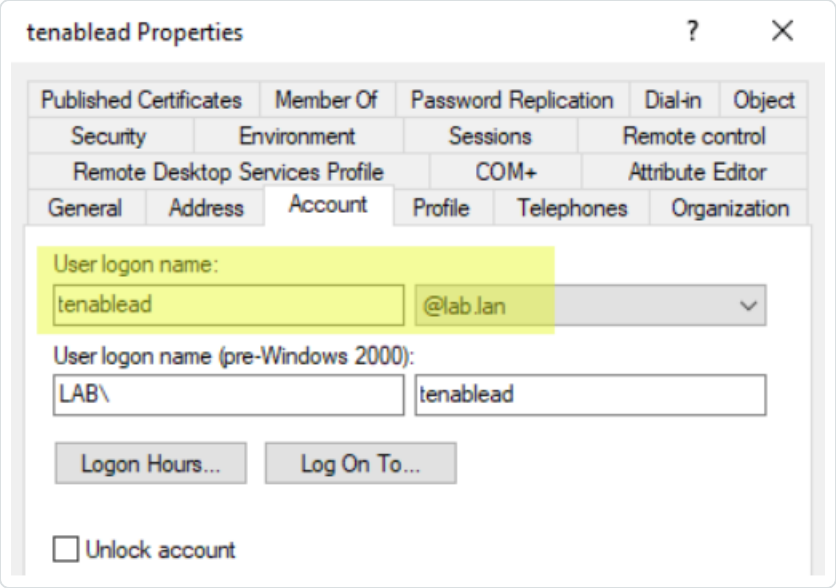
  참고: Directory Listener 또는 Relay 시스템은 도메인에 가입하지 않아도 Kerberos를 사용할 수 있습니다.

서비스 계정 및 도메인 구성

Kerberos를 사용하도록 Tenable Identity Exposure의 AD 서비스 계정 및 AD 도메인을 구성하는 방법:

1. 로그인에 UPN(User PrincipalName) 형식을 사용합니다. 이 예에서 UPN 특성은 "`tenablead@lab.lan`"입니다.

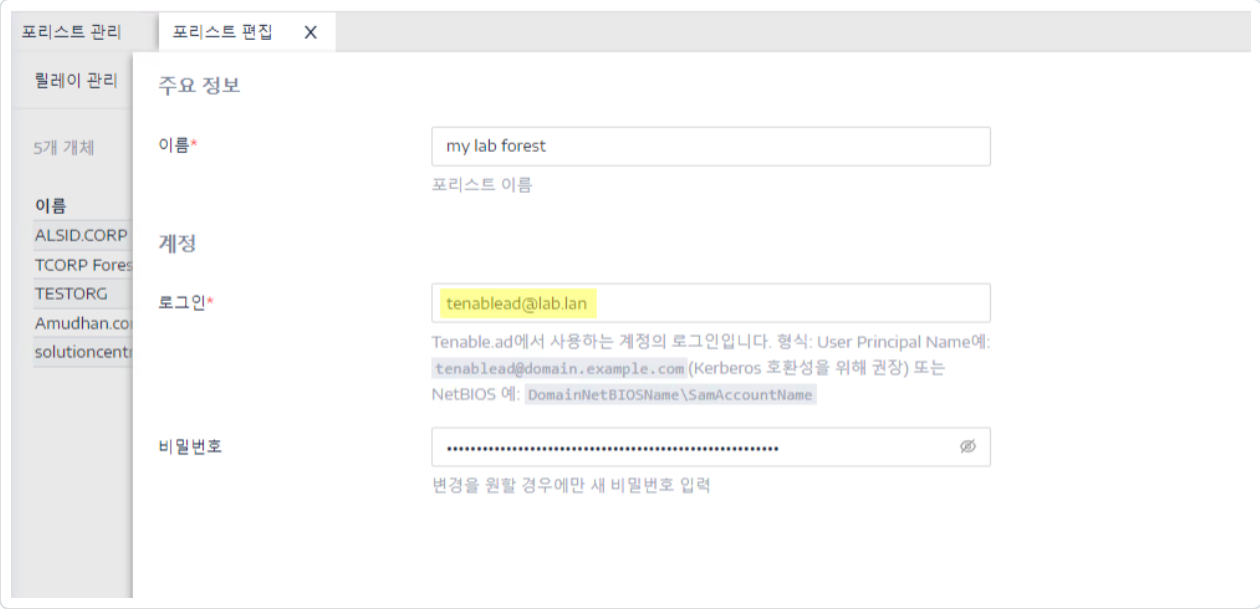
    a. 다음과 같이 서비스 계정이 포함된 포리스트의 도메인에서 UPN 속성을 찾습니다.



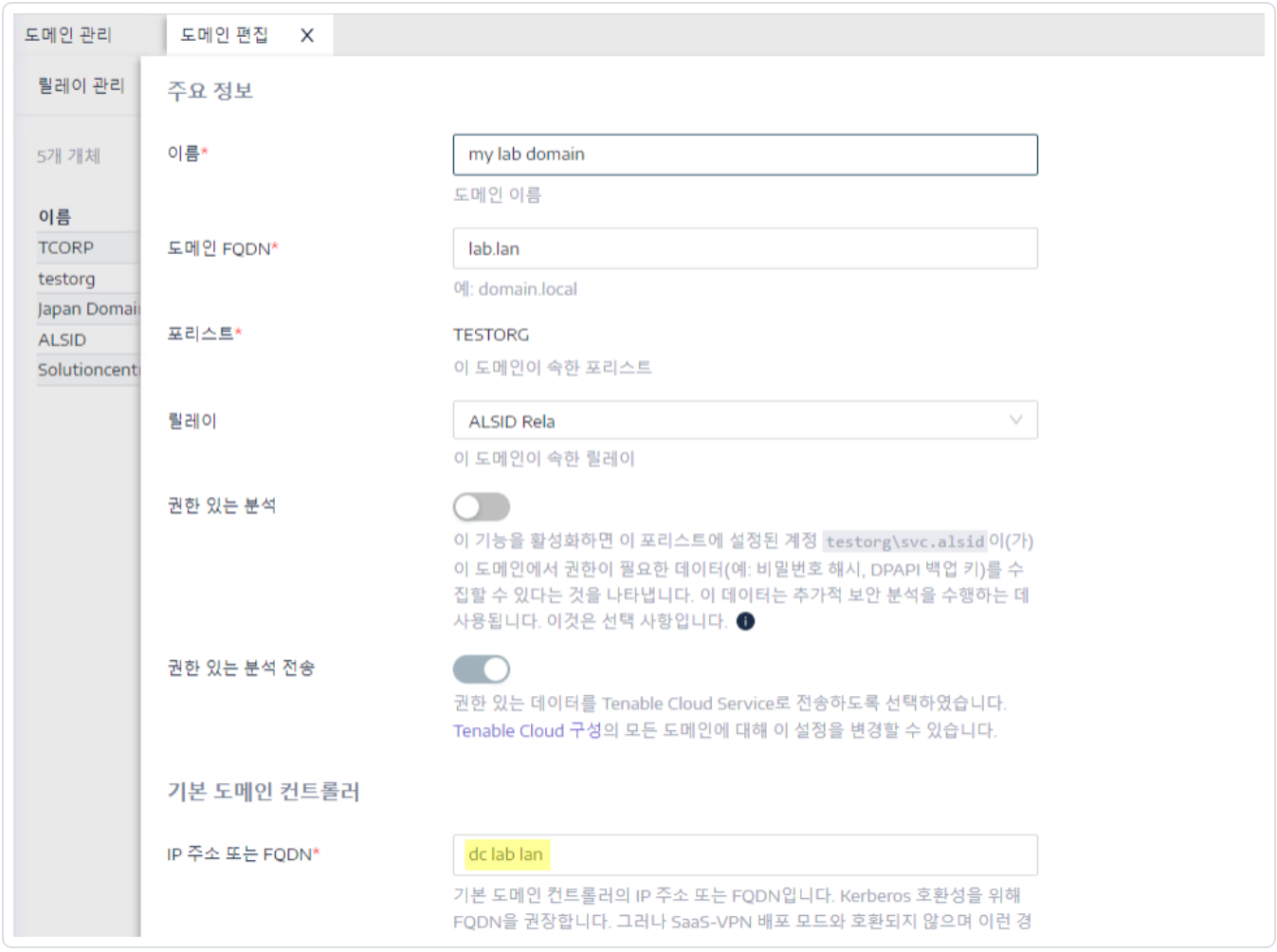

```
PS C:\Users\admin> Get-ADUser tenablead


DistinguishedName : CN=tenablead,CN=Users,DC=lab,DC=lan
Enabled           : True
GivenName         : tenablead
Name              : tenablead
ObjectClass       : user
ObjectGUID        : 70020328-b176-40d0-8a79-7948c1d4cb74
SamAccountName    : tenablead
SID               : S-1-5-21-1891480667-311803191-3341389180-22602
Surname           :
UserPrincipalName : tenablead@lab.lan
```

참고: UPN은 이메일 주소처럼 보이며 항상 그런 것은 아니지만 종종 사용자의 이메일과 동일합니다.

b. Tenable Identity Exposure의 포리스트 구성 섹션에서 다음과 같이 짧은 "`username`" 형식 또는 NetBIOS "`domain\username`" 형식 대신 이 UPN을 설정합니다.



2. 정규화된 도메인 이름(FQDN) 사용 Tenable Identity Exposure의 도메인 구성에서 기본 도메인 컨트롤러(PDC)에 대해 IP 대신 FQDN을 설정합니다.

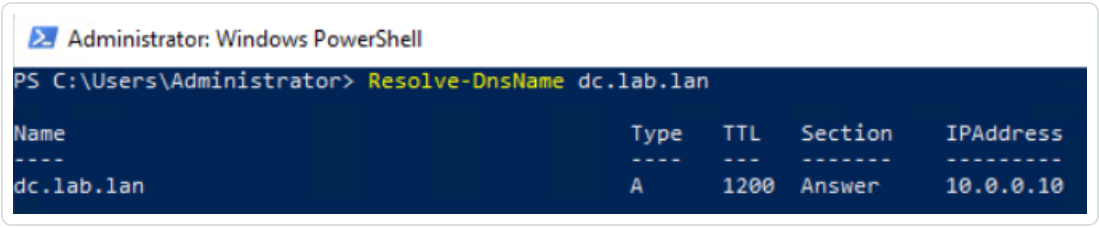


문제 해결

Kerberos가 제대로 작동하려면 몇 가지 구성 단계가 필요합니다. 그렇지 않으면 Windows에서는 또한 Tenable Identity Exposure에서도 NTLM 인증으로 자동으로 대체됩니다.

DNS

Directory Listener 또는 Relay 시스템에서 사용되는 DNS 서버가 다음과 같이 제공된 PDC FQDN을 확인할 수 있는지 확인합니다.



Kerberos

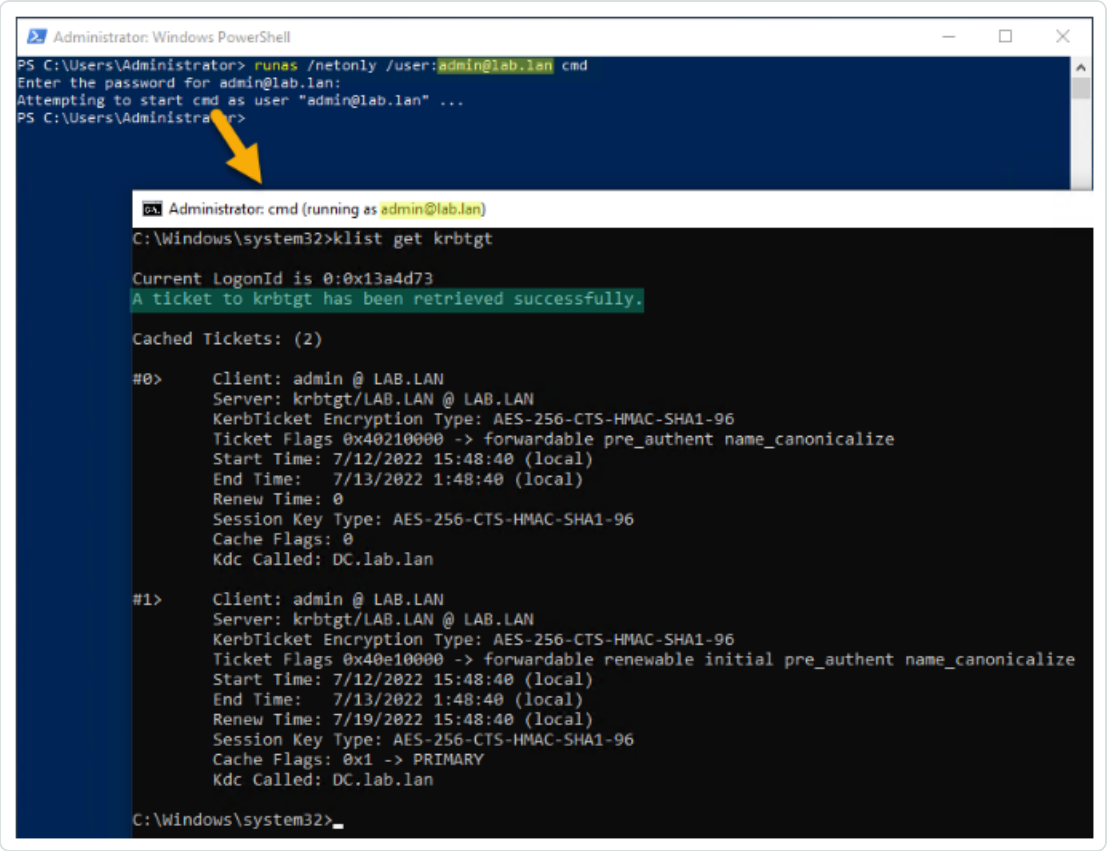
Kerberos가 Directory Listener 또는 Relay 시스템에서 실행하는 명령과 함께 작동하는지 확인하려면 다음을 수행하십시오.

1. Tenable Identity Exposure에 구성된 AD 서비스 계정이 TGT를 얻을 수 있는지 확인합니다.

    a. 명령줄 또는 PowerShell에서 "`runas /netonly /user:<UPN> cmd`"를 입력하고 비밀번호를 입력합니다. "`/netonly`" 플래그로 인해 비밀번호를 확인할 수 없으므로 비밀번호를 입력하거나 붙여넣을 때 각별히 주의하십시오.

    b. 두 번째 명령 프롬프트에서 "`klist get krbtgt`"를 실행하여 TGT 티켓을 요청합니다.

    다음 예는 성공적인 결과를 보여줍니다.

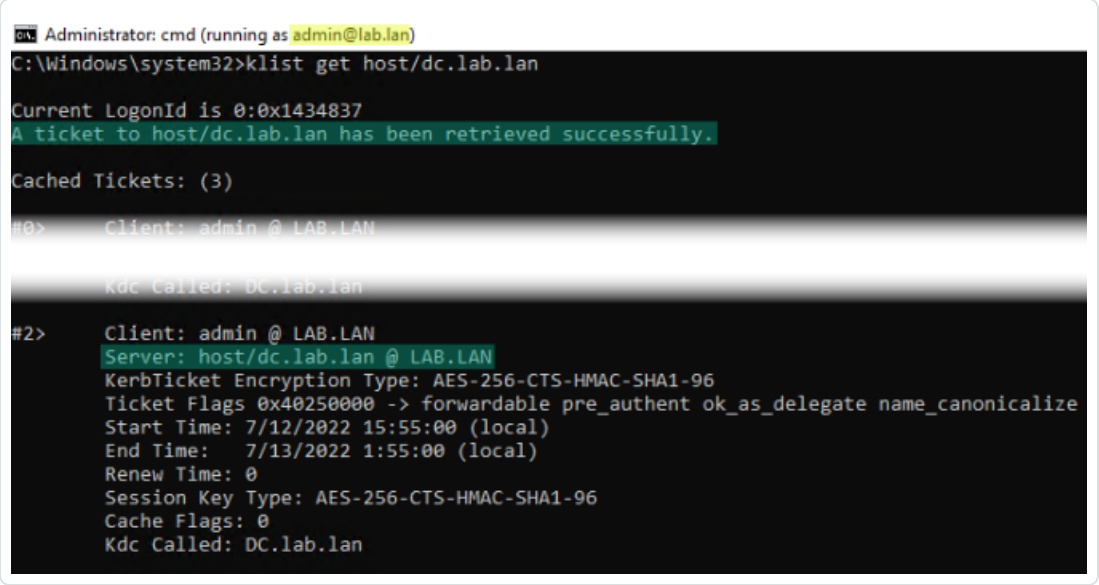


다음은 잠재적 오류 코드입니다.

- `0xc0000064`: "철자가 틀리거나 잘못된 사용자 계정으로 사용자 로그인" -> 로그인 정보를 확인하십시오(즉, UPN에서 '@' 앞 부분).
- `0xc000006a`: "철자가 틀리거나 잘못된 암호로 사용자 로그인" -> 비밀번호를 확인하십시오.
- `0xc000005e`: "현재 로그인 요청을 처리할 수 있는 로그인 서버가 없습니다." -> DNS 확인이 작동하는지 및 서버가 반환된 KDC에 접속할 수 있는지 등을 확인하십시오.
- 기타 오류 코드: 4625 이벤트와 관련된 Microsoft 설명서를 참조하십시오.

2. Tenable Identity Exposure에 구성된 도메인 컨트롤러가 서비스 티켓을 얻을 수 있는지 확인합니다. 동일한 두 번째 명령 프롬프트에서 `"klist get host/<DC_FQDN>"`(`"<DC_FQDN>"` 바꾸기)을 실행합니다.

다음 예는 성공적인 결과를 보여줍니다.



알림

라이선스 필요: 보내려는 알림의 유형에 따라 공격 지표나 위험 노출 지표 라이선스가 필요할 수 있습니다.

Tenable Identity Exposure의 알림 시스템을 이용하면 모니터링되는 Active Directory의 보안 저하 및/또는 공격을 식별하는 데 도움이 됩니다. 이것은 이메일 또는 Syslog 알림을 통해 실시간으로 취약성과 공격에 관한 분석 데이터를 푸시합니다.

- SMTP 서버 구성
- 이메일 알림
- Syslog 알림
- Syslog 및 이메일 알림 세부 정보

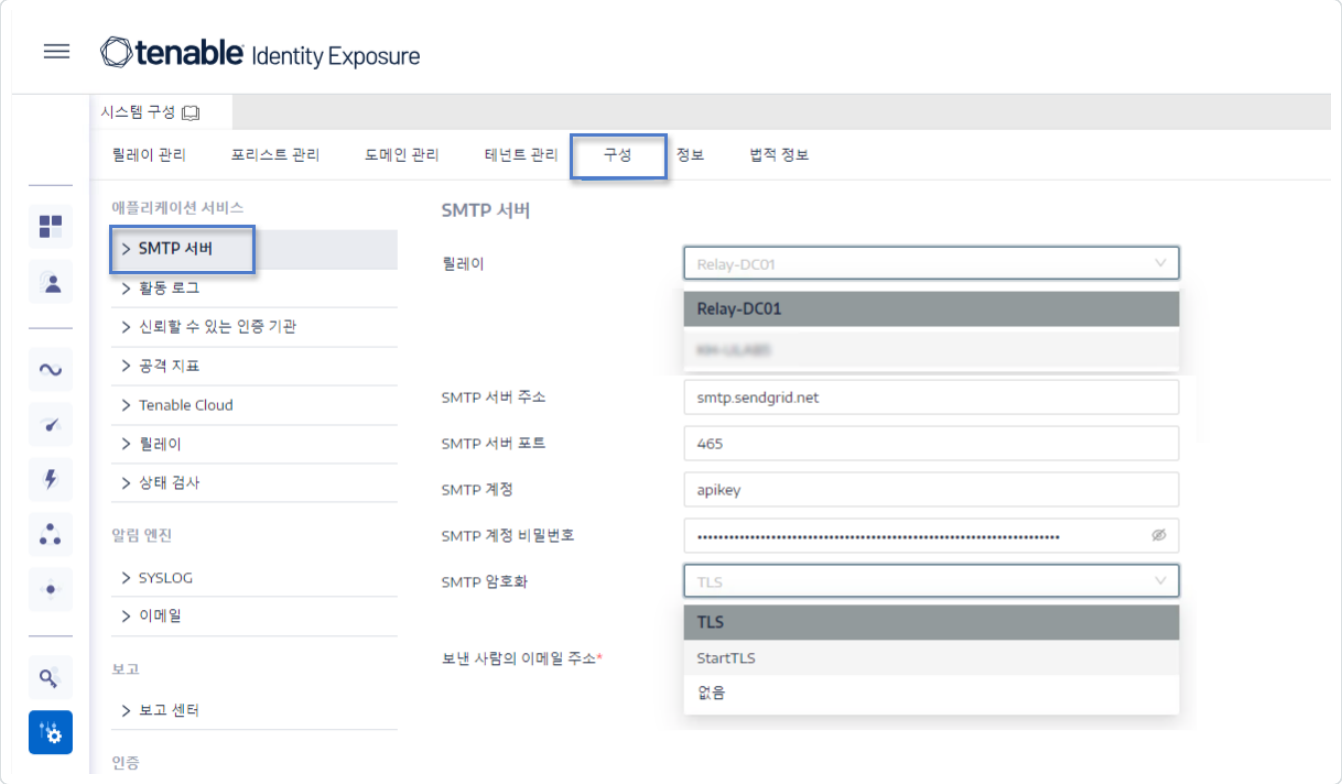
SMTP 서버 구성

알림을 보내려면 Tenable Identity Exposure에 SMTP(Simple Mail Transfer Protocol) 구성이 필요합니다.

SMTP 서버를 구성하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 클릭합니다.
2. **애플리케이션 서비스** 아래에서 **SMTP 서버**를 선택합니다.

   SMTP 서버 창이 열립니다.



3. **네트워크가 Secure Relay를 사용하는 경우: Relay** 상자에서 화살표를 클릭하여 드롭다운 목록에서 SMTP 서버와 통신할 Relay를 선택합니다.
4. 다음과 같은 정보를 입력합니다.
   - SMTP 서버 주소
   - SMTP 서버 포트

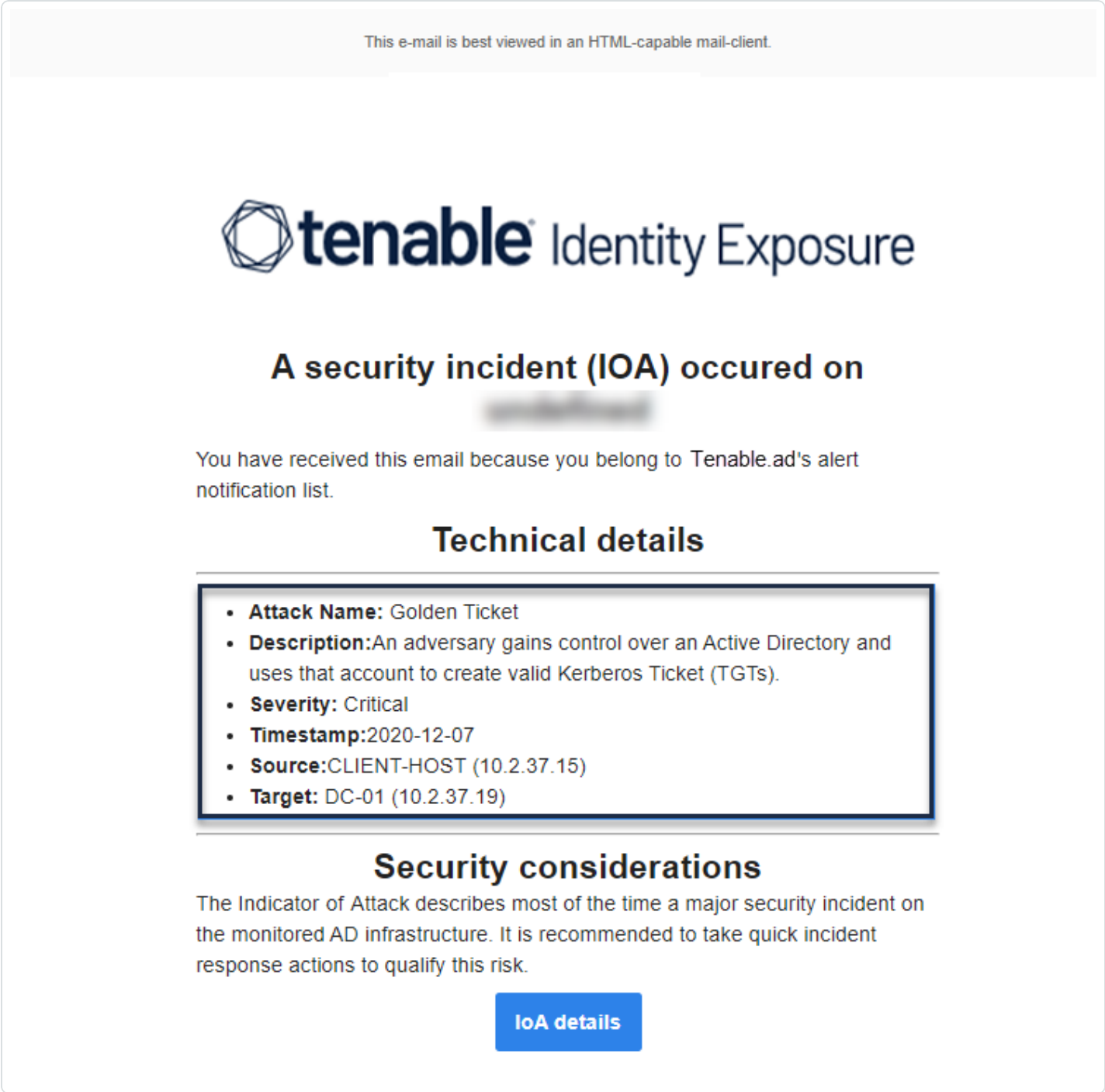
- SMTP 계정
- SMTP 계정 비밀번호

5. SMTP 암호화 상자에서 화살표를 클릭하여 드롭다운 목록에서 암호화 방법을 선택합니다.
6. **보낸 사람의 이메일 주소** 상자에 이메일을 보낼 때 Tenable Identity Exposure에서 사용할 이메일 주소를 입력합니다.
7. **저장**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 SMTP 매개 변수를 업데이트했다고 확인합니다.

이메일 알림

Tenable Identity Exposure에서는 이벤트가 특정 심각도 임계값에 도달하여 수정 작업이 필요한 경우, 자동으로 이메일 알림을 보내 사용자에게 알립니다. 다음은 이메일 알림의 예입니다.



이메일 알림을 추가하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **이메일**을 클릭합니다.
2. 오른쪽에 있는 **이메일 알림 추가** 버튼을 클릭합니다.

   이메일 알림 추가 창이 표시됩니다.
3. **기본 정보** 섹션 아래에 다음과 같은 정보를 입력합니다.
   - **이메일 주소** 상자에 알림을 받을 받는 사람의 이메일 주소를 입력합니다.
   - **설명** 상자에 받는 사람 주소에 대한 설명을 입력합니다.
4. **알림 트리거** 드롭다운 목록에서 다음 중 하나를 선택합니다.
   - **각 일탈에 대해**: Tenable Identity Exposure에서 각각의 일탈 IoE 탐지마다 알림을 보냅니다.
   - **각 공격에 대해**: Tenable Identity Exposure에서 각각의 일탈 IoA 탐지마다 알림을 보냅니다.
   - **각 상태 검사 상태 변경에 대해**: Tenable Identity Exposure에서 상태 검사 상태가 변경될 때마다 알림을 보냅니다.
5. **프로필** 상자에서 이 이메일 알림에 사용할 프로필을 클릭하여 선택합니다(해당하는 경우).
6. **최초 분석 단계에서 일탈 탐지될 때 알림 보내기**: 다음 중 하나를 수행(해당하는 경우):
   - 확인란 선택: 시스템 재부팅이 알림을 트리거하는 경우 Tenable Identity Exposure에서 대량의 이메일 알림을 보냅니다.
   - 확인란 선택 취소: 시스템 재부팅이 알림을 트리거하는 경우 Tenable Identity Exposure에서 이메일 알림을 보내지 않습니다.
7. **심각도 임계값**: 드롭다운 상자 화살표를 클릭하여 Tenable Identity Exposure에서 알림을 보낼 임계값을 선택합니다(해당하는 경우).
8. 이전에 선택한 알림 트리거에 따라:
   - **위험 노출 지표**: **각 일탈에 대해** 알림을 트리거하도록 설정한 경우, 각 심각도 옆에 있는 화살표를 클릭하여 위험 노출 지표 목록을 펼친 다음 알림을 보낼 항목을 선택합니다.
   - **공격 지표**: **각 공격에 대해** 알림을 트리거하도록 설정한 경우, 각 심각도 옆에 있는 화살표를 클릭하여 공격 지표 목록을 펼친 다음 알림을 보낼 항목을 선택합니다.

- **상태 검사 상태 변경**: **상태 검사**를 클릭하여 알림을 트리거할 상태 검사 유형을 선택한 다음, **선택 항목 필터링**을 클릭합니다.

9. **도메인** 상자를 클릭하여 Tenable Identity Exposure에서 알림을 보낼 도메인을 선택합니다.

   포리스트 및 도메인 창이 표시됩니다.

   a. 포리스트 또는 도메인을 선택합니다.

   b. **선택 항목 필터링**을 클릭합니다.

10. **구성 테스트**를 클릭합니다.

    메시지가 표시되어 Tenable Identity Exposure에서 서버에 이메일 알림을 보냈다고 확인합니다.

11. **추가**를 클릭합니다.

    메시지가 표시되어 Tenable Identity Exposure에서 이메일 알림을 만들었다고 확인합니다.

이메일 알림을 편집하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **이메일**을 클릭합니다.
2. 이메일 알림 목록에서 수정하려는 항목을 가리킨 다음 줄 끝의 ✎ 아이콘을 클릭합니다.

   이메일 알림 편집 창이 표시됩니다.
3. 이메일 알림을 추가하는 방법: 절차에 설명된 대로 필요한 부분을 수정합니다.
4. **편집**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 알림을 업데이트했음을 확인합니다.

이메일 알림을 삭제하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **이메일**을 클릭합니다.
2. 이메일 알림 목록에서 삭제하려는 항목을 가리킨 다음 줄 끝의 🗑 아이콘을 클릭합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.
3. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 알림을 삭제했음을 확인합니다.

참고 항목

- SMTP 서버 구성
- Syslog 및 이메일 알림 세부 정보

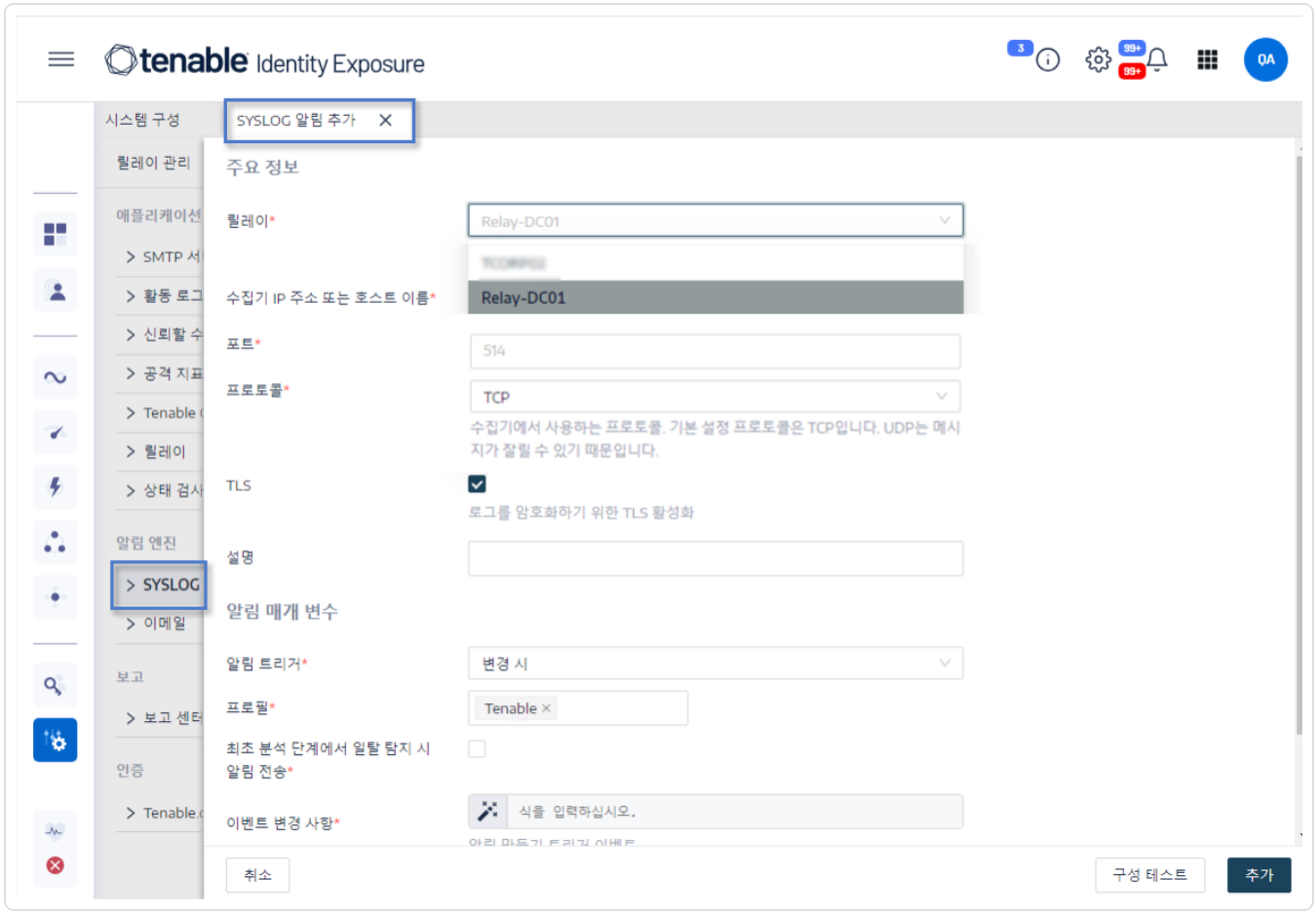
Syslog 알림

기업에 따라서 잠재적인 위협과 보안 인시던트에 관한 로그를 수집하는 데 SIEM(Security Information and Event Management)을 사용하는 경우도 있습니다. Tenable Identity Exposure에서 Active Directory와 관련한 보안 정보를 SIEM Syslog 서버로 푸시하여 알림 메커니즘을 개선할 수 있습니다.

새 Syslog 알림을 추가하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **Syslog**를 클릭합니다.
2. 오른쪽에 있는 **Syslog 알림 추가** 버튼을 클릭합니다.

   Syslog 알림 추가 창이 표시됩니다.



3. **기본 정보** 섹션 아래에 다음과 같은 정보를 입력합니다.

- **네트워크가 Secure Relay를 사용하는 경우: Relay** 상자에서 화살표를 클릭하여 드롭다운 목록에서 SIEM과 통신할 Relay를 선택합니다.
- **수집기 IP 주소 또는 호스트 이름** 상자에 알림을 받을 서버 IP 또는 호스트 이름을 입력합니다.
- **포트** 상자에 수집기의 포트 번호를 입력합니다.
- **프로토콜** 상자에서 화살표를 클릭하여 UDP 또는 TCP를 선택합니다.
  - TCP를 선택하는 경우, TLS 보안 프로토콜에서 로그를 암호화할 수 있게 하려면 **TLS** 옵션 확인란을 선택합니다.
- **설명** 상자에 해당 수집기에 대한 간략한 설명을 입력합니다.

4. **알림 트리거** 드롭다운 목록에서 다음 중 하나를 선택합니다.
   - **변경 시**: 사용자가 지정한 이벤트가 발생할 때마다 Tenable Identity Exposure에서 알림을 보냅니다.
   - **각 일탈에 대해**: Tenable Identity Exposure에서 각각의 일탈 IoE 탐지마다 알림을 보냅니다.
   - **각 공격에 대해**: Tenable Identity Exposure에서 각각의 일탈 IoA 탐지마다 알림을 보냅니다.
   - **각 상태 검사 상태 변경에 대해**: Tenable Identity Exposure에서 상태 검사 상태가 변경될 때마다 알림을 보냅니다.
5. **프로필** 상자에서 이 Syslog 알림에 사용할 프로필을 클릭하여 선택합니다(해당하는 경우).
6. **최초 분석 단계에서 일탈 탐지될 때 알림 보내기**: 다음 중 하나를 수행(해당하는 경우):
   - 확인란 선택: 시스템 재부팅이 알림을 트리거하는 경우 Tenable Identity Exposure에서 대량의 이메일 알림을 보냅니다.
   - 확인란 선택 취소: 시스템 재부팅이 알림을 트리거하는 경우 Tenable Identity Exposure에서 이메일 알림을 보내지 않습니다.
7. **심각도 임계값**: 드롭다운 상자 화살표를 클릭하여 Tenable Identity Exposure에서 알림을 보낼 임계값을 선택합니다(해당하는 경우).
8. 이전에 선택한 알림 트리거에 따라:

- **이벤트 변경**: **변경 시** 알림을 트리거하도록 설정한 경우, 이벤트 알림을 트리거할 식을 입력합니다.

  아이콘을 클릭하여 검색 마법사를 사용하거나 검색 상자에 쿼리 식을 입력한 다음 **유효성 검사**를 클릭할 수 있습니다. 자세한 내용은 Trail Flow 쿼리 사용자 지정을 참조하십시오.

- **위험 노출 지표**: **각 일탈에 대해** 알림을 트리거하도록 설정한 경우, 각 심각도 옆에 있는 화살표를 클릭하여 위험 노출 지표 목록을 펼친 다음 알림을 보낼 항목을 선택합니다.

- **공격 지표**: **각 공격에 대해** 알림을 트리거하도록 설정한 경우, 각 심각도 옆에 있는 화살표를 클릭하여 공격 지표 목록을 펼친 다음 알림을 보낼 항목을 선택합니다.

- **상태 검사 상태 변경**: **상태 검사**를 클릭하여 알림을 트리거할 상태 검사 유형을 선택한 다음, **선택 항목 필터링**을 클릭합니다.

9. **도메인** 상자를 클릭하여 Tenable Identity Exposure에서 알림을 보낼 도메인을 선택합니다.

   포리스트 및 도메인 창이 표시됩니다.

   a. 포리스트 또는 도메인을 선택합니다.

   b. **선택 항목 필터링**을 클릭합니다.

10. **구성 테스트**를 클릭합니다.

    메시지가 표시되어 Tenable Identity Exposure에서 서버에 Syslog 알림을 보냈다고 확인합니다.

11. **추가**를 클릭합니다.

    메시지가 표시되어 Tenable Identity Exposure에서 Syslog 알림을 만들었다고 확인합니다.

Syslog 알림을 편집하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **Syslog**를 클릭합니다.
2. Syslog 알림 목록에서 수정하려는 항목을 가리킨 다음 줄 끝의 아이콘을 클릭합니다.

   Syslog 알림 편집 창이 표시됩니다.

3. 새 Syslog 알림을 추가하는 방법: 절차에 설명된 대로 필요한 부분을 수정합니다.
4. **편집**을 클릭합니다.

메시지가 표시되어 Tenable Identity Exposure에서 알림을 업데이트했음을 확인합니다.

Syslog 알림을 삭제하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성** > **Syslog**를 클릭합니다.
2. Syslog 알림 목록에서 삭제하려는 항목을 가리킨 다음 줄 끝의 아이콘을 클릭합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.
3. **삭제**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 알림을 삭제했음을 확인합니다.

참고 항목

- Syslog 및 이메일 알림 세부 정보

Syslog 및 이메일 알림 세부 정보

Syslog 또는 이메일 알림을 활성화하면 Tenable Identity Exposure에서 일탈, 공격 또는 변경을 탐지하면 알림을 보냅니다.

알림 헤더

Syslog 알림 헤더(RFC-3164)는 SIEM(Security Information and Event Management)을 통합하는 솔루션의 일반적인 형식인 CEF(Common Event Format)를 사용합니다.

위험 노출 지표(IoE) 알림의 예

IoE 알림 헤더

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

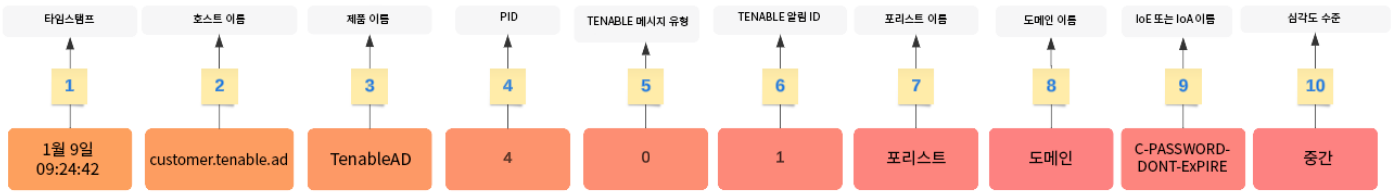
공격 지표(IoA) 알림의 예

IoA 알림 헤더

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync" "medium" "yoda.alsid.corp" "10.0.0.1" "antoinex1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_name"="MyDC"
```

알림 정보

일반 요소

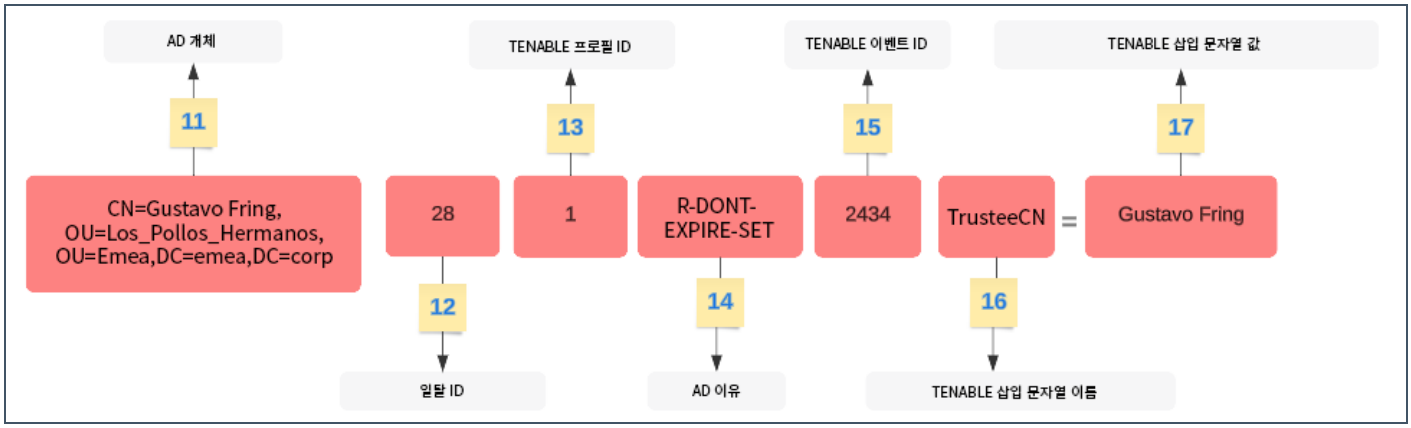


헤더 구조에는 표에 설명된 대로 다음 부분이 포함됩니다.

부분	설명
1	**타임스탬프** - 탐지 날짜. 예: "Jun 7 05:37:03"

2	**호스트 이름** – 애플리케이션의 호스트 이름입니다. 예: "customer.tenable.ad"
3	**제품 이름** - 일탈을 트리거한 제품의 이름. 예: "TenableAD", "AnotherTenableADProduct"
4	**PID** - 제품(Tenable Identity Exposure) ID. 예: [4]
5	**Tenable Msg Type** - 이벤트 소스의 식별자. 예: "0" (= 각 일탈에서), "1" (= 변경 사항에서), "2" (= 각 공격에서)
6	**Tenable Alert ID** - 해당 알림의 고유 ID. 예: "0", "132"
7	**Forest Name** - 관련 이벤트의 포리스트 이름. 예: "Corp Forest"
8	**Domain Name** - 해당 이벤트와 관련된 도메인 이름. 예: "tenable.corp", "zwx.com"
9	**Tenable Codename** - 위험 노출 지표(IoE) 또는 공격 지표(IoA)의 코드 이름. 예: "C-PASSWORD-DONT-EXPIRE", "DC Sync".
10	**Tenable Severity Level** - 관련 일탈의 심각도 수준. 예: "위험", "높음", "중간"

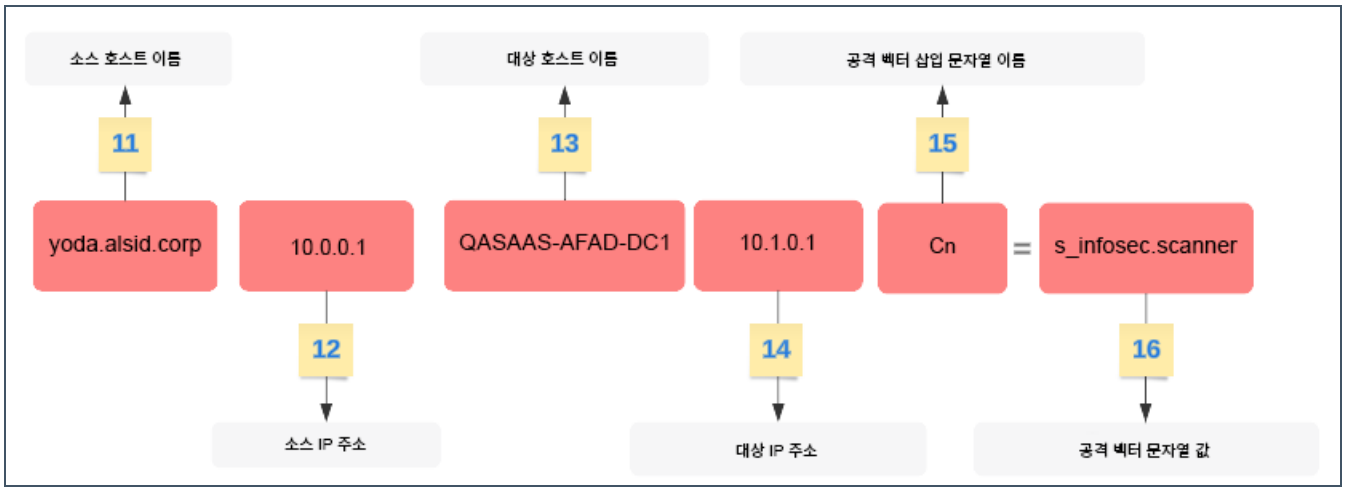
IoE 관련 요소



부분	설명
11	**AD Object** - 일탈 개체의 고유 이름. 예: "CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local"
12	**Tenable Deviance ID** - 일탈의 ID. 예: "24980", "132", "28"
13	**Tenable Profile ID** - Tenable Identity Exposure가 일탈을 트리거한 프로필의 ID. 예: "1"

	(Tenable), "2"(sec_team)
14	**AD Reason Codename** - 일탈 이유의 코드명. 예: "R-DONT-EXPIRE-SET", "R-UNCONST-DELEG"
15	**Tenable Event ID** - 일탈에서 트리거된 이벤트의 ID. 예: "40667", "28"
16	**Tenable Insertion Strings Name** - 일탈 개체에서 트리거된 특성의 이름. 예: "Cn", "useraccountcontrol", "member", "pwdlastset"
17	**Tenable Insertion Strings Name** - 일탈 개체에서 트리거된 특성의 값. 예: "s_infosec.scanner", "CN=Backup Operators,CN=Builtin,DC=domain,DC=local"

IoA 관련 요소



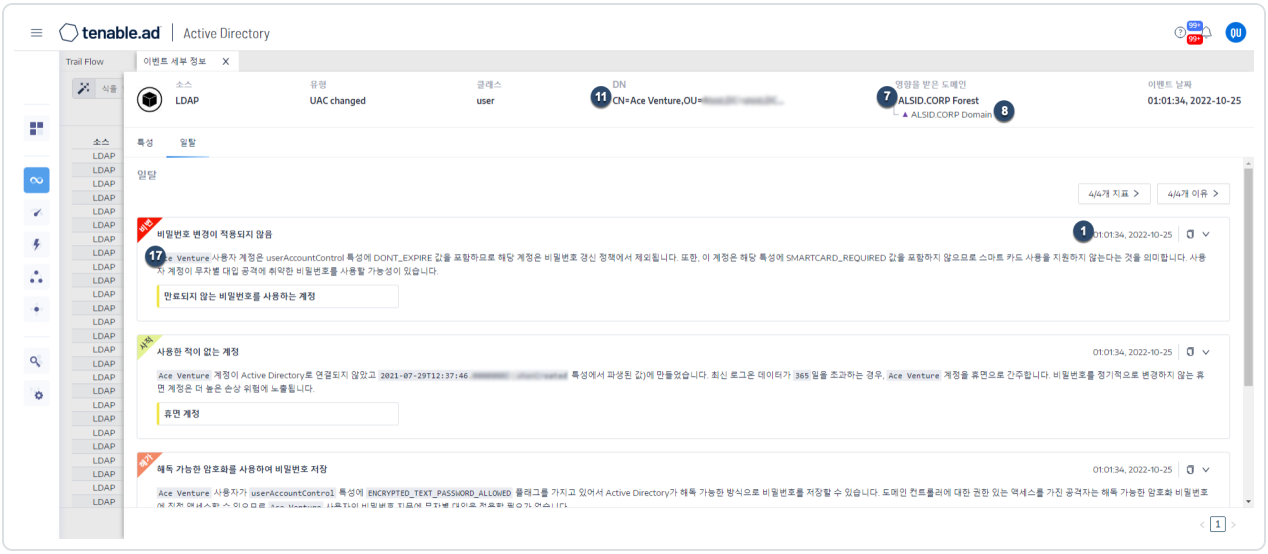
부분	설명
11	**소스 호스트 이름** – 공격하는 호스트의 호스트 이름입니다. 값은 "알 수 없음"일 수도 있습니다.
12	**소스 IP 주소** - 공격하는 호스트의 IP 주소. 값은 IPv4 또는 IPv6일 수 있습니다.
13	**대상 호스트 이름** – 공격을 받는 호스트의 호스트 이름입니다.
14	**대상 IP 주소** – 공격을 받는 호스트의 IP 주소입니다. 값은 IPv4 또는 IPv6일 수 있습니다.
15	**공격 벡터 삽입 문자열 이름** - 일탈 개체가 트리거한 특성 이름.
16	**공격 벡터 삽입 문자열 값** - 일탈 개체가 트리거한 특성의 값.

예

Trail Flow 이벤트 세부 정보

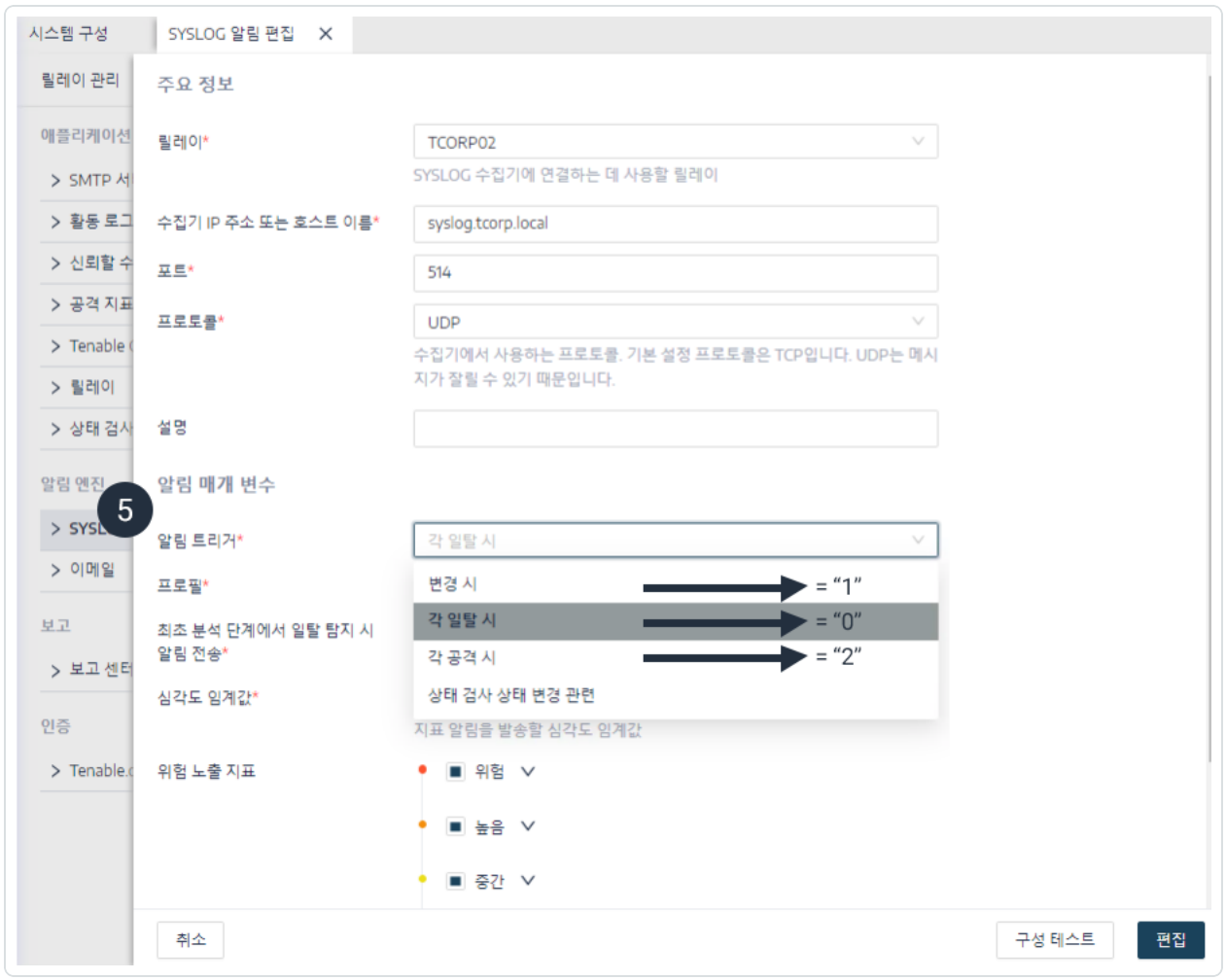
다음 예시는 다음과 같은 항목을 포함한 Trail Flow 이벤트의 세부 정보를 표시한 것입니다.

- 타임스탬프(1)
- 일탈 개체 이름(11)
- 포리스트(7) 및 도메인(8) 이름
- 일탈 개체에서 트리거된 특성의 값(17)



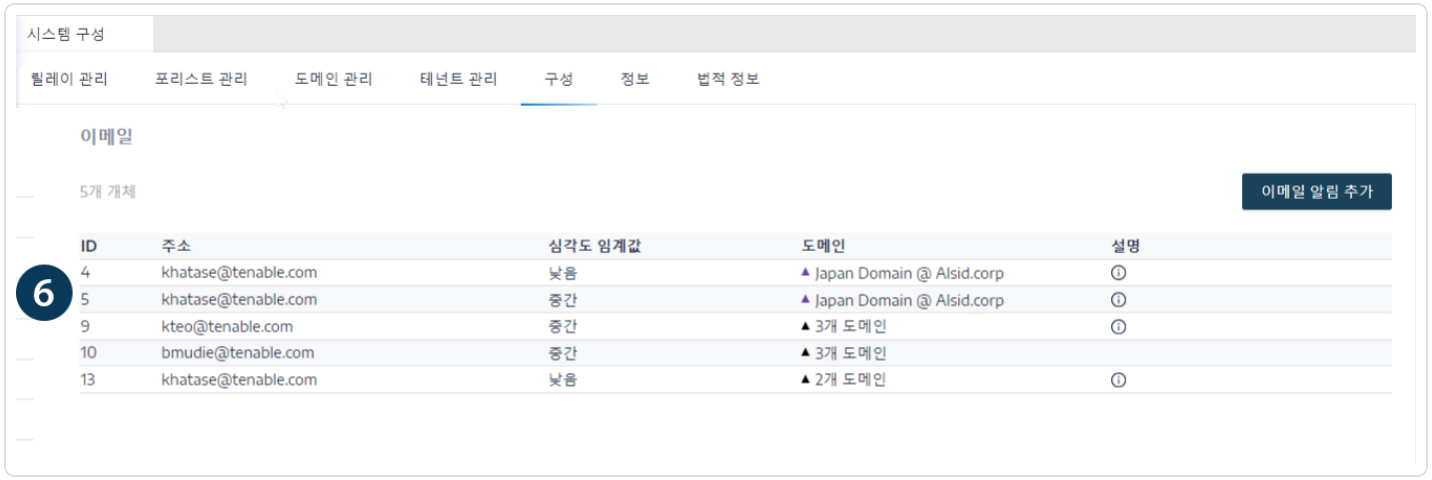
이벤트 소스

이 예시는 이벤트(5)의 소스를 보여줍니다. Syslog 구성 페이지에서 이 매개 변수를 설정합니다. 자세한 내용은 Syslog 알림을 참조하십시오.



알림 ID

이 예시는 Tenable Identity Exposure의 **시스템** > **구성** > **이메일**에 있는 구성된 이메일 주소 목록에서 볼 수 있는 알림의 고유 ID(6)를 보여줍니다.



상태 검사

Tenable Identity Exposure의 **상태 검사** 기능을 사용하면 도메인과 서비스 계정의 구성을 하나의 통합된 보기로 실시간으로 확인할 수 있으며 여기에서 드릴다운하여 인프라에 연결 또는 기타 문제를 초래하는 각종 구성 이상을 조사할 수 있습니다. 이를 통해 Tenable Identity Exposure의 원활한 작동을 위해 모든 것이 적절히 설정되었는지 확인하고 문제 해결을 위해 빠르고 정확하게 조치할 수 있으며 Tenable Identity Exposure가 효율적으로 작동할 수 있도록 최적의 구성 설정이 이루어졌음을 확신할 수 있습니다.

상태 검사는 관리 역할에는 기본적으로 표시되며 특정 사용자 역할에는 권한이 부여되면 표시됩니다. 상태 검사 상태가 변경될 때마다 Syslog 또는 이메일 알림을 생성할 수도 있습니다.

상태 검사 및 DC Sync 공격 탐지

상태 검사를 통해 Tenable Identity Exposure 서비스의 상태와 사용 가능성에 관한 중요한 정보를 얻을 수 있습니다. 상태 검사는 서비스 계정이 비밀번호 해시 및 권한 있는 분석에 사용되는 DPAPI 백업 키와 같이 중요한 정보를 수집할 수 있는지 확인합니다. Tenable은 상태 검사 보고서에서 서비스 계정에 권한 있는 분석 기능이 제대로 구성되었는지 알아보기 위해 중요한 데이터를 수집하려 시도하되, 이 기능이 사용 중이 아닌 경우 실제로는 아무것도 수집하지 않습니다. 이 프로세스 중에 DCSync 공격을 탐지하지 않도록 하기 위해 Tenable은 자동으로 DCSync 공격 지표에 대하여 제공된 서비스 계정을 허용 목록에 추가합니다.

도메인 상태

Tenable Identity Exposure에서는 각 도메인에 대해 다음과 같은 검사를 수행합니다.

- AD 도메인에 대한 인증 - LDAP 설정 및 상태, 자격 증명, SMB 액세스.
- 도메인 연결 가능성 - 동적 RPC 포트에 대한 작동 중인 연결, 연결 가능한 SMB 서버, 연결 가능한 도메인 컨트롤러 IP 주소 또는 FQDN, RPC 포트에 대한 작동 중인 연결, 연결 가능한 LDAP 서버, 연결 가능한 전역 카탈로그 LDAP 서버.
- 권한 - AD 도메인에 액세스하고 권한 있는 데이터를 수집하는 기능.
- 릴레이에 연결된 도메인 - 도메인이 릴레이 서비스에 바르게 연결되었습니다.

플랫폼 상태

Tenable Identity Exposure에서는 플랫폼 구성에 대하여 다음과 같은 검사를 수행합니다.

- 릴레이 서비스 실행 - Relay 구성이 올바른지 검사하고 문제 해결 팁 제공.
- 릴레이 버전 일관성 - Relay 버전이 Tenable Identity Exposure 버전과 일치하는지 검사.
- AD 데이터 수집기 서비스 실행 - 데이터 수집기 서비스, 브로커 및 수집기 브리지가 작동하여 데이터를 다른 서비스로 전달하는지 검사.

상태 검사에 액세스하는 방법:

1. Tenable Identity Exposure 페이지 하단 왼쪽에 있는  아이콘을 마우스로 가리키면 인프라의 전체 상태가 표시됩니다.
2. 아이콘을 클릭하여 **상태 검사** 페이지를 엽니다. **도메인 상태** 또는 **플랫폼 상태** 탭에 다음 중 하나가 표시됩니다.
    - 모든 상태 검사를 통과했다는 메시지
    - 특정 상태를 포함한 경고 또는 문제 목록:

	검사가 성공했고 정상 결과가 표시됩니다.
	검사가 실패했고 문제가 확인됩니다.
	검사는 실패했지만 해당 문제로 인해 Tenable Identity Exposure가 올바로 작동할 수 없는 것은 아닙니다. 예를 들어 데이터 수집 검사의 경우 서비스 계정이 권한 있는 데이터를 수집할 수 없으면 클라이언트 쪽의 Active Directory 구성 오류로 인해 검사가 실패하게 됩니다. 하지만 이것은 심각한 문제가 아닙니다. Tenable Identity Exposure의 이 도메인에서 권한 있는 분석 기능을 활성화하지 않았기 때문에 경고가 발생했을 뿐입니다. 하지만 권한 있는 분석을 활성화하면 검사는 즉시 실패합니다.
	종속된 검사가 실패했기 때문에 검사 결과는 알 수 없음으로 표시됩니다. 예를 들어 인증 검사에 실패한 경우, 네트워크 연결 가능성 검사를 진행할 수 없습니다.

모든 상태 검사를 표시하는 방법:

- 오른쪽에 있는 상태 검사 목록 위에서 **성공한 검사 표시** 토글을 클릭하여 사용 설정하여 Tenable Identity Exposure에서 수행한 모든 검사를 다음과 같은 정보와 함께 목록으로 표시합니다.
    - 상태 검사 이름
    - 상태(통과, 실패, 실패했지만 차단 안 함, 알 수 없음)
    - 영향을 받은 도메인 및 그와 연결된 포리스트(도메인 상태 검사만 해당)
    - 마지막으로 검사를 수행한 시간
    - 검사가 이 상태로 유지된 기간

상태 검사 페이지를 새로 고치는 방법:

- Tenable Identity Exposure에서는 정기적으로 상태 검사를 수행하지만, 결과를 실시간으로 페이지에 업데이트하지는 않습니다. 결과 목록을 새로 고치려면  를 클릭하십시오.

상태 검사 유형 또는 도메인 기준으로 결과를 필터링하는 방법:

1. 오른쪽에 있는 상태 검사 목록 위에서 **n/n 상태 검사** 또는 **n/n 도메인**(도메인 상태만 해당)을 클릭합니다.

   상태 검사 또는 **포리스트 및 도메인** 창이 열립니다.
2. 상태 검사 유형 또는 포리스트/도메인(해당하는 경우)을 선택하고 **선택 항목 필터링**을 클릭합니다.

각 상태 검사에 대한 자세한 정보를 찾기 위해 드릴다운하는 방법:

1. 상태 검사 목록에서 상태 검사 이름을 하나 클릭하거나 줄 끝에 있는 파란색 화살표(→)를 클릭합니다.

   세부 정보 창이 열려 검사에 대한 설명과 관련 세부 정보 목록이 표시됩니다.

상태 검사 이름	유형	검사 설명	이유
도메인 도달 가능성	도메인	AD 도메인과 연결을 설정할 수 있음	• IP-UNREACHABLE R-LDAP-GLOBAL-CATALOG-

			UNREACHABLE • LDAP-SERVER-UNREACHABLE • SMB-SERVER-UNREACHABLE • DYNAMIC-RPC-CONNECTION-NOT-WORKING • RPC-CONNECTION-NOT-WORKING
AD 도메인에 인증	도메인	AD 도메인에 인증할 수 있음	• INCORRECT-CREDENTIALS • LDAP-SERVER-BUSY • LDAP-SERVER-UNAVAILABLE • LDAP-SERVER-ACCESS-DENIED • SMB-SERVER-ACCESS-DENIED
AD 도메인 데이터를 수집할 권한	도메인	AD 도메인 데이터를 수집할 수 있음	• MISSING-PERMISSIONS-PRIVILEGED-DATA
AD 컨테이너에 액세스하는 권한	도메인	AD 컨테이너에 액세스할 수 있음	• MISSING-PERMISSIONS-DELETED-OBJECTS-ACCESS • MISSING-PERMISSIONS-PASSWORD-SETTINGS-ACCESS
도메인이 릴레이에 연결됨	도메인	도메인이 릴레이에 연결됨	• LINKED-TO-RELAY-DOWN
릴레이 서비스 작	플랫	릴레이가 예상대로	• RELAY-DOWN

동	폼	작동 중	
릴레이 서비스 버전	플랫폼	릴레이 버전이 제품과 일치함	• VERSION-MISMATCH
AD 데이터 수집기 작동	플랫폼	AD 데이터 수집기가 예상대로 작동 중	• DATA-COLLECTOR-SERVICE-DOWN • DATA-COLLECTOR-BRIDGE-DOWN • BROKER-DOWN

2. 세부 정보 줄 끝의 화살표를 클릭하여 확장하면 해당 결과에 관한 자세한 정보가 표시됩니다.

상태 검사 상태 아이콘을 숨기는 방법:

기본적으로, Tenable Identity Exposure에서는 화면 왼쪽 하단에 상태 검사 상태 아이콘을 표시합니다.

1. Tenable Identity Exposure에서 왼쪽 탐색 모음의 **시스템**으로 이동하여 **구성** 탭을 선택합니다.

   아니면 상태 검사 페이지의 오른쪽 상단에 있는 ⋯를 클릭한 다음 **구성**을 선택해도 됩니다.

2. **애플리케이션 서비스**에서 **상태 검사**를 선택합니다.
3. **전역 상태 검사 상태 표시** 토글을 클릭하여 사용 중지로 설정합니다.

   Tenable Identity Exposure에서 화면 왼쪽 하단의 상태 검사 아이콘을 숨깁니다.

사용자 역할에 상태 검사 권한을 할당하는 방법:

1. Tenable Identity Exposure에서 왼쪽 탐색 모음의 **계정**으로 이동하여 **역할 관리** 탭을 선택합니다.
2. 역할 목록에서 사용자 역할을 선택한 다음 줄 끝의 ✎를 클릭합니다.

   역할 편집 창이 열립니다.

3. **시스템 구성 엔터티** 탭을 선택합니다.
4. **상태 검사** 엔터티를 선택하고 권한 토글을 클릭하여 **권한 없음**에서 **부여됨**으로 바꿉니다.

5. **적용 및 닫기**를 클릭합니다.

권한에 관한 자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

상태 검사 상태 변경에 대한 알림을 설정하는 방법:

1. Tenable Identity Exposure에서 왼쪽 탐색 모음의 **시스템**으로 이동하여 **구성** 탭을 선택합니다.

   또는 상태 검사 페이지의 오른쪽 상단에 있는 ⋯를 클릭한 다음 **알림**을 선택해도 됩니다.

2. **알림 엔진**에서 **Syslog** 또는 **이메일**을 선택합니다.
3. **Syslog 알림 추가** 또는 **이메일 알림 추가**를 클릭합니다.

   새 창이 열립니다. 전체 절차는 알림를 참조하십시오.

4. **알림 매개 변수** 아래 **알림 트리거** 상자의 드롭다운 메뉴에서 **상태 검사 상태 변경 관련**을 선택합니다.
5. **상태 검사** 상자의 화살표를 클릭하여 알림을 트리거할 상태 검사 유형을 선택한 다음 **선택 항목 필터링**을 클릭합니다.
6. **추가**를 클릭합니다.

보고 센터

Tenable Identity Exposure의 **보고 센터**에서는 조직 내 주요 이해 관계자에게 중요한 데이터를 보고서 형식으로 내보낼 수 있게 해주는 유용한 기능을 제공합니다. 보고 센터를 이용하면 미리 정의된 목록에서 보고서를 만들 수 있으므로 효율적이고 원활한 프로세스를 보장합니다.

관리자는 최대 한 분기까지 보고 기간을 유연하게 정해 여러 사용자를 대상으로 다양한 유형의 보고서를 작성할 수 있습니다. Tenable Identity Exposure에서 입수한 중요한 ID 데이터를 공유함으로써 조직은 위험을 선제적으로 완화하고 잠재적인 ID 기반 공격을 파악할 수 있습니다.

보고서를 다운로드할 수 있도록 사용자는 URL을 포함한 이메일을 받습니다. 이 URL을 통해 페이지로 이동하면 해당 사용자가 관리자에게서 받은 보고서 액세스 키를 입력합니다. 보고서는 30일간 다운로드할 수 있으며 이 기간이 지나면 Tenable Identity Exposure에서 보고서를 삭제합니다. 사용자는 지정된 기간 동안 Tenable Identity Exposure에서 새 보고서를 만들어 이전 버전을 덮어쓰기 전에 보고서를 다운로드해야 합니다.

보고 센터에 액세스하는 방법:

1. Tenable Identity Exposure에서 **시스템** > **구성**을 선택합니다.
2. **보고** 아래의 **보고 센터**를 클릭합니다.

   창이 열려 구성된 보고서 및 그와 연결된 정보(예: 보고서 이름, 유형, 도메인, 프로필, 기간, 반복, 받는 사람 이메일 등)가 포함된 목록이 표시됩니다.

보고서를 만드는 방법:

1. **보고 센터** 창에서 **보고서 만들기**를 클릭합니다.

   보고서 구성 창이 열립니다.
2. **보고서 유형** 아래에서 다음과 같은 정보를 작성합니다.
   a. **보고서 유형**에서 **일탈** 또는 **공격** 중 하나를 선택합니다.
   b. **지표**에서 **n/n 지표**를 클릭하여 **위험 노출 지표**(일탈인 경우) 또는 **공격 지표**(공격인 경우) 중 하나를 선택하고 **선택 항목 필터링**을 클릭합니다.
   c. **도메인**에서 **n/n 도메인**을 클릭하여 보고서의 포리스트나 도메인을 선택한 다음 **선택 항**

목 필터링을 클릭합니다.

d. **프로필**에서 화살표를 클릭하여 드롭다운 메뉴에서 프로필을 하나 선택합니다.

3. **보고서 이름**에 보고서의 이름을 입력합니다.
4. **생성 매개 변수** 아래에서 다음과 같은 설정을 선택합니다.

   a. **데이터 기간** - 보고서는 지금보다 앞선 기간을 포함합니다(예를 들어 전날, 전 주, 전달 또는 전 분기).

   b. **반복** - Tenable Identity Exposure에서 사용자가 정의한 각 기간에 대하여 새 보고서를 생성합니다. 화살표를 클릭하여 드롭다운 메뉴에서 해당하는 값을 선택하십시오.

   c. **표준 시간대** - 보고서와 관련된 표준 시간대입니다.

5. **받는 사람** 아래에서 **이메일 추가**를 클릭하고 받는 사람의 이메일 주소를 입력합니다. 필요에 따라 받는 사람을 얼마든지 추가해도 됩니다.

   보고서 수신자의 이메일을 설정하는 방법에 대한 자세한 내용은 SMTP 서버 구성을 참조하십시오.

6. **보고서 만들기**를 클릭합니다.

사용자에게 보고서 다운로드를 허용하는 방법:

- **보고 센터** 창 맨 위의 **보고서 액세스 키**에서 를 클릭하여 복사합니다. 받는 사람에게 보낸 이메일의 링크에서 보고서를 다운로드하려면 이 액세스 키가 필요합니다. 이 키는 모든 사용자와 보고서마다 고유합니다.
- 필요한 경우, 를 클릭하여 새 액세스 키를 생성합니다.

  주의: 액세스 키를 새로 생성하면 이전 키를 사용할 수 없게 됩니다. 새 액세스 키만 기존 보고서에 대한 액세스 권한을 부여할 수 있습니다.

보고서 구성을 편집하는 방법:

1. 보고서 목록에서 보고서를 하나 선택하고 줄 끝에 있는 를 클릭하여 **보고서 구성** 창을 엽니다.
2. 필요에 따라 수정합니다.

3. **저장**을 클릭합니다.

보고서를 삭제하는 방법:

1. 보고서 목록에서 보고서를 하나 선택하고 줄 끝에 있는 🗑를 클릭하여 삭제합니다.

   메시지가 표시되어 삭제할 것인지 확인을 요청합니다.

2. **삭제**를 클릭합니다.

   이 보고서 구성과 연결된 가장 최근에 생성한 보고서를 더 이상 다운로드할 수 없게 됩니다.

역할에 권한을 부여하는 방법:

- **권한 관리**의 **데이터 엔터티** > **보고서**에서 관리자가 전체 또는 특정 보고서 구성을 만들거나 읽거나 편집하는 권한을 사용자 역할에 부여할 수 있습니다.

  자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

참고 항목

- 위젯

Microsoft Entra ID 지원

Tenable Identity Exposure에서는 Active Directory 외에 Microsoft Entra ID(이전의 Azure AD, 즉 AAD)도 지원하여 조직의 ID 범위를 확장합니다. 이 기능은 Microsoft Entra ID 관련 위험에 초점을 맞춘 새 위험 노출 지표를 활용합니다.

Microsoft Entra ID를 Tenable Identity Exposure에 통합하려면 이 온보딩 절차를 정확히 따르십시오.

1. 필수 조건을 충족합니다.
2. 권한을 확인합니다.
3. Microsoft Entra ID 설정 구성
4. Microsoft Entra ID 지원 활성화
5. 테넌트 스캔 활성화

필수 조건

Microsoft Entra ID 지원 기능을 사용하려면 **Tenable Vulnerability Management 계정**이 있어야 합니다. 이 계정을 사용하면 Microsoft Entra ID에 대하여 Tenable 스캔을 구성하고 스캔 결과를 수집할 수 있습니다.

권한

Microsoft Entra ID를 지원하려면 Microsoft Entra ID에서 사용자, 그룹, 애플리케이션, 서비스 주체, 역할, 권한, 정책, 로그 등과 같은 데이터를 수집해야 합니다. 이 데이터는 Microsoft 권장 사항에 따라 Microsoft Graph API 및 서비스 주체 자격 증명을 사용하여 수집합니다.

- Microsoft Graph에서 **테넌트 전반에 걸친 관리자 동의를 부여할 권한이 있는 사용자**로서 Microsoft Entra ID에 로그인해야 합니다(Microsoft에 따른 전역 관리자 또는 권한 있는 역할 관리자 역할(또는 적절한 권한을 가진 각종 사용자 지정 역할)이 있어야 함).
- Microsoft Entra ID의 구성과 데이터 시각화에 액세스하려면 **Tenable Identity Exposure 사용자 역할**에 적절한 권한이 있어야 합니다. 자세한 내용은 역할에 대한 권한 설정을 참조하십시오.

Microsoft Entra ID 설정 구성

다음과 같은 절차(Microsoft 빠른 시작: Microsoft ID 플랫폼에 애플리케이션 등록 문서에서 수정)를 사용해 Microsoft Entra ID의 필수 설정을 모두 구성하십시오.

1. **애플리케이션 만들기:**

   a. Azure 관리자 포털에서 **앱 등록** 페이지를 엽니다.

   b. **+ 신규 등록**을 클릭합니다.

   c. 애플리케이션에 이름을 지정합니다(예: "Tenable Identity Collector"). 다른 옵션의 경우, 기본값을 그대로 두어도 됩니다.

   d. **등록**을 클릭합니다.

   e. 새로 생성된 이 앱의 개요 페이지에서 "애플리케이션(클라이언트) ID"와 "디렉터리(테넌트) ID"를 기록해 둡니다.

2. **애플리케이션에 자격 증명 추가:**

   a. Azure 관리자 포털에서 **앱 등록** 페이지를 엽니다.

   b. 만든 애플리케이션을 클릭합니다.

   c. 왼쪽 메뉴에서 **인증서 및 암호**를 클릭합니다.

   d. **+ 새 클라이언트 암호**를 클릭합니다.

   e. **설명** 상자에 이 암호에 실용적인 이름을 부여하고 정책에 부합하는 **만료** 값을 입력합니다. 만료 날짜가 가까워지면 이 암호를 갱신해야 합니다.

   f. Azure는 이 값을 한 번만 표시하므로 암호 값을 안전한 위치에 저장하십시오. 잃어버린 경우 다시 만들어야 합니다.

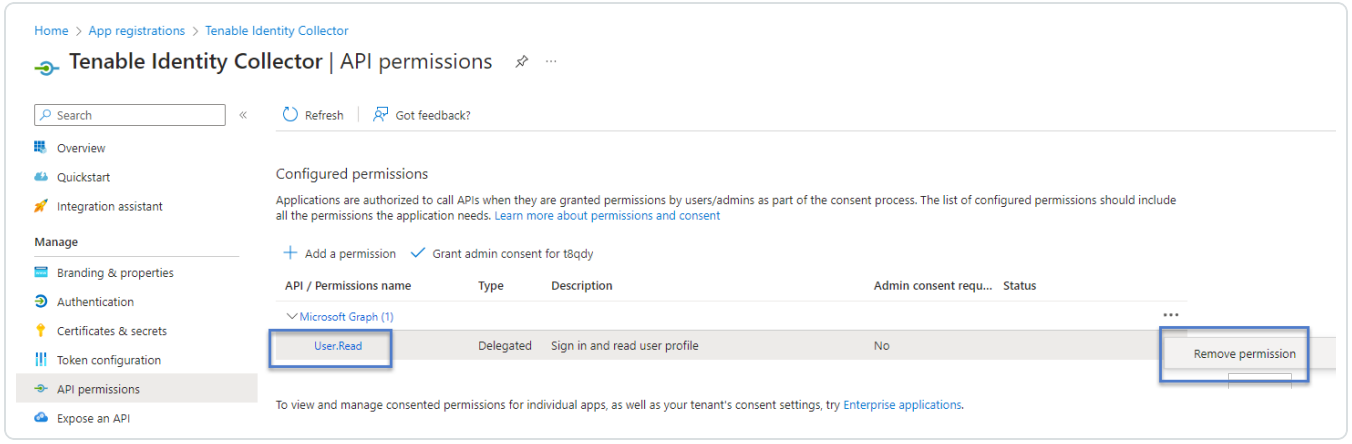
3. **애플리케이션에 권한 할당:**

   a. Azure 관리자 포털에서 **앱 등록** 페이지를 엽니다.

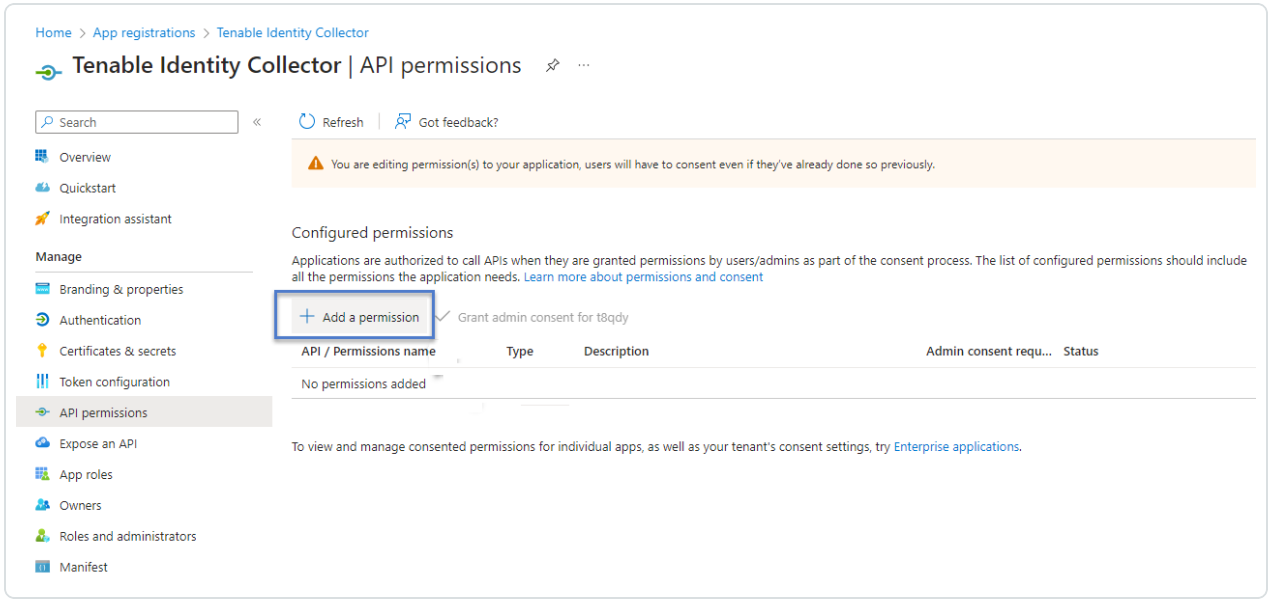
   b. 만든 애플리케이션을 클릭합니다.

   c. 왼쪽 메뉴에서 **API 권한**을 클릭합니다.

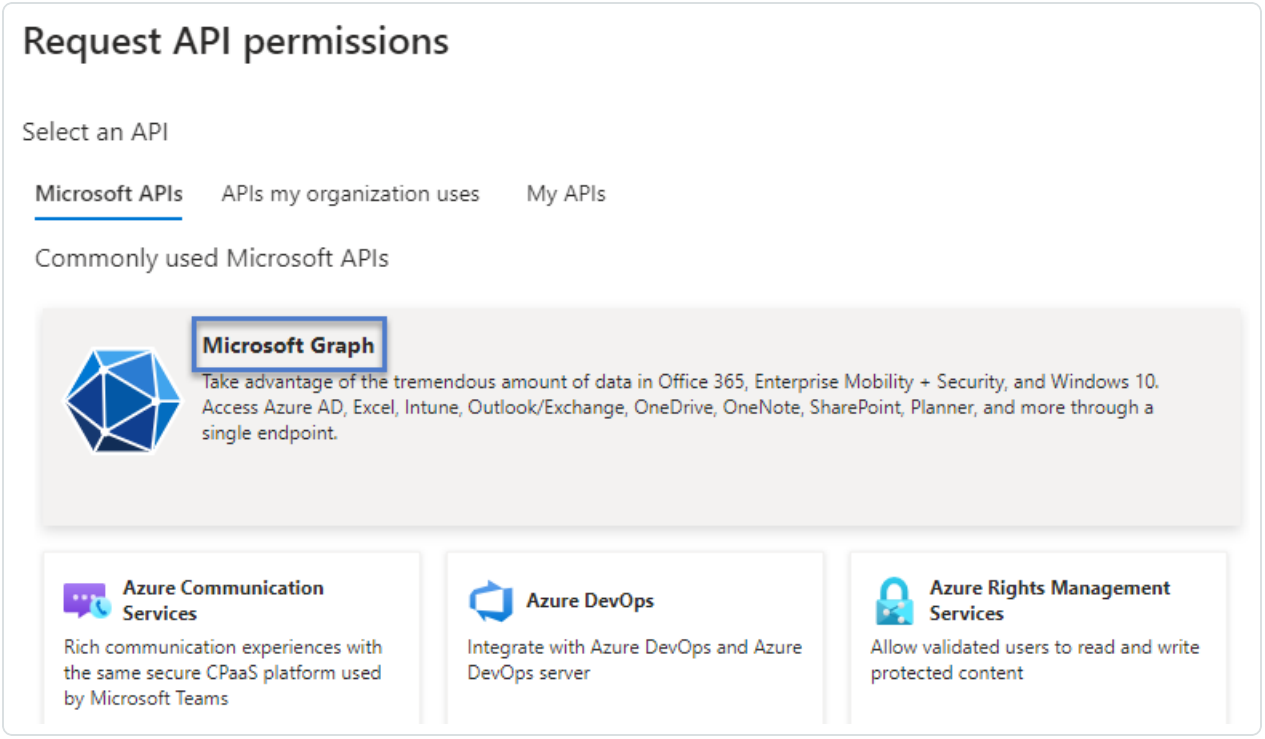
   d. 기존 `User.Read` 권한을 제거합니다.



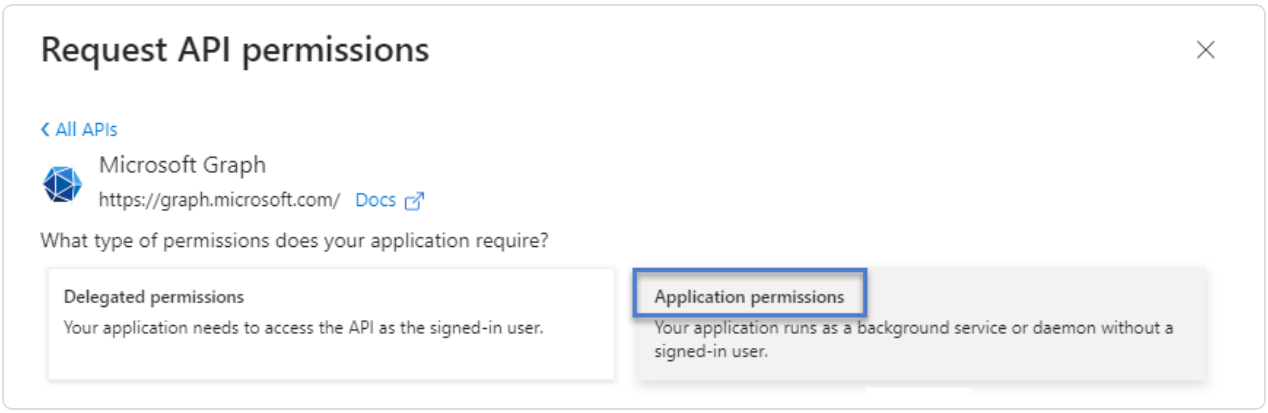
e. **+ 권한 추가**를 클릭합니다.



f. **Microsoft Graph**를 선택합니다.



g. **애플리케이션 권한**을 선택합니다("위임된 권한" 아님).



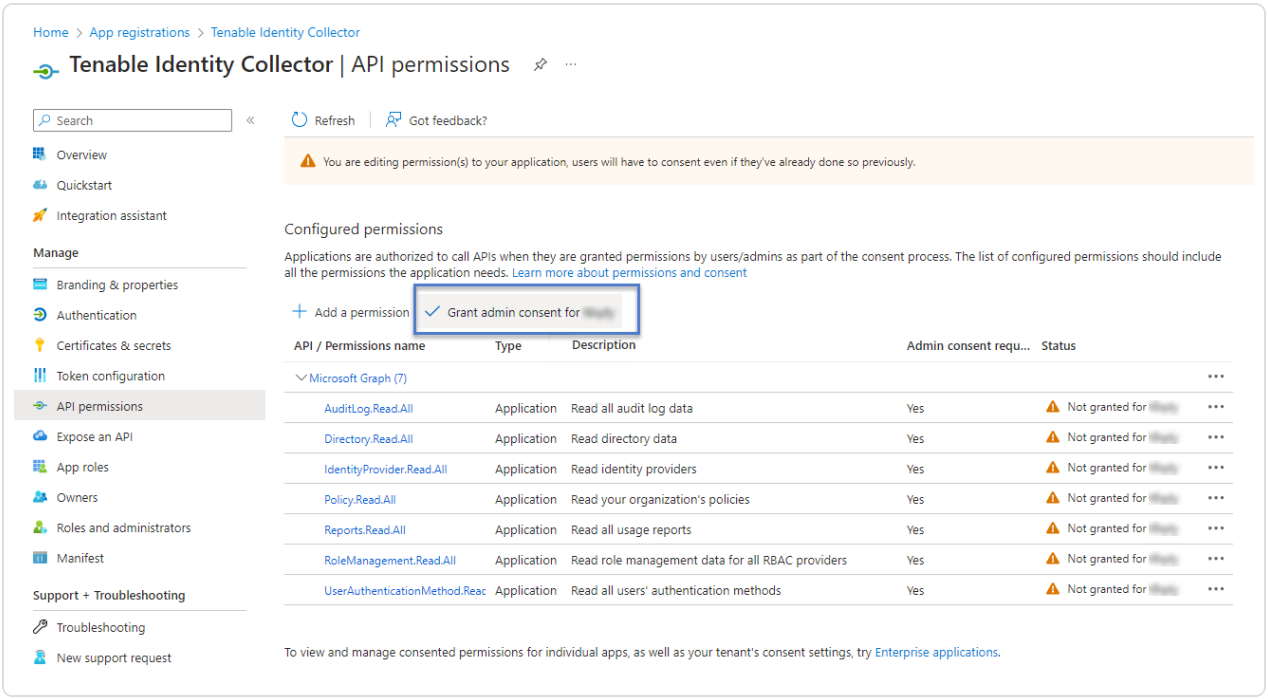
h. 목록 또는 검색창을 사용하여 다음과 같은 권한을 찾아 모두 선택합니다.

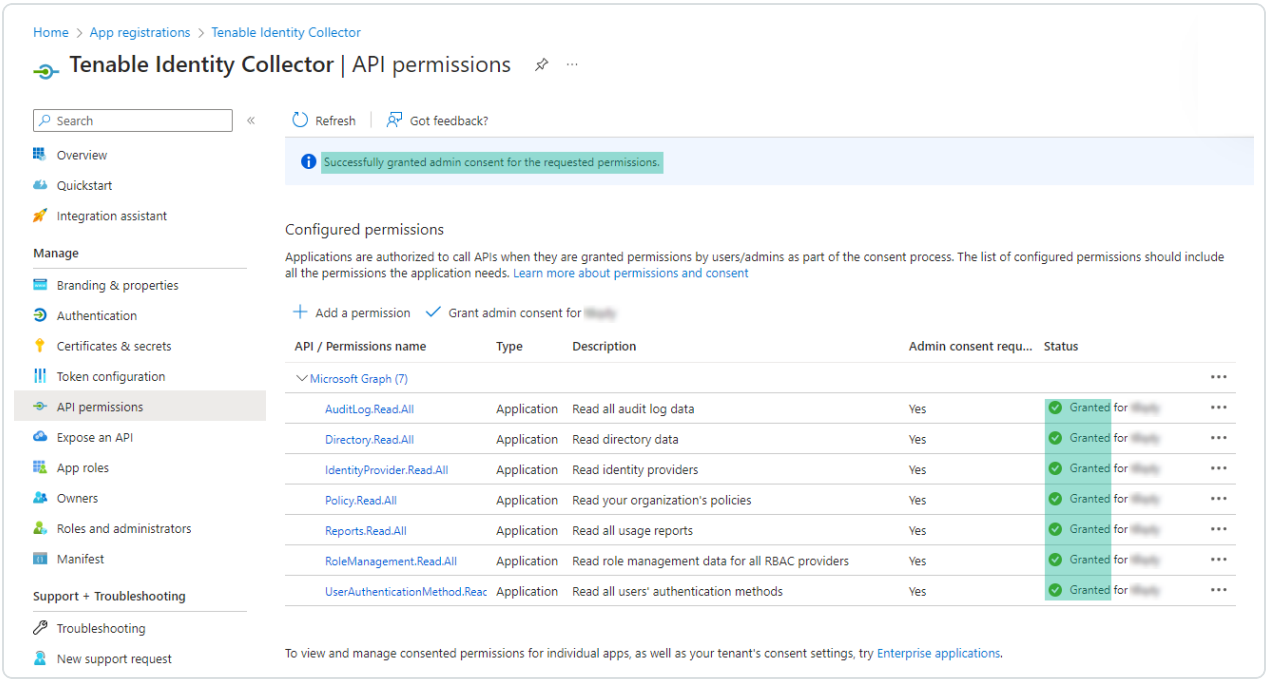
- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`

- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. **권한 추가**를 클릭합니다.

j. **<tenant name>에 관리자 동의 부여**를 클릭하고 **예**를 클릭하여 확인합니다.





4. Microsoft Entra ID에서 모든 필수 설정을 구성한 다음:

    a. Tenable Vulnerability Management에 'Microsoft Azure' 유형의 새 자격 증명을 만듭니다.

    b. "키" 인증 방법을 선택하고 이전 절차에서 가져온 값(테넌트 ID, 애플리케이션 ID 및 클라이언트 암호)을 입력합니다.

Microsoft Entra ID 지원 활성화

지원을 활성화하는 방법:

참고: 이 기능을 활성화하려면 액세스와 암호 키를 생성한 Tenable Cloud 사용자에게 Tenable Identity Exposure 라이선스가 참조하는 Tenable Cloud 컨테이너의 관리 권한이 있어야 합니다. 자세한 내용은 Tenable Identity Exposure 라이선싱을 참조하십시오.

1. Tenable Identity Exposure에서 왼쪽 탐색 메뉴의 시스템 아이콘  을 클릭합니다.
2. **구성** 탭을 클릭합니다.

    구성 페이지가 열립니다.
3. 애플리케이션 서비스 아래에서 **Tenable Cloud**를 클릭합니다.
4. **Microsoft Entra ID 활성화** 지원에서 토글을 클릭하여 사용 설정합니다.
5. 이전에 Tenable Cloud에 로그인한 적이 없는 경우, 링크를 클릭하여 로그인 페이지로 이동합니다.

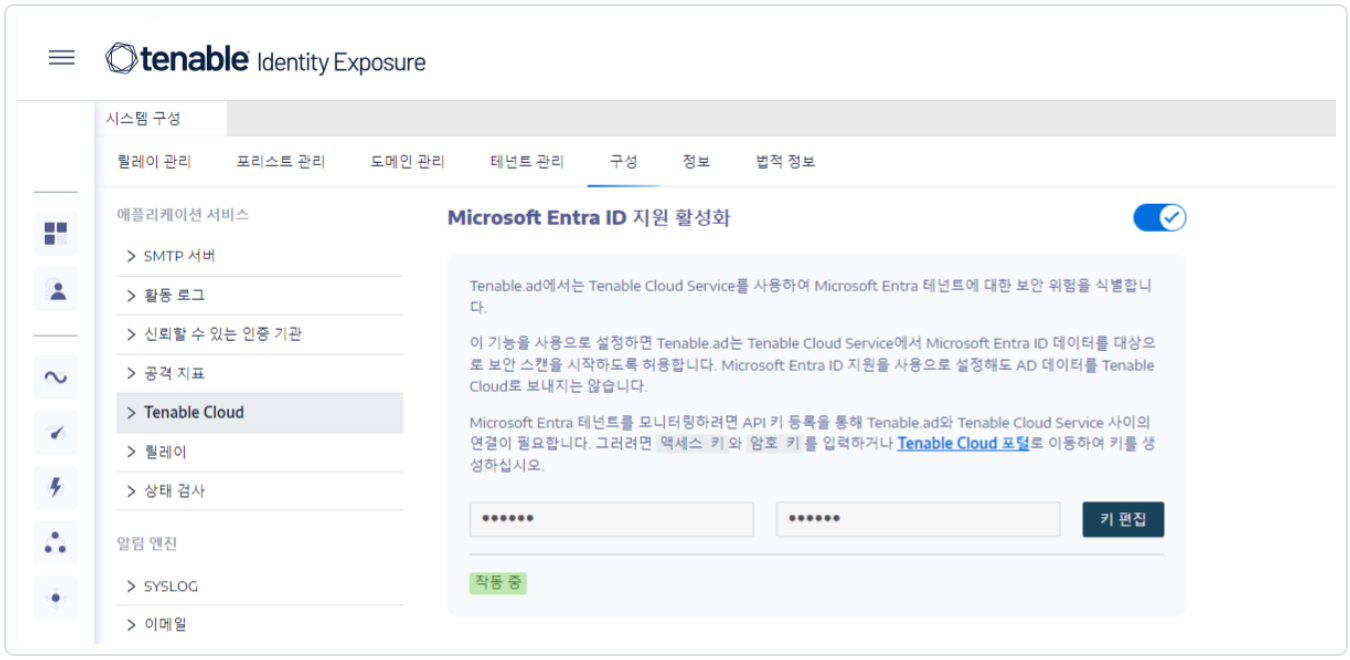
    a. **비밀번호를 잊으셨습니까?** 를 클릭하여 비밀번호 재설정을 요청합니다.

    b. Tenable Identity Exposure 라이선스와 연결된 이메일 주소를 입력하고 **비밀번호 재설정 요청**을 클릭합니다.

    그러면 Tenable에서 비밀번호를 재설정할 링크를 포함한 이메일을 해당 주소로 보냅니다.

    참고: 이메일 주소가 Tenable Identity Exposure 라이선스와 연결된 이메일과 다른 경우, 고객 지원팀에 지원을 요청하십시오.
6. Tenable Vulnerability Management에 로그인합니다.

7. Tenable Vulnerability Management에서 API 키를 생성하려면 Tenable Vulnerability Management > **설정** > **내 계정** > **API 키**로 이동합니다.
8. Tenable Vulnerability Management "관리자" 사용자 `AccessKey`와 `SecretKey`를 입력해 Tenable Identity Exposure와 Tenable Cloud Services 사이의 연결을 설정합니다.
9. **키 편집**을 클릭하여 API 키를 제출합니다.



Tenable Identity Exposure에서 API 키를 업데이트했다는 확인 메시지를 표시합니다.

테넌트 스캔 활성화

새 테넌트를 추가하는 방법:

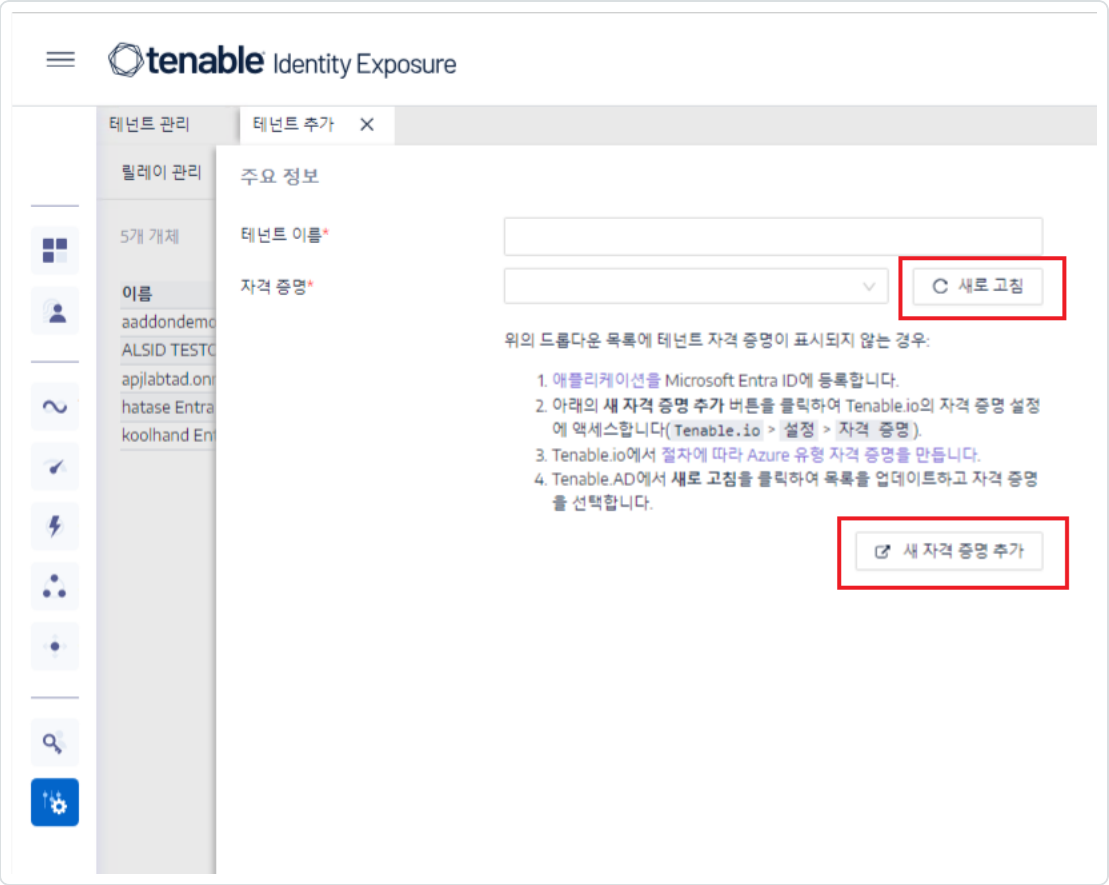
테넌트를 추가하면 Tenable Identity Exposure를 Microsoft Entra ID 테넌트와 연결하여 해당 테넌트에서 스캔을 수행할 수 있습니다.

1. 구성 페이지에서 **테넌트 관리** 탭을 클릭합니다.

   테넌트 관리 페이지가 열립니다.

2. **테넌트 추가**를 클릭합니다.

   테넌트 추가 페이지가 열립니다.



3. **테넌트 이름** 상자에 이름을 입력합니다.
4. **자격 증명** 상자에서 드롭다운 목록을 클릭하여 자격 증명을 선택합니다.
5. 자격 증명이 목록에 표시되지 않는 경우, 다음 중 한 가지 조치를 취할 수 있습니다.
    - Tenable Vulnerability Management(Tenable Vulnerability Management > **설정** > **자격 증명**)에서 만듭니다. 자세한 내용은 Tenable Vulnerability Management에서 Azure 유형 자격 증명을 만드는 절차를 참조하십시오.
    - Tenable Vulnerability Management에서 자격 증명에 대하여 "사용할 수 있음" 또는 "편집할 수 있음" 권한이 있는지 확인하십시오. 이러한 권한이 없으면 Tenable Identity Exposure에서 해당 자격 증명을 드롭다운 목록에 표시하지 않습니다.
6. **새로 고침**을 클릭하여 자격 증명 드롭다운 목록을 업데이트합니다.
7. 만든 자격 증명을 선택합니다.
8. **추가**를 클릭합니다.

메시지가 표시되어 Tenable Identity Exposure에서 테넌트를 추가했다고 확인하며 해당 테넌트는 이제 테넌트 관리 페이지 목록에 표시됩니다.

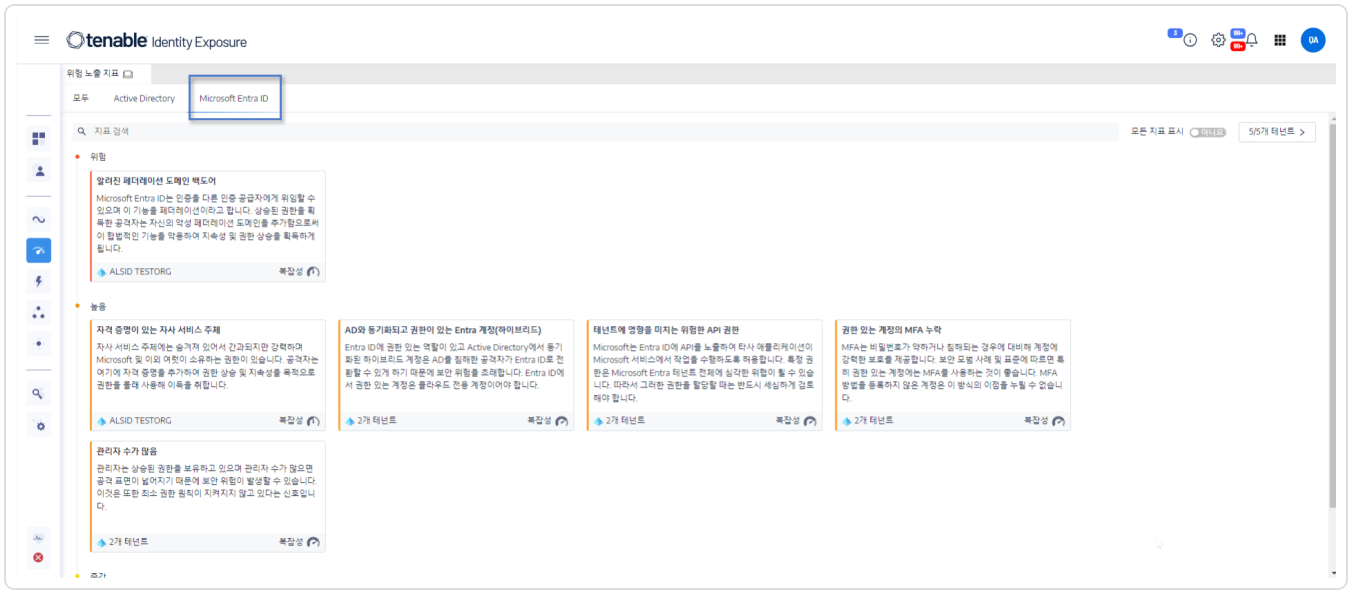
테넌트 스캔을 사용 설정하는 방법:

참고: 테넌트 스캔은 실시간으로 수행되지 않으며 Microsoft Entra ID 데이터가 Identity Explorer에 표시되기까지 최소 45분이 필요합니다.

- 목록에서 테넌트를 선택하고 토글을 클릭하여 **스캔 사용**으로 바꿉니다.

Tenable Identity Exposure에서 해당 테넌트에 대한 스캔을 요청하고 결과가 위험 노출 지표 페이지에 표시됩니다.

참고: 두 스캔 사이의 필수 최소 시간 지연은 **30분**입니다.



Tenable Cloud 데이터 수집

Tenable Cloud는 Tenable Identity Exposure의 데이터 수집 기능으로, 정보를 자체 프라이빗 클라우드에 전송하여 보안 분석과 서비스를 제공합니다. 데이터 수집에 대한 자세한 내용은 Tenable의 신뢰 및 보증 성명을 참조하십시오.

Tenable Cloud 사용하는 방법:

1. Tenable Identity Exposure에서 사이드 탐색 모음의 **시스템**을 클릭하고 **시스템**을 클릭합니다.

   시스템 구성 창이 열립니다.

2. **구성** 탭을 선택합니다.

3. **애플리케이션 서비스** 섹션 아래에서 **Tenable Cloud**를 클릭합니다.

   Tenable Cloud 창이 열립니다.

4. Tenable Cloud 서비스 사용 토글을 클릭하여 **사용**으로 설정합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 정보 전송 구성을 업데이트했다고 확인합니다.

권한 있는 분석

권한 있는 분석은 Tenable Identity Exposure의 선택 사항 기능으로, (다른 기능과는 달리) 이 기능을 사용하지 않았다면 보호되었을 데이터를 가져와 더 많은 보안 분석을 제공하기 위해 더 많은 권한이 필요한 기능입니다.

데이터 가져오기

> 참고: 권한 있는 분석 기능에는 높은 권한이 필요합니다. 권한 있는 분석에 대한 액세스를 참조하십시오.

권한 있는 분석을 사용하면 다음과 같은 추가 데이터를 가져옵니다.

- **비밀번호 해시** – Tenable Identity Exposure에서 비밀번호 분석을 위해 LM 및 NT 해시를 가져옵니다. Tenable Identity Exposure에서는 LM 해시를 가져와서 오래되고 약한 알고리즘을 사용하고 있는 것을 경고하지만 저장하지는 않습니다. 해시 수집 범위는 다음을 포함합니다.
    - 사용으로 설정된 모든 사용자 계정
    - 사용으로 설정된 모든 도메인 컨트롤러 컴퓨터 계정

데이터 보호

Active Directory(AD) 자체는 사용자 비밀번호를 직접적으로 저장하지 않고, LM 또는 NT 해싱 알고리즘을 사용해 해시만 저장합니다. 이 경우 원래 비밀번호 복원이 허용되지 않습니다. Tenable Identity Exposure에서는 LM 해시를 저장하지 않습니다.

Relay만 비밀번호를 취급하기 때문에 비밀번호는 절대로 클라이언트의 인프라에서 떠나지 않습니다 (단, SAAS-VPN 플랫폼에서 Relay를 호스팅하는 클라이언트는 예외). Relay는 비밀번호를 저장하지는 않지만, 분석을 위해 필요할 때마다 사용자의 비밀번호를 가져와 일시적으로만 캐시에 보관하며 보통 몇 밀리초에 불과합니다. 하지만 Tenable Identity Exposure에서는 최소 비트의 비밀번호 해시 데이터를 Relay의 RAM에 안전하게 저장한 상태로 보관하며 비밀번호가 동일한 사용자를 확인하기 위한 K-anonymity 분석을 수행하기 위한 목적일 뿐입니다.

> **참고**: SaaS-VPN 플랫폼 클라이언트의 경우, 동작은 같지만 Tenable에서 Relay를 호스팅합니다.

활동 로그

Tenable Identity Exposure의 활동 로그를 이용하면 특정 IP 주소, 사용자 또는 작업과 관련하여 Tenable Identity Exposure 플랫폼에서 발생한 모든 활동의 흔적을 볼 수 있습니다.

활동 로그를 구성하는 방법:

1. Tenable Identity Exposure 사이드 탐색 창의 **관리** 아래에서 **시스템**을 클릭합니다.

   시스템 구성 창이 열립니다.

2. **애플리케이션 서비스** 섹션에서 **활동 로그**를 클릭합니다.

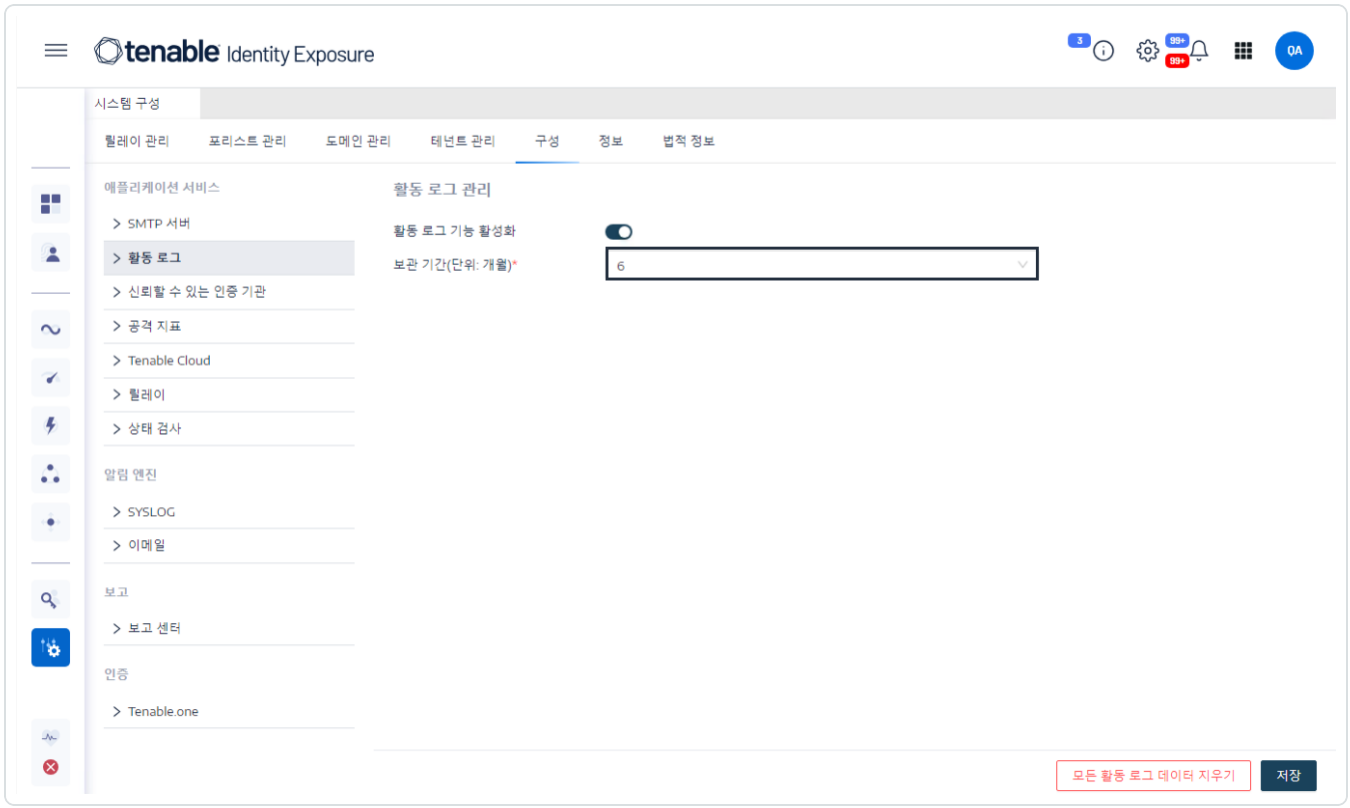
   활동 로그 관리 창이 열립니다.

3. 활동 로그 기능을 활성화하려면, 토글을 클릭하여 **사용**으로 설정합니다.

4. 보관 기간(월 단위) 상자에서 **>**를 클릭하여 활동을 로그할 개월 수를 선택합니다.

5. **저장**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 설정을 업데이트했다고 확인합니다.



활동 로그 데이터를 지우는 방법:

1. Tenable Identity Exposure 사이드 탐색 창의 **관리** 아래에서 **시스템**을 클릭합니다.

   시스템 구성 창이 열립니다.

2. **애플리케이션 서비스** 섹션에서 **활동 로그**를 클릭합니다.

   활동 로그 관리 창이 열립니다.

3. **모든 활동 로그 데이터 지우기** 아래에서 **지우기**를 클릭합니다.

   메시지가 표시되어 확인을 요청합니다.

4. **확인**을 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 설정을 업데이트했다고 확인합니다.

사용자 자신의 활동 로그에 대한 권한을 설정하는 방법:

1. Tenable Identity Exposure 사이드 탐색 창의 **관리** 아래에서 **계정**을 클릭합니다.

   사용자 계정 관리 창이 열립니다.

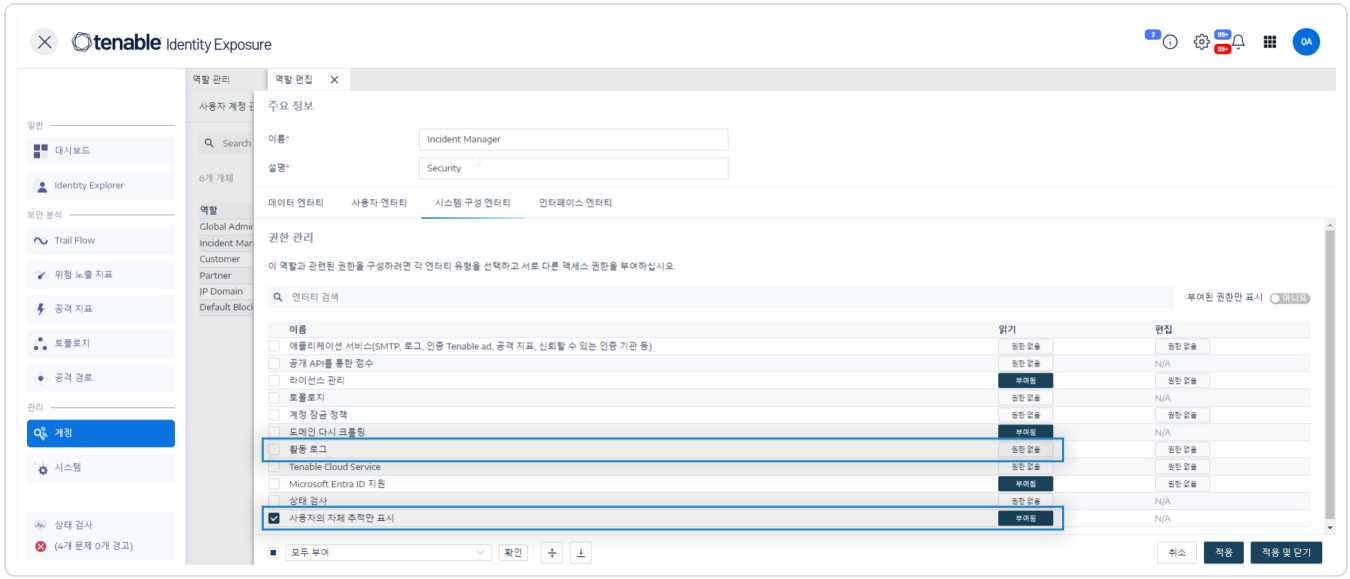
2. **역할 관리** 탭을 선택합니다.
3. 역할 목록에서 이 권한이 필요한 사용자를 가리키고 줄 끝의 ✎ 아이콘을 클릭합니다.

   역할 편집 창이 열립니다.

4. **기본 정보** 섹션 아래에서 **시스템 구성 엔터티** 탭을 선택합니다.
5. **권한 관리** 섹션 아래에서 다음과 같은 작업을 수행합니다.
   - **활동 로그**의 권한을 선택 취소하여 *권한 없음*으로 바꿉니다.
   - **사용자의 자체 추적만 표시** 권한을 선택하여 *허가됨*으로 바꿉니다.

6. **적용 및 닫기**를 클릭합니다.

   메시지가 표시되어 Tenable Identity Exposure에서 사용자 역할을 업데이트했다고 확인합니다.



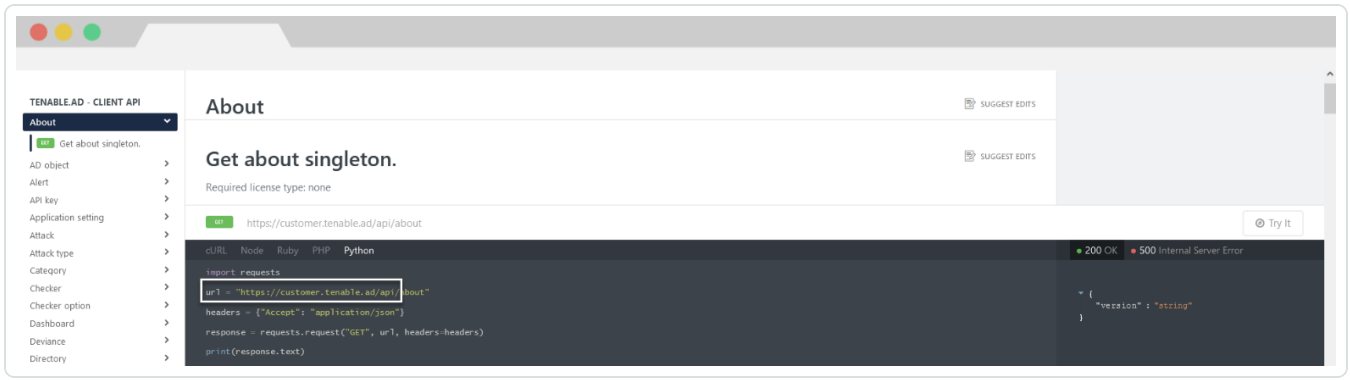
Tenable Identity Exposure 공개 API

Tenable Identity Exposure의 API를 사용하면 데이터베이스 서비스와 통신할 수 있습니다.

Tenable Identity Exposure의 API 구조와 리소스를 포함한 OpenAPI 파일을 여기에서 이용할 수 있습니다.

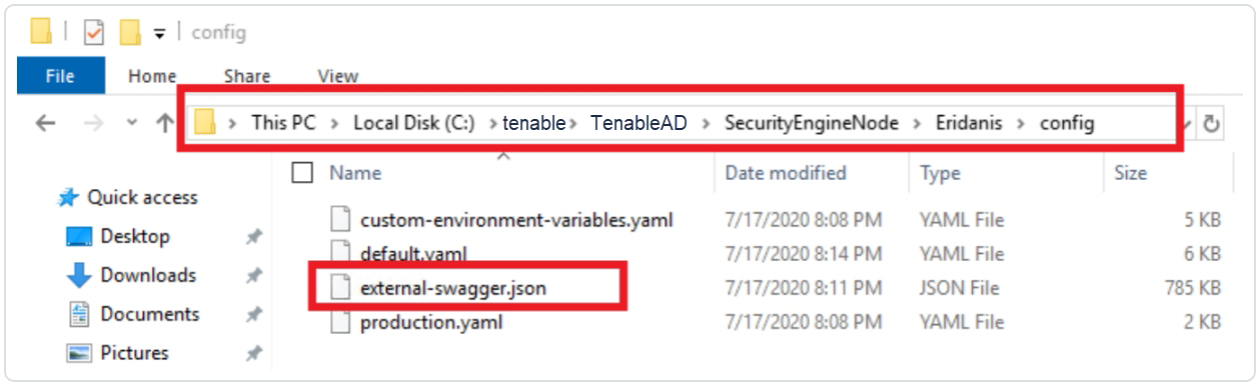
Tenable Identity Exposure 인스턴스의 API에 액세스하는 방법:

- 브라우저에서 다음 URL을 엽니다.



OpenAPI 파일을 다운로드하는 방법:

- 온프레미스 설치인 경우, 이 경로를 따라 보안 엔진 노드로 이동합니다.



- SaaS 설치의 경우, Tenable Identity Exposure API 탐색기로 이동합니다.

API 키를 가져오는 방법:

1. Tenable Identity Exposure에서 사용자 프로필을 클릭하고 **기본 설정**을 선택합니다.

   기본 설정 창이 열립니다.

2. 메뉴에서 **API 키**를 선택합니다.

   Tenable Identity Exposure에서 현재 API 키를 표시합니다.

3. API 키를 클립보드에 복사하려면 아이콘을 클릭합니다.

API 키를 새로 고치는 방법:

API 키 새로 고침을 클릭하거나 API 키 또는 액세스 토큰을 생성하는 권한을 잃으면 액세스 토큰이 만료됩니다. 만료는 시간 또는 API 요청 수와 관련이 없습니다. API 키 생성 또는 새로 고침은 현재 사용자에만 해당하며 다른 계정 API 키에는 방해가 되지 않습니다. API 키를 획득하면 새로 고침 토큰도 받게 됩니다. 이 새로 고침 토큰을 사용하여 새 API 키를 가져올 수 있습니다.

주의: API 키를 새로 고치면 Tenable Identity Exposure에서 현재 API 키를 비활성화합니다. 새로 고침 토큰도 받습니다.

1. **API 키 새로 고침**을 클릭합니다.

   메시지가 표시되어 확인을 요청합니다.

2. **확인**을 클릭합니다.

데이터 관리

Tenable Identity Exposure는 6개월 동안 데이터를 보관합니다. 이 데이터 관리 기간은 구성할 수 없습니다.

배포 리전

Tenable Identity Exposure SaaS는 현재 다음 Azure 리전에 배포됩니다.

국가	Azure 리전
미주	
브라질 – 상파울루	브라질 남부
캐나다 – 퀘벡시	캐나다 동부
캐나다 – 토론토	캐나다 중부
미국 – 캘리포니아	미국 서부
미국 – 아이오와	미국 중부
미국 – 버지니아	미국 동부 2
유럽, 중동, 아프리카	
프랑스 – 파리	프랑스 중부
아일랜드	북유럽
네덜란드	서유럽
남아프리카 – 요하네스버그	남아프리카 북부
스위스 – 취리히	스위스 북부
아랍에미리트 – 두바이	아랍에미리트 북부
영국 – 런던	영국 남부
아시아 태평양	
호주 – 뉴사우스웨일스	호주 동부
호주 – 빅토리아	호주 남동부
홍콩	동아시아
인도 – 푸네	인도 중부

일본 – 오사카	일본 서부
싱가포르	동남아시아

Tenable Identity Exposure 라이선싱

이 주제에서는 Tenable Identity Exposure를 독립형 제품으로 사용하는 경우 라이선싱 프로세스를 자세히 다루었습니다. 또한 자산을 계수하는 방법과, 라이선스가 한도 초과되거나 만료되면 어떤 일이 발생하는지도 설명했습니다. Tenable Identity Exposure 사용 방법을 알아보려면 Tenable Identity Exposure 사용자 가이드를 참조하십시오.

Tenable Identity Exposure 라이선싱

Tenable Identity Exposure에는 버전이 두 가지 있습니다. 하나는 클라우드 버전이고, 다른 하나는 온프레미스 버전입니다. Tenable에서는 상황에 따라 구독 가격을 제공하기도 합니다.

Tenable Identity Exposure를 사용하려면 조직의 요구 사항과 환경 세부 정보에 따라 적절한 라이선스를 구매해야 합니다. 그러면 Tenable Identity Exposure에서 그러한 라이선스를 *자산*에 할당합니다. 자산이란 디렉터리 서비스의 사용 설정된 사용자를 말합니다.

환경이 확장되면 자산 수도 늘어나므로, 변화를 감안해 라이선스를 추가 구매하게 됩니다. Tenable 라이선스는 점진적인 가격 책정 방식을 사용하므로 많이 구매할수록 단가가 낮아집니다. 가격은 Tenable 담당자에게 문의하십시오.

팁: 현재 라이선스 수와 이용 가능한 자산을 조회하려면 Tenable 상단 탐색 모음에서 아이콘을 클릭한 다음 **라이선스 정보**를 클릭합니다. 자세한 내용은 라이선스 정보 페이지를 참조하십시오.

참고: Tenable에서는 관리형 보안 서비스 공급자(MSSP)를 위해 간소화된 가격 책정 방식을 제공하고 있습니다. 자세한 내용을 알아보려면 Tenable 담당자에게 문의하십시오.

자산을 계수하는 방법

구매한 Tenable Identity Exposure 라이선스마다 사용자 한 사람의 고유한 ID 또는 디지털 신분증을 스캔할 권한을 부여합니다. Tenable에서는 ID를 중복 계수하지 않습니다. 예를 들어 Microsoft Active Directory와 Microsoft Entra ID에서 모두 같은 ID에 대하여 사용 설정된 사용자 계정은 Tenable 라이선스 한 개로 계수됩니다.

Tenable Identity Exposure 구성 요소

Tenable Identity Exposure의 두 버전 모두 다음과 같은 구성 요소가 함께 제공됩니다.

- Trail Flow 보기
- 토폴로지 보기
- 위험 노출 지표
- 공격 지표
- 공격 경로
- Identity 탐색기
- Microsoft Entra ID 지원

라이선스 회수

라이선스를 구매하면 라이선스 총 개수는 계약 기간 동안 고정된 채로 유지됩니다(단, 라이선스를 추가 구매하는 경우는 예외). 다만 Tenable Identity Exposure에서는 고객 환경의 디렉터리 서비스에서 사용 설정된 사용자를 삭제하면 실시간으로 라이선스를 회수합니다.

라이선스 한도 초과

하드웨어 교체, 갑작스러운 환경 확장 또는 예기치 못한 위협으로 인해 사용량이 급증하는 경우에 대비하기 위해 Tenable 라이선스는 탄력적으로 운영됩니다. 다만, 라이선스를 획득한 것보다 많은 양의 자산을 스캔하면 Tenable에서 초과분에 대해 명확히 알린 다음, 세 단계에 걸쳐 기능을 축소합니다.

상황	결과
획득한 라이선스 수량보다 많은 ID를 3일 연속으로 사용 설정함	Tenable Identity Exposure에 메시지가 표시됩니다.
획득한 라이선스 수량보다 많은 ID를 15일 이상 사용 설정함	Tenable Identity Exposure에 메시지와 기능 축소에 관한 경고가 표시됩니다.
획득한 라이선스 수량보다 많은 ID를 45일 이상 사용 설정함	Tenable Identity Exposure에 메시지가 표시됩니다. 내보내기 기능이 사용 중지됩니다.

라이선스 만료

구매한 Tenable Identity Exposure 라이선스는 계약 기간 동안 유효합니다. 라이선스 만료 30일 전에 사용자 인터페이스에 경고가 표시됩니다. 이 갱신 기간 동안 Tenable 담당자와 협력해 제품을 추가 또는 제거하거나 라이선스 수를 변경하십시오.

라이선스가 만료된 뒤에는 더 이상 Tenable 플랫폼에 로그인할 수 없습니다.

라이선스 관리

Tenable Identity Exposure에는 Tenable 또는 공인 엔터프라이즈 파트너에서 제공하는 라이선스 파일이 필요합니다. 라이선스 사용자 수에는 모든 사용으로 설정된 사용자와 서비스 계정이 포함됩니다.

Tenable Identity Exposure를 구성하고 사용하려면 라이선스 파일을 업로드해야 합니다.

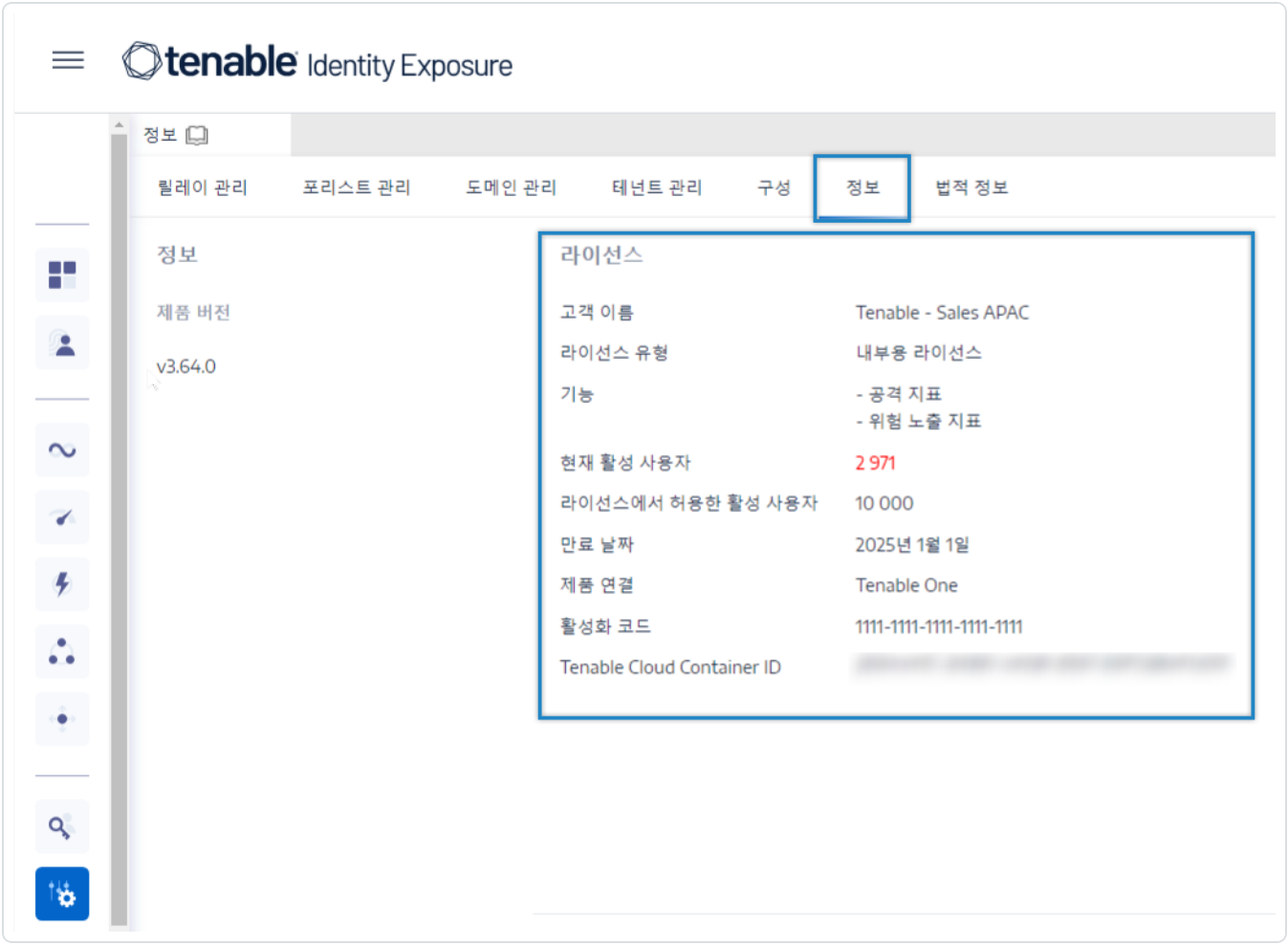
Tenable Identity Exposure 라이선스에는 다음 항목이 포함될 수 있습니다.

- 공격 지표
- 위험 노출 지표
- 위의 두 가지 모두

라이선스를 조회하는 방법:

- Tenable Identity Exposure에서 **시스템**  > **정보** 탭을 클릭합니다.

  라이선스가 표시됩니다.



라이선스 사용

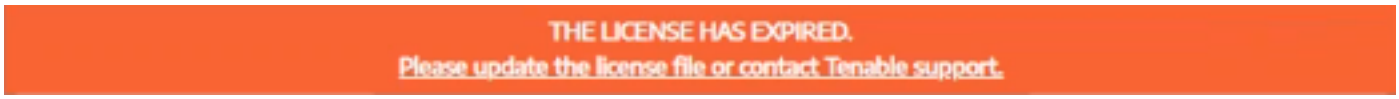
온프레미스 설치의 경우 Tenable Identity Exposure는 사용 가능한 인터넷 연결이 있으면 라이선스 사용을 추적합니다.

라이선스 유효성

Tenable Identity Exposure 라이선스는 다음 기준을 충족하는 한 유효합니다.

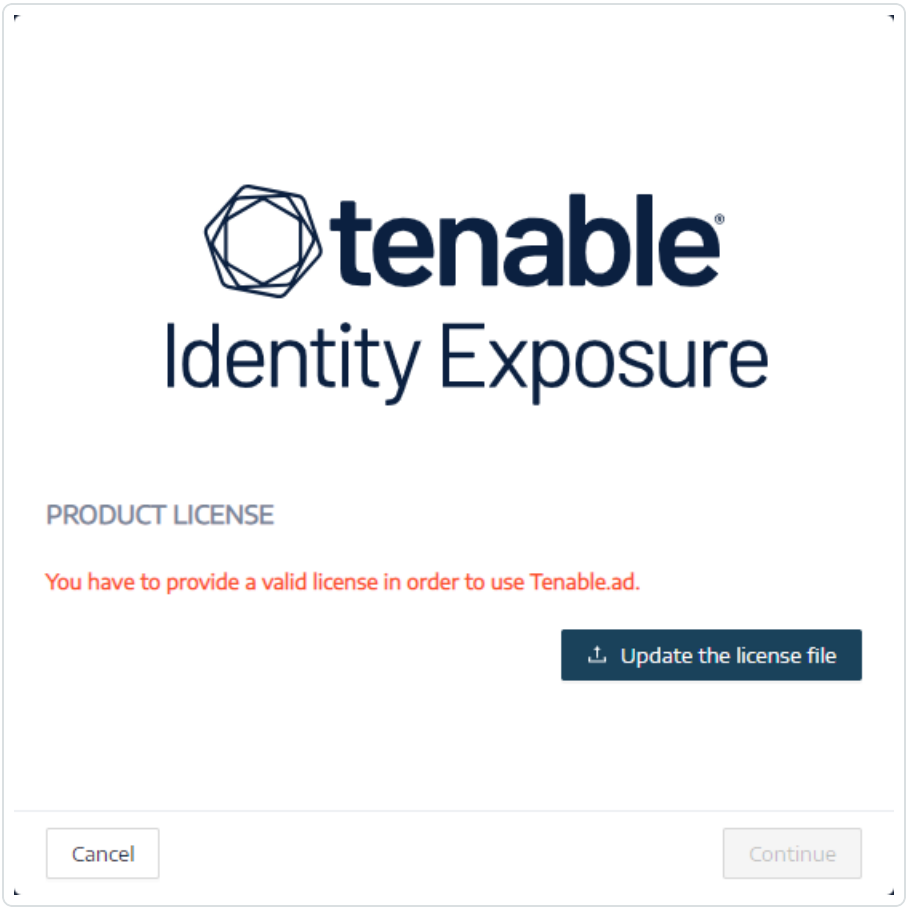
- 사용자 수가 라이선스에 허용된 수를 초과하지 않습니다.
- 만료 날짜가 지나지 않았습니다.

위의 기준 중 하나라도 부합하지 않으면 Tenable Identity Exposure에서 경고를 표시하여 라이선스를 업데이트하라고 알립니다.



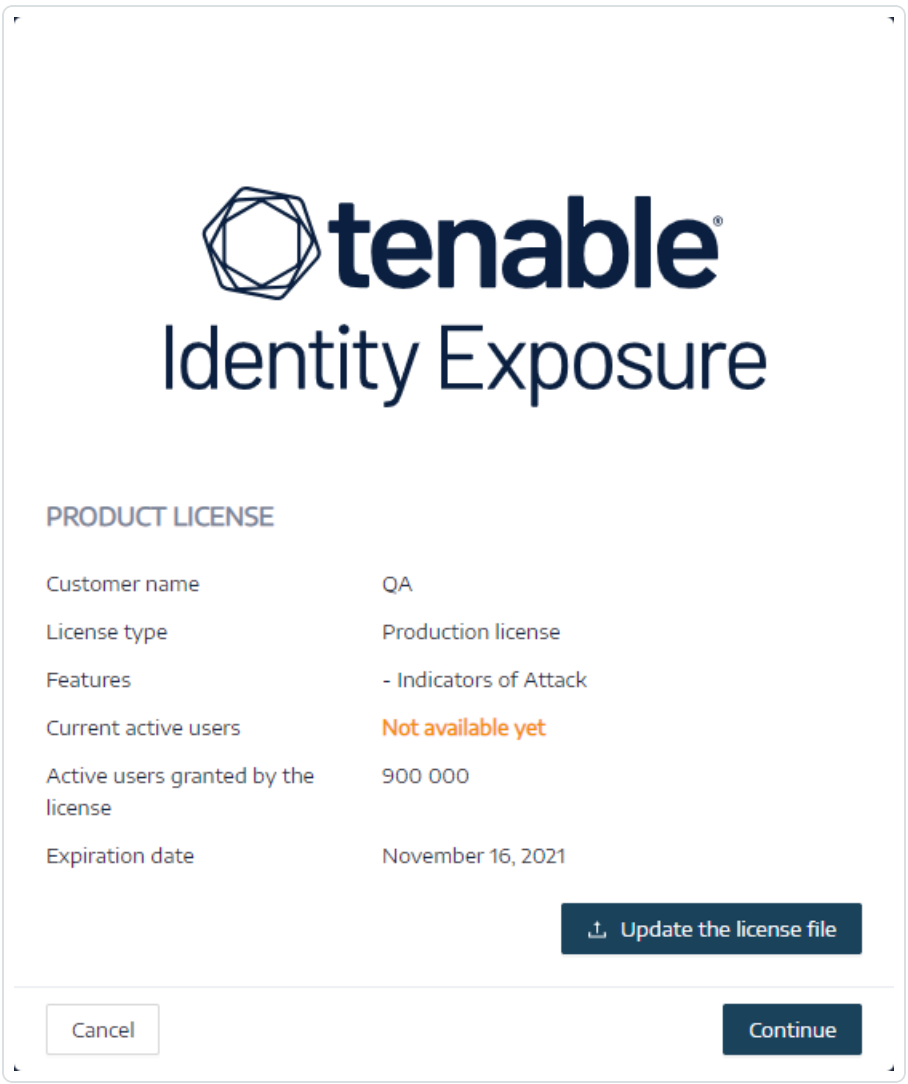
라이선스 파일을 업로드하는 방법:

1. 로그인 창에서 **라이선스 파일 업데이트**를 클릭합니다.



2. 라이선스 파일의 위치로 이동하여 **열기**를 클릭합니다.

   아래는 성공적으로 라이선스 파일을 적용한 예를 보여줍니다.



3. **계속**을 클릭하여 Tenable Identity Exposure를 시작합니다.

라이선스 파일을 업데이트하는 방법:

1. Tenable Identity Exposure에서 **시스템**과 **정보**를 클릭합니다.
2. **라이선스 파일 업데이트**를 클릭합니다.
3. 라이선스 파일의 위치로 이동하여 **열기**를 클릭합니다.

   Tenable Identity Exposure에서 라이선스 파일을 업데이트합니다. 유효하지 않은 라이선스 파일의 경우, 고객 지원에 문의하십시오.

Tenable Identity Exposure 문제 해결

다음 항목은 Tenable Identity Exposure(이전의 Tenable.ad)를 사용할 때 발생할 수 있는 문제를 해결하는 데 도움이 됩니다.

- Tenable Identity Exposure 진단 도구
- Tenable Identity Exposure와 SYSVOL 강화 간섭

Tenable Identity Exposure 진단 도구

Tenable Identity Exposure는 고객 지원팀이 문제를 분석하고 도움을 줄 수 있도록 Tenable Identity Exposure 설치와 관련된 로그 정보를 검색하는 진단 도구를 제공합니다.

Tenable 다운로드 포털에서 이 진단 도구를 다운로드합니다.

참고: 이 진단 도구는 Tenable Identity Exposure의 **온프레미스 설치**에서만 작동합니다.

진단 도구는 다음을 수행할 수 있습니다.

- (실행 파일을 실행한) 현재 시스템이 SM(Storage Manager), SEN(Security Engine Node) 또는 DL(Directory Listener)을 호스팅하는지 식별합니다.
- 네트워크에서 사용 가능한 다른 Tenable Identity Exposure 설치를 찾으려면 환경을 스캔합니다.
- Tenable Identity Exposure 설치와 관련된 로그 소스 목록을 탐지하여 이에 대한 정보를 테스트하고 검색합니다.
- 실패한 Tenable Identity Exposure 설치 시도에 대한 MSI 로그를 검색합니다.

최상의 결과를 얻기 위한 몇 가지 팁

- SEN에서 진단 도구를 실행합니다.
- 대부분의 로그 소스 또는 모든 로그 소스를 활성화하려면 권한이 상승된 사용자로 진단 도구를 실행합니다.
- SM 또는 기타 설치를 탐지하려면 다음 조건을 충족하는지 확인합니다.
    - 구성을 통해 원격 컴퓨터에서 원격 명령을 실행할 수 있습니다(Invoke-Command cmdlet).
    - 구성에서 디스크에 대한 원격 액세스를 허용합니다.
    - WMI가 사용으로 설정되어 있고 현재 사용자 계정에 대해 허용됩니다.

진단 도구를 실행하는 방법:

1. Tenable 다운로드 포털에서 `TenableAdDiagnosticTool.OnPrem.Console.exe` 파일을 다운로드합니다.

2. 실행 파일을 관리자 권한으로 Tenable Identity Exposure 시스템에서 실행합니다. SEN을 호스팅하는 시스템이면 더 좋습니다.
3. 프롬프트에서 다음 옵션 중 하나를 입력합니다.
    - `E` - 모든 로그(기본 옵션)
    - `Msi` - Tenable Identity Exposure 설치와 관련된 로그
    - `Tenable` - Tenable Identity Exposure와 관련된 로그
4. Enter 키를 누릅니다.

    진단 도구가 설치를 스캔합니다. 스캔이 완료되면 결과 출력은 현재 디렉터리에 압축 파일로 저장됩니다.
5. 이 압축 파일을 Tenable Identity Exposure 고객 지원팀으로 보냅니다. 어떤 식으로든 파일 내용을 변경하지 마십시오.

명령줄을 사용하여 진단 도구를 실행하는 방법:

1. 명령줄에서 실행 파일 `TenableAdDiagnosticTool.OnPrem.Console.exe`를 Tenable Identity Exposure 시스템(가급적이면 SEN을 호스팅하는 시스템)의 관리자 권한으로 실행합니다.

    진단 도구가 설치를 스캔합니다. 스캔이 완료되면 결과 출력은 현재 디렉터리에 압축 파일로 저장됩니다.
2. 이 압축 파일을 Tenable Identity Exposure 고객 지원팀으로 보냅니다. 어떤 식으로든 파일 내용을 변경하지 마십시오.

다른 옵션

이 진단 도구는 명령줄을 사용하여 다음 옵션도 제공합니다.

- `-- help` - 진단 도구 사용법에 대한 간략한 설명입니다.
- `-- commands` - 시스템 기능을 테스트하고 다른 설치를 스캔하기 위한 Powershell/WMI 쿼리 목록입니다.

Tenable Identity Exposure와 SYSVOL 강화 간섭

SYSVOL은 Active Directory 도메인의 각 도메인 컨트롤러(DC)에 있는 공유 폴더입니다. 그룹 정책(GPO)에 대한 폴더와 파일을 저장합니다. SYSVOL의 내용은 모든 DC에 복제되며 `\\<example.com>\SYSVOL` 또는 `\\<DC_IP_or_FQDN>\SYSVOL`과 같은 보편적 명명 규칙(UNC) 경로를 통해 액세스합니다.

SYSVOL 강화란 "UNC 강화 액세스", "강화 UNC 경로", "UNC 경로 강화" 또는 "강화 경로" 등으로도 알려진 UNC 강화 경로 매개 변수를 사용하는 것입니다. 이 기능은 그룹 정책의 MS15-011(KB 3000483) 취약성에 대응하기 위해 도입되었습니다. CIS 벤치마크와 같은 많은 사이버 보안 표준이 이 기능의 적용을 필수로 지정합니다.

SMB(서버 메시지 블록) 클라이언트에 이 강화 매개 변수를 적용하면 실제로 도메인 가입 시스템의 보안이 강화되어 SYSVOL에서 검색하는 GPO 콘텐츠가 네트워크의 공격자에 의해 변조되지 않습니다. 그러나 특정 상황에서 이 매개 변수는 Tenable Identity Exposure의 작업을 방해할 수도 있습니다.

강화된 UNC 경로가 Tenable Identity Exposure와 SYSVOL 공유 간의 연결을 방해하는 경우, 이 문제 해결 섹션의 안내를 따르십시오.

영향을 받는 환경

다음 Tenable Identity Exposure 배포 옵션에서 이 문제가 발생할 수 있습니다.

- 온프레미스
- Secure Relay를 사용하는 SaaS

다음 배포 옵션은 영향을 받지 않습니다.

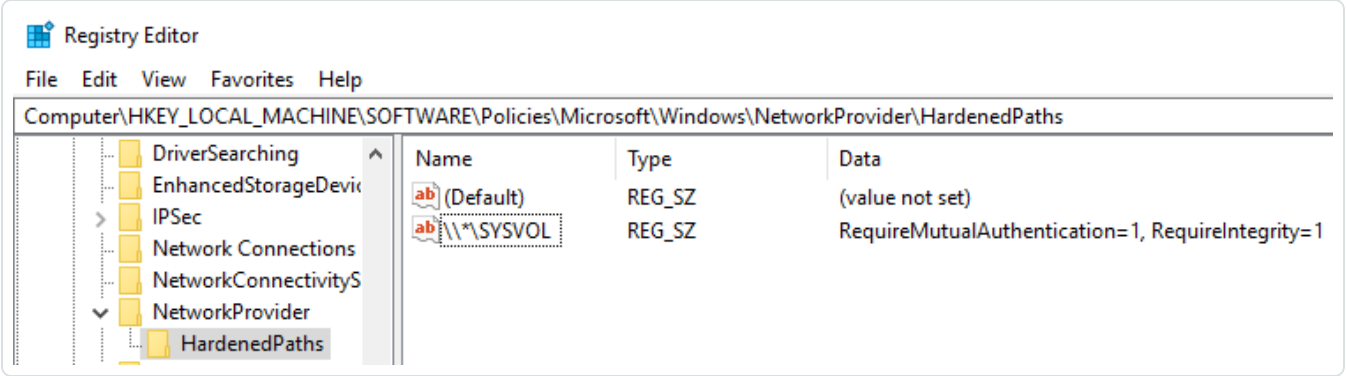
- VPN을 사용하는 SaaS

SYSVOL 강화는 클라이언트 측 매개 변수입니다. 즉, 도메인 컨트롤러가 아닌 SYSVOL 공유에 연결되는 시스템에서 작동합니다.

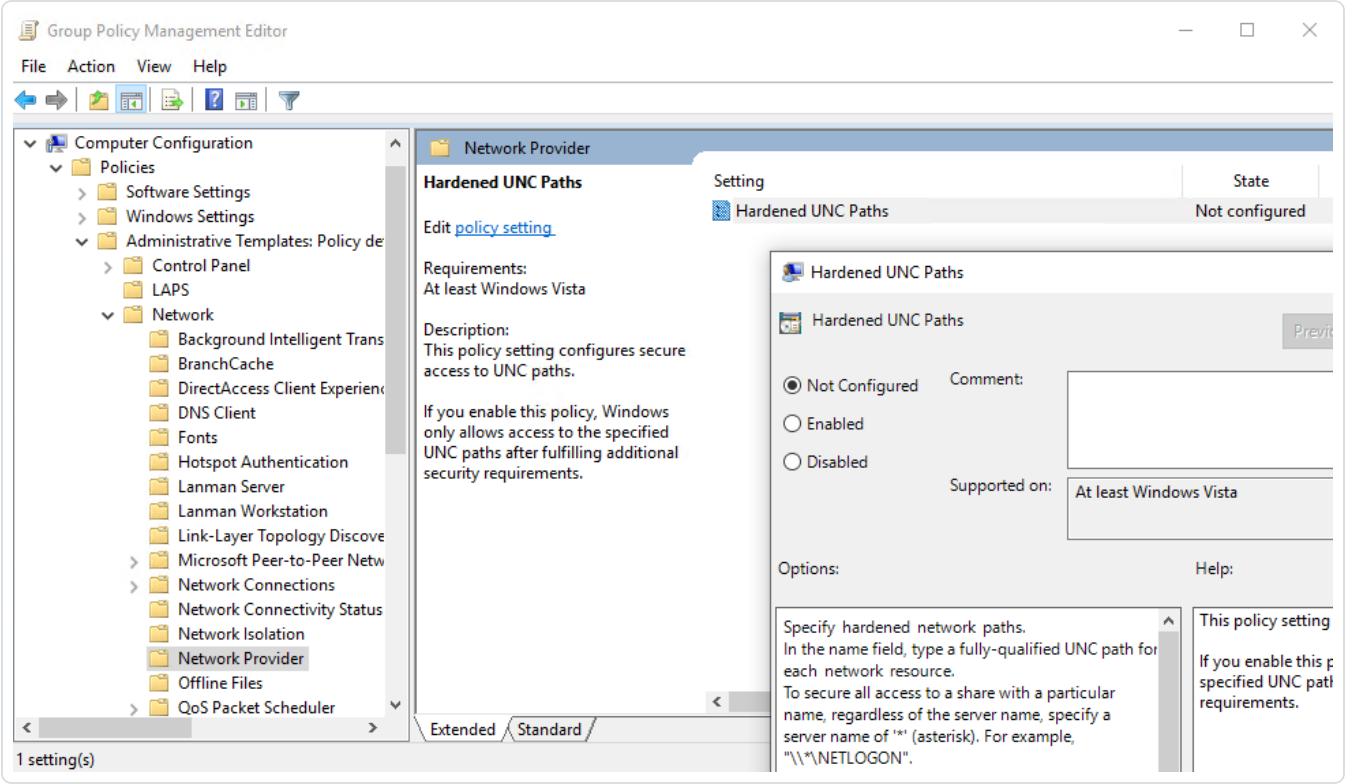
Windows는 이 매개 변수를 기본적으로 사용으로 설정하며 Tenable Identity Exposure를 방해할 수 있습니다.

또한 일부 조직에서는 관련 GPO 설정을 사용하거나 해당 레지스트리 키를 직접 설정하여 이 매개 변수의 활성화를 보장하고 적용해야 합니다.

- "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" 에서 UNC 강화 경로와 관련된 레지스트리 키를 찾을 수 있습니다.



- "Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths"에서 해당 GPO 설정을 찾을 수 있습니다.



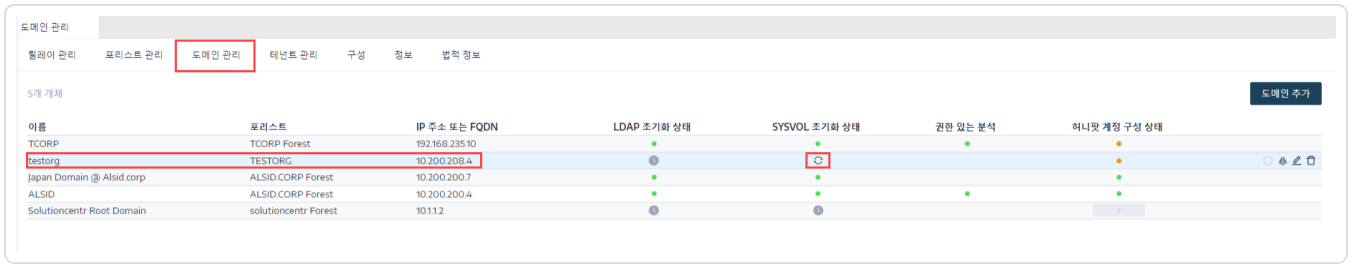
SYSVOL 강화 적용은 SYSVOL을 참조하는 UNC 경로(예: "*\SYSVOL")에 "RequireMutualAuthentication" 및 "RequireIntegrity" 매개 변수가 "1" 값으로 설정된 경우 발생합니다.

SYSVOL 강화에 문제가 있다는 징후

SYSVOL 강화가 Tenable Identity Exposure를 방해한다는 의심되면 다음을 확인하십시오.

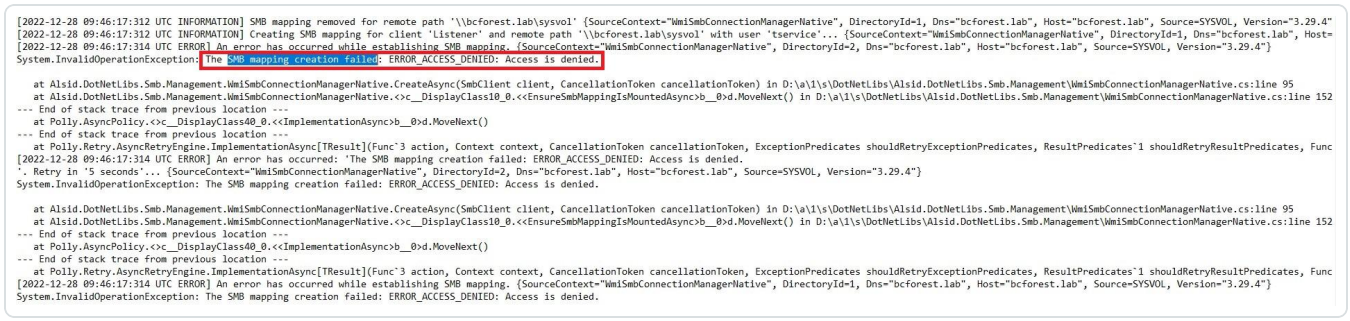
1. Tenable Identity Exposure에서 **시스템** > **도메인 관리**로 이동하여 각 도메인에 대한 LDAP 및 SYSVOL 초기화 상태를 확인합니다.

   연결이 정상인 도메인은 녹색 지표로 표시되고 연결 문제가 있는 도메인은 무한히 계속되는 크롤링 지표가 표시될 수 있습니다.



2. Directory Listener 또는 Relay 시스템에서 로그 폴더 `<Installation Folder>\DirectoryListener\logs`를 엽니다.

3. Ceti 로그 파일을 열고 "SMB mapping creation failed" 또는 "Access is denied" 문자열을 검색합니다. 이 문구가 포함된 오류 로그는 UNC 강화가 Directory Listener 또는 Relay 시스템에 적용되었을 가능성이 있음을 나타냅니다.



수정 옵션

가능한 수정 옵션에는 Kerberos 인증으로 전환 또는 SYSVOL 강화 사용 중지, 두 가지가 있습니다.

Kerberos 인증으로 전환

강화 기능의 사용 중지를 방지하기 때문에 선호하는 옵션입니다.

SYSVOL 강화가 Tenable Identity Exposure를 방해하는 것은 NTLM 인증을 사용하여 모니터링되는 도메인 컨트롤러에 연결하는 경우에만 해당합니다. 이는 NTLM이

"RequireMutualAuthentication=1" 매개 변수와 호환되지 않기 때문입니다. Tenable Identity Exposure는 Kerberos도 지원합니다. Kerberos를 올바르게 구성하고 사용하는 경우, SYSVOL 강화를 사용 중지할 필요가 없습니다. 자세한 내용은 Kerberos 인증를 참조하십시오.

SYSVOL 강화 사용 중지

Kerberos 인증으로 전환할 수 없는 경우, SYSVOL 강화를 사용 중지하는 옵션도 있습니다.

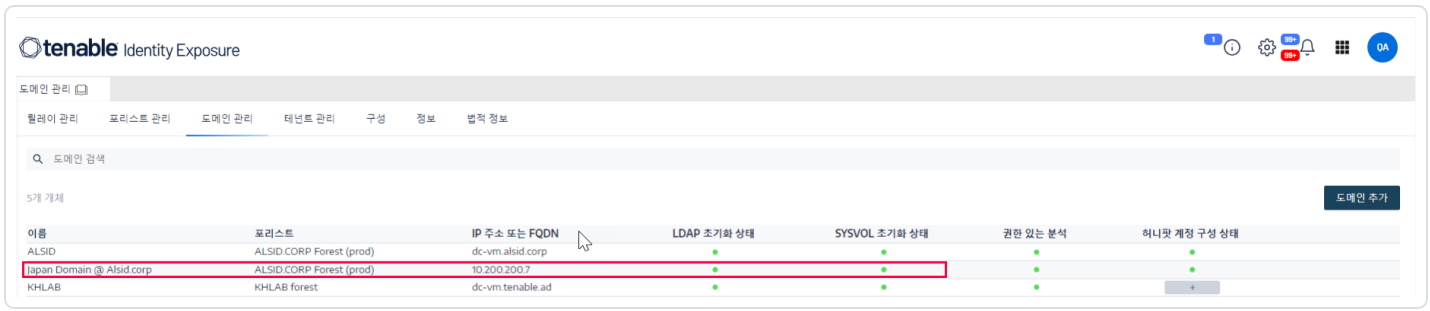
Windows는 기본적으로 SYSVOL 강화를 사용으로 설정하므로 레지스트리 키 또는 GPO 설정을 제거하는 것만으로는 충분하지 않습니다. 이 기능을 명시적으로 사용 중지하고 Directory Listener(온프레미스) 또는 Relay(Secure Relay를 사용하는 SaaS)를 호스팅하는 시스템에만 이 변경 사항을 적용해야 합니다. 이것은 다른 시스템에 영향을 미치지 않으며 도메인 컨트롤러 자체에서 SYSVOL 강화를 사용 중지할 필요가 없습니다.

Directory Listener(온프레미스) 또는 Relay(Secure Relay를 사용하는 SaaS)를 호스팅하는 시스템에서 사용되는 Tenable Identity Exposure 설치 프로그램은 이미 로컬에서 SYSVOL 강화를 사용 중지합니다. 그러나 사용자 환경의 GPO 또는 스크립트가 이 레지스트리 키를 제거하거나 덮어쓸 수 있습니다.

가능한 경우는 두 가지가 있습니다.

- Directory Listener 또는 Relay 시스템이 **도메인에 참가하지 않은** 경우 - GPO를 사용하여 시스템을 구성할 수 없습니다. 레지스트리에서 SYSVOL 강화를 사용 중지해야 합니다(레지스트리 - GUI 또는 레지스트리 – PowerShell 참조).
- Directory Listener 또는 Relay 시스템이 **도메인에 참가한** 경우(Tenable Identity Exposure에서 권장하지 않음) - 레지스트리에서(레지스트리 - GUI 또는 레지스트리 – PowerShell 참조) 직접 설정을 적용하거나 GPO를 사용하여 설정을 적용할 수 있습니다. 이러한 방법을 사용해서 GPO 또는 스크립트가 레지스트리 키를 덮어쓰지 않도록 해야 합니다. 다음 중 한 가지 방법으로 이 작업을 수행할 수 있습니다.
    - 이 시스템에 적용되는 모든 GPO를 주의 깊게 검토합니다.
    - 변경 사항을 적용하고 잠시 기다리거나 "gpupdate /force"를 사용하여 GPO 애플리케이션을 강제 실행하고 레지스트리 키가 해당 값을 유지하는지 확인합니다.

Directory Listener 또는 Relay 시스템을 다시 시작하고 나면 수정된 도메인의 크롤링 지표가 녹색 지표로 변경되어야 합니다.

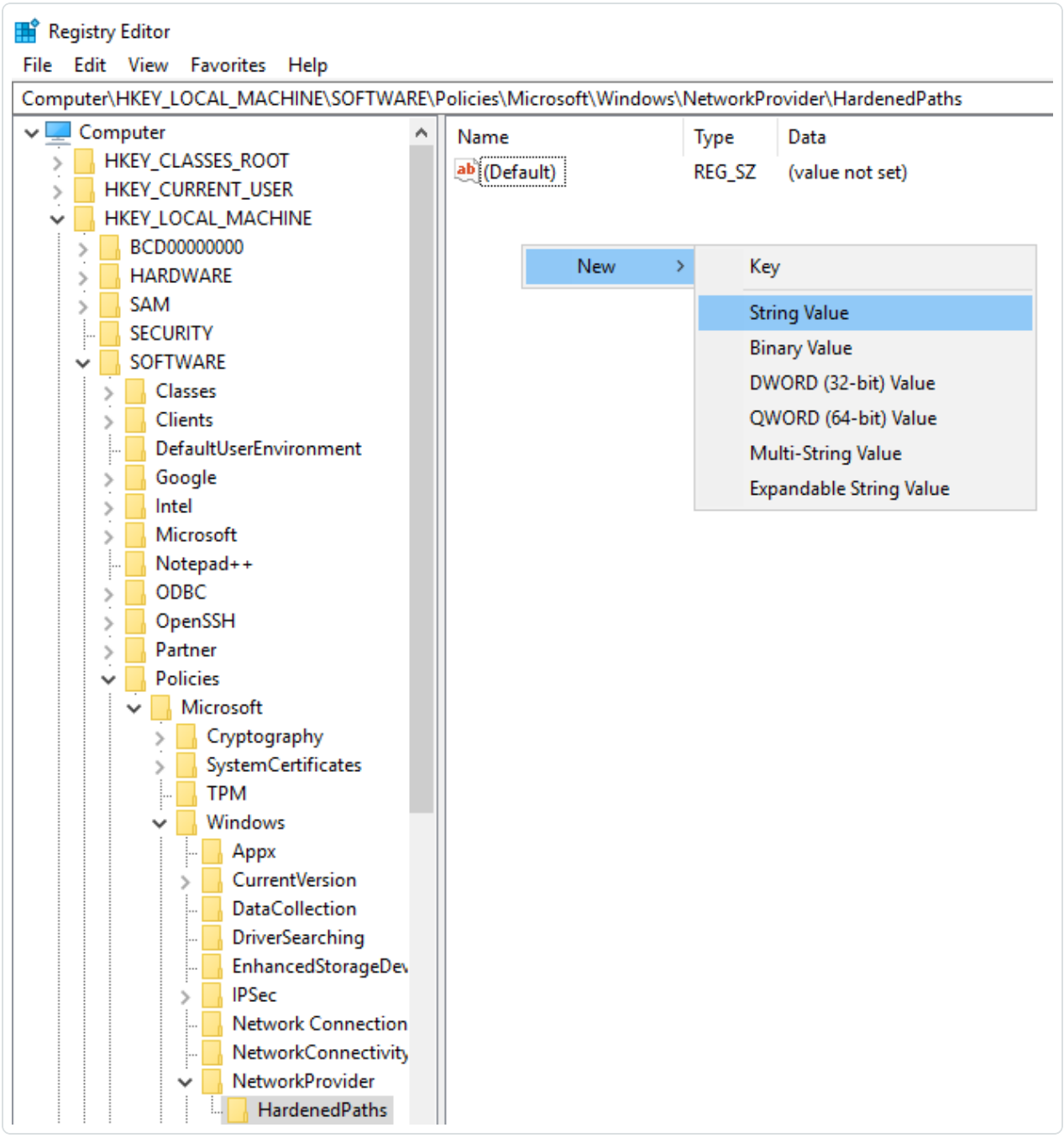


레지스트리 - GUI

GUI를 사용하여 레지스트리에서 SYSVOL 강화를 사용 중지하는 방법:

1. 관리자 권한으로 Directory Listener 또는 Relay 시스템에 연결합니다.
2. 레지스트리 편집기를 열고 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`로 이동합니다.
3. 이 키가 아직 존재하지 않는 경우, 다음과 같이 "`\\*\SYSVOL`" 키를 만듭니다.

a. 오른쪽 창을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기** > **문자열 값**을 선택합니다.



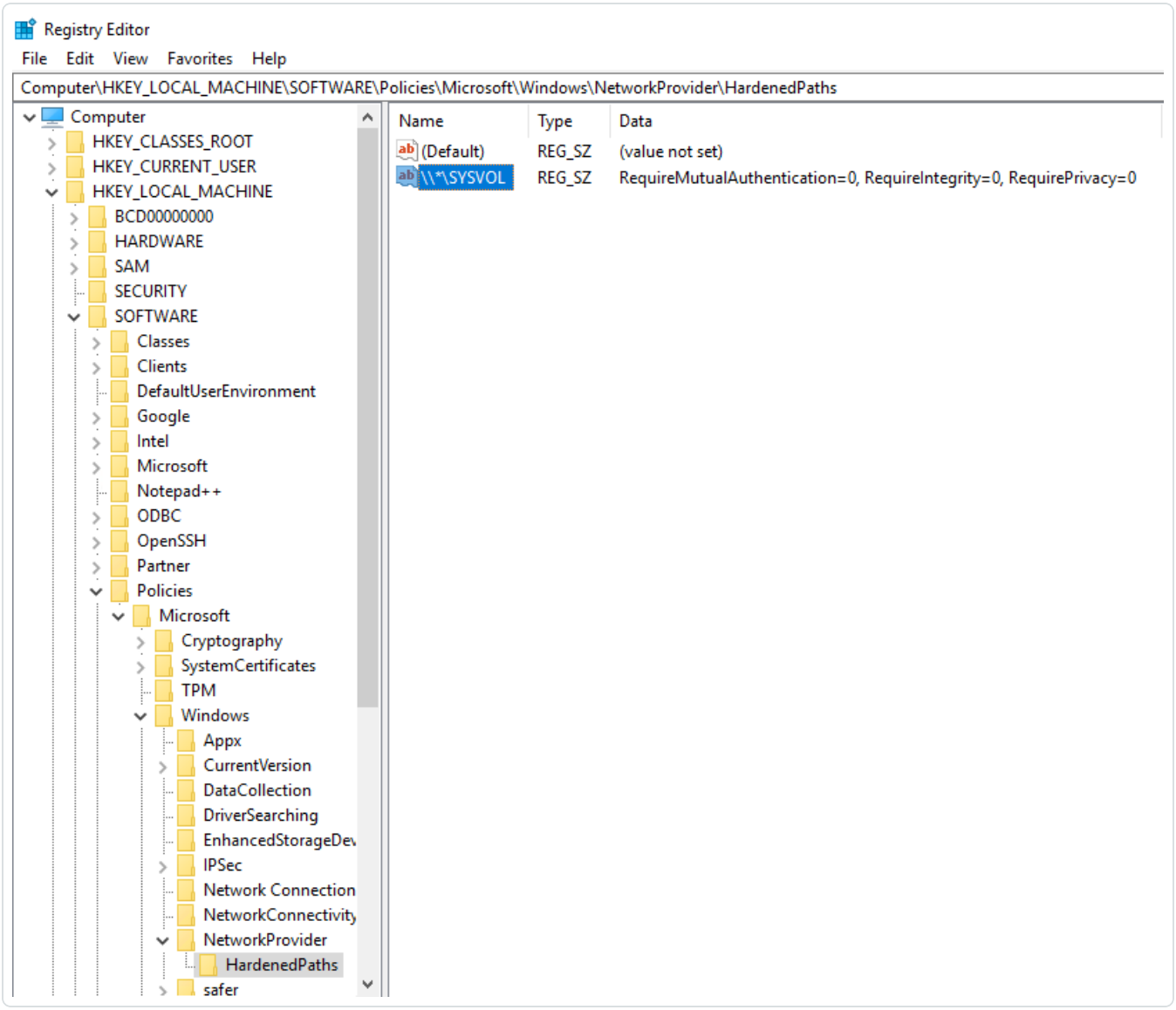
b. 이름 필드에 `\\*\SYSVOL`을 입력합니다.

4. "`\\*\SYSVOL`" 키(새로 만들었거나 이미 존재)를 두 번 클릭하여 **문자열 편집** 창을 엽니다.

5. **값** 데이터 필드에 `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0` 값을 입력합니다.

6. **저장**을 클릭합니다.

   결과는 다음과 같이 표시되어야 합니다.



7. 시스템을 다시 시작합니다.

레지스트리 – PowerShell

PowerShell을 사용하여 레지스트리에서 SYSVOL 강화를 사용 중지하는 방법:

1. 이 PowerShell 명령을 사용하여 참조할 UNC 강화 경로 레지스트리 키의 현재 값을 수집합니다.

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. 권장 값을 설정합니다.

```
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. 시스템을 다시 시작합니다.

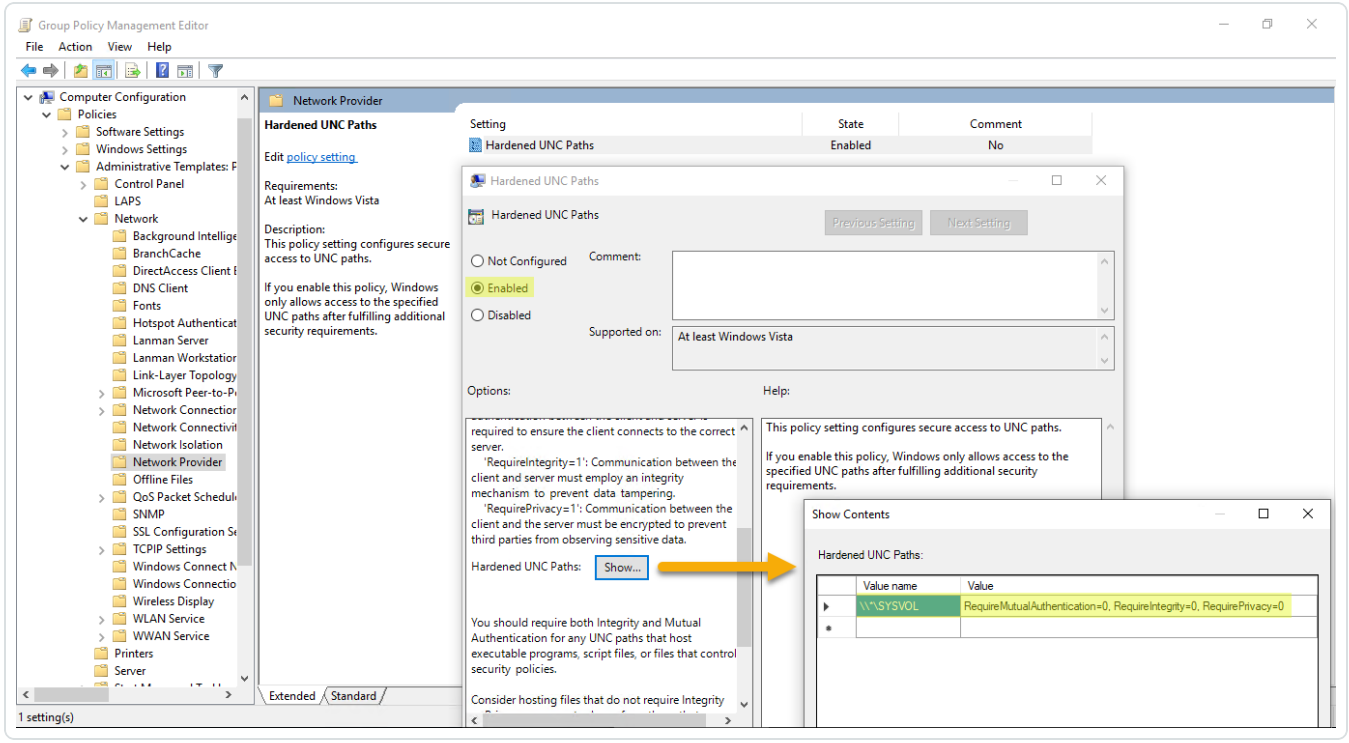
GPO

필수 조건: 도메인에서 GPO를 만들고 Tenable Identity Exposure Directory Listener 또는 Relay 시스템이 있는 조직 단위에 연결할 권한이 있는 Active Directory 사용자로 연결해야 합니다.

GPO를 사용하여 SYSVOL 강화를 사용 중지하는 방법:

1. 그룹 정책 관리 콘솔을 엽니다.
2. 새 GPO를 만듭니다.
3. GPO를 편집하고 `Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths` 위치로 이동합니다.
4. 이 설정을 사용으로 설정하고 다음을 사용하여 새로운 강화 UNC 경로를 만듭니다.
   - 값 이름 = `\\*\SYSVOL`
   - 값 = `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

   결과는 다음과 같이 표시되어야 합니다.



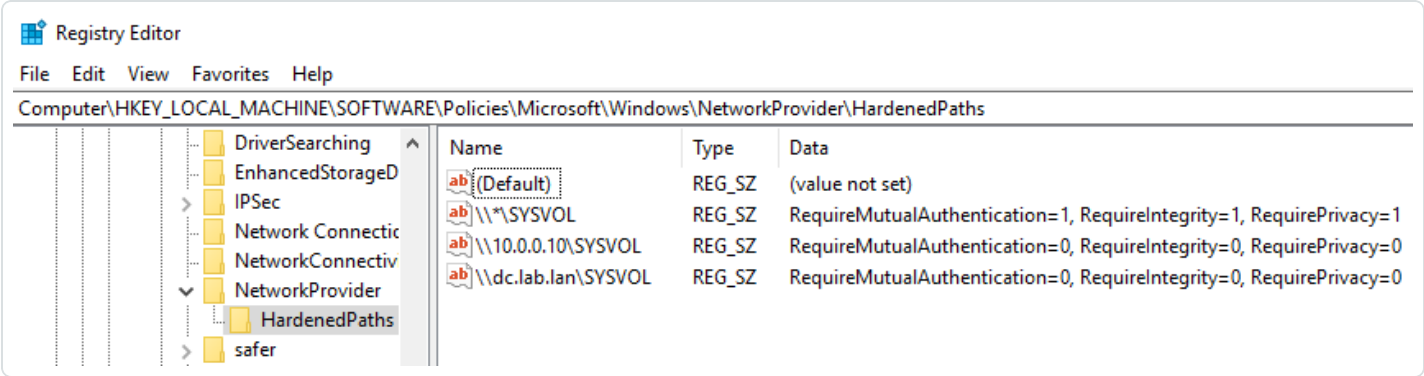
5. **확인**을 클릭하여 확인합니다.

6. 이 GPO를 Tenable Identity Exposure Directory Listener 또는 Relay 시스템이 있는 조직 구성 단위에 연결합니다. 또한, 보안 그룹 필터 GPO 기능을 사용하여 이 GPO가 이 시스템에만 적용되도록 할 수도 있습니다.

특정 UNC 경로 예외

이전 절차에서는 와일드카드 UNC 경로 "*\SYSVOL"을 사용하여 SYSVOL 강화를 사용 중지합니다. 특정 IP 주소 또는 FQDN에 대해서만 사용 중지할 수도 있습니다. 즉, "*\SYSVOL"에 대해 UNC 강화 경로 설정을 활성 상태(값 "1")로 유지할 수 있고 Tenable Identity Exposure에 구성된 도메인 컨트롤러의 각 IP 주소 또는 FQDN에 상응하는 예외가 발생하게 됩니다.

다음 이미지는 Tenable Identity Exposure에서 구성한 도메인 컨트롤러인 "`10.0.0.10`" 및 "`dc.lab.lan`"을 제외한 모든 서버("*")에 대해 활성화된 SYSVOL 강화의 예시를 보여줍니다.



위에서 설명한 레지스트리 또는 GPO 방법을 사용하여 이러한 추가 설정을 추가할 수 있습니다.

참고: Tenable Identity Exposure에 구성된 정확한 값을 지정해야 합니다(예: Tenable Identity Exposure 구성에서 FQDN을 사용하는 경우 IP 주소를 지정할 수 없음). 또한 Tenable Identity Exposure 도메인 관리 페이지에서 IP 주소 또는 FQDN을 변경할 때마다 이 키를 업데이트해야 합니다.

SYSVOL 강화를 사용 중지하는 경우의 위험

SYSVOL 강화는 보안 기능이며 사용 중지하면 실질적 문제가 발생할 수 있습니다.

- 도메인에 참가하지 않은 시스템 - SYSVOL 강화를 사용 중지해도 위험이 없습니다. 이러한 시스템은 GPO를 적용하지 않기 때문에 실행하기 위해 SYSVOL 공유에서 콘텐츠를 가져오지 않습니다.
- 도메인에 참가한 시스템(Directory Listener 또는 Relay 시스템)(Tenable Identity Exposure에서 권장하지 않음) - Directory Listener 또는 Relay 시스템과 도메인 컨트롤러 사이에 "중간자" 공격이 발생할 위험이 있는 경우, SYSVOL 강화를 사용 중지하는 것은 안전하지 않습니다. 이 경우, Tenable Identity Exposure에서는 대신 Kerberos 인증으로 전환할 것을 권장합니다.

이 비활성화하는 범위는 Directory Listener 또는 Relay 시스템에만 적용되고 다른 도메인 컴퓨터에는 적용되지 않으며 도메인 컨트롤러에는 절대로 적용되지 않습니다.