Tenable Identity Exposure 3.x – Benutzer- und Administratorhandbuch

Letzte Überarbeitung: 05. April 2024

Inhalt

Willkommen bei Tenable Identity Exposure

Zuletzt aktualisiert: 30.04.2024

Tenable Identity Exposure (ehemals Tenable.ad) ermöglicht es Ihnen durch die Vorhersage von Bedrohungen, das Erkennen von Sicherheitsverletzungen und die Reaktion auf Angriffe, Ihre Infrastruktur zu sichern. Über ein intuitives Dashboard zur Echtzeitüberwachung Ihres Active Directory können Sie auf einen Blick die kritischsten Schwachstellen und die empfohlenen Behebungsmaßnahmen sehen. Mit den Indicators of Attack (IoA) und Indicators of Exposure (IoE) von Tenable Identity Exposure können Sie zugrundeliegende Probleme in Ihrem Active Directory aufdecken, gefährliche Vertrauensstellungen identifizieren und Details zu Angriffen umfassend analysieren.

> Die Funktionen „Indicators of Attack" und „Indicators of Exposure" sind je nach erworbener Lizenz verfügbar.

Um loszulegen, siehe Erste Schritte mit Tenable Identity Exposure.

> **Hinweis:** Tenable Identity Exposure kann einzeln oder als Teil des Tenable One-Pakets erworben werden. Weitere Informationen finden Sie unter Tenable One.

> **Tipp:** Das *Benutzerhandbuch* zu *Tenable Identity Exposure* ist in Englisch, Japanisch, Deutsch, Koreanisch, vereinfachtem Chinesisch und traditionellem Chinesisch verfügbar. Die Benutzeroberfläche von *Tenable Identity Exposure* ist in Englisch, Japanisch, Deutsch, Französisch, Koreanisch, vereinfachtem Chinesisch und traditionellem Chinesisch verfügbar. Informationen zum Ändern der Sprache der Benutzeroberfläche finden Sie unter Benutzervoreinstellungen.

Weitere Informationen zu Tenable Identity Exposure finden Sie in den folgenden Materialien für Kundenschulungen:

- Tenable Identity Exposure Self Help Guide
- Einführung in Tenable Identity Exposure (Tenable University)

Exposure-Management-Plattform Tenable One

Tenable One ist eine Exposure-Management-Plattform, mit deren Hilfe Unternehmen Sichtbarkeit auf ihrer gesamten modernen Angriffsoberfläche erzielen, Maßnahmen zur Verhinderung von

wahrscheinlichen Angriffen fokussieren und Cyberrisiken präzise kommunizieren können, um eine optimale Unternehmensperformance zu unterstützen.

Die Plattform kombiniert eine umfassende Schwachstellen-Abdeckung über IT-Assets, Cloud-Ressourcen, Container, Web-Apps und Identitätssysteme hinweg, baut auf der Schnelligkeit und Breite der Schwachstellen-Abdeckung von Tenable Research auf und bietet zudem umfangreiche Analytik, um Maßnahmen zu priorisieren und Cyberrisiken zu kommunizieren Mit Tenable One können Unternehmen:

- Umfassenden Einblick in die gesamte moderne Angriffsoberfläche erzielen
- Bedrohungen vorhersehen und Maßnahmen zur Verhinderung von Angriffen priorisieren
- Cyberrisiken kommunizieren, um bessere Entscheidungen zu treffen

Tenable Identity Exposure ist als eigenständiges Produkt erhältlich oder kann als Teil der Exposure Management-Plattform Tenable One erworben werden.

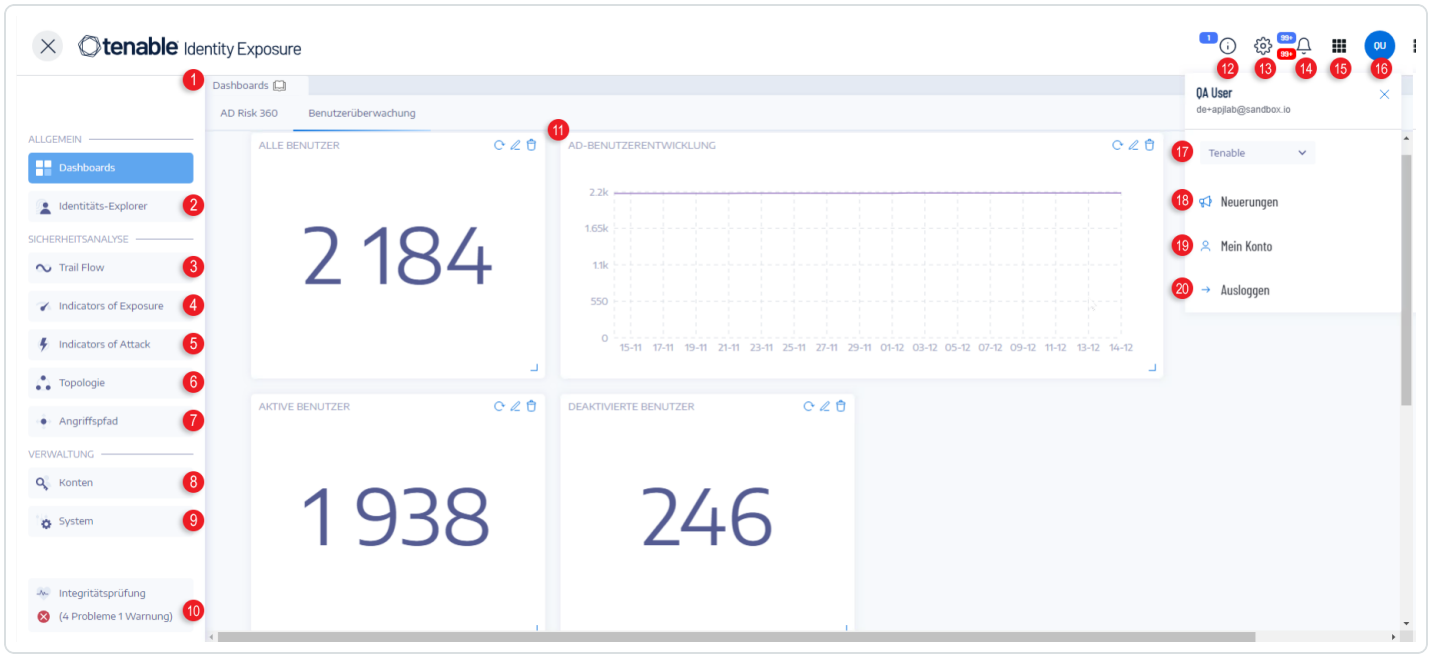
> **Tipp:** Weitere Informationen zu den ersten Schritten mit Tenable One-Produkten finden Sie im Tenable One Deployment Guide.

In Tenable Identity Exposure navigieren

Nach dem Einloggen bei Tenable Identity Exposure öffnet sich die Startseite, wie in diesem Beispiel gezeigt.

So erweitern oder reduzieren Sie die seitliche Navigationsleiste:

- Erweitern: Klicken Sie oben links im Fenster auf das Menü ☰.
- Reduzieren: Klicken Sie oben links im Fenster auf das **X**.



#	Element	Funktion
1	Dashboards	Über Dashboards können Sie die Sicherheit in einer Active Directory-Infrastruktur effizient und auf visuelle Weise verwalten und überwachen.
2	Identitäts-Explorer	Die Identitäts-Explorer-Ansicht von Tenable Identity Exposure vereinheitlicht Identitäten in Active Directory und Microsoft Entra ID. Diese Ansicht zeigt den Identitätsrisiko-Score (Beta) für jedes

		aufgelistete Asset und die potenzielle Reichweite kompromittierter Identitäten.
3	Trail Flow	Der Trail Flow zeigt die Echtzeitüberwachung und -analyse von Ereignissen, die Ihr Active Directory betreffen.
4	Indicators of Exposure	Tenable Identity Exposure misst den Sicherheitsreifegrad Ihres Active Directory mithilfe von Indicators of Exposure (IoEs) und weist dem Strom von Ereignissen, die überwacht und analysiert werden, Schweregradstufen zu (Kritisch, Hoch, Mittel oder Gering).
5	Indicators of Attack	Mithilfe von Indicators of Attack kann Tenable Identity Exposure Angriffe in Echtzeit erkennen.
6	Topology	Die Seite „Topologie" enthält eine interaktive grafische Visualisierung Ihres Active Directory. Sie zeigt die Gesamtstrukturen, Domänen und die zwischen ihnen bestehenden Vertrauensstellungen.
7	Angriffspfad	Auf den Angriffspfad-Seiten werden grafische Darstellungen der Active Directory-Beziehungen angezeigt: • Angriffsradius: Evaluiert laterale Bewegungen im AD, die von einem potenziell kompromittierten Asset

		ausgehen. • Angriffspfad: Antizipiert Techniken zur Rechteausweitung, um von einem bestimmten Einstiegspunkt aus auf ein Objekt zuzugreifen. • Asset-Exposure: Misst die Anfälligkeit eines Assets mithilfe der Asset-Exposure-Visualisierung und berücksichtigt alle Eskalationspfade.
8, 9	Verwaltung **Erforderliche Benutzerrolle**: Organisationsbenutzer mit entsprechenden Berechtigungen.	In diesem Abschnitt können Sie Folgendes konfigurieren: • Konten: Benutzerkonten, Rollen und Sicherheitsprofile. • System: Gesamtstrukturen und Domänen, Anwendungsdienste, Warnungen und Authentifizierung. Weitere Informationen finden Sie im Tenable Identity Exposure-Administratorhandbuch.
10	Integritätsprüfungen	Integritätsprüfungen bieten Ihnen Echtzeit-Einblicke in die Konfiguration Ihrer Domänen und Dienstkonten. Diese Daten werden in einer konsolidierten Ansicht dargestellt, die Sie aufschlüsseln können, um detailliertere

		Informationen zu erhalten.
11	Widgets	Widgets sind anpassbare Datasets in einem Dashboard. Sie können Balkendiagramme, Liniendiagramme und Zähler enthalten.
12	Produkt-Updates	Informationen über die neuesten Produktfunktionen.
13	Einstellungen	Zugriff auf Systemkonfiguration, Gesamtstruktur- und Domänenverwaltung, Lizenz-, Benutzer- und Rollenverwaltung, Profile und Aktivitätsprotokolle.
14	Benachrichtigungen (Glocke)	Ein Glockensymbol und die Anzahl der Badges informieren Sie über Angriffswarnungen und/oder Exposure-Warnungen, die auf Ihre Bestätigung warten.
15	App-Schnellzugriff	Klicken Sie auf dieses Symbol, um vom Tenable Arbeitsbereich aus zwischen Anwendungen zu wechseln.
16, 19	Benutzerprofil-Symbol (Benutzervoreinstellungen)	Klicken Sie auf dieses Symbol, um ein Untermenü zu öffnen, in dem Sie auf Sicherheitsprofile, Versionshinweise, Aktivitätsprotokolle und Voreinstellungen zugreifen und sich ausloggen können.
17	Sicherheitsprofile	Über Sicherheitsprofile können Sie verschiedene Arten von Benutzern verwalten, um die Sicherheitsanalyse unter verschiedenen Gesichtspunkten zu überprüfen.

18	Neuerungen	Klicken Sie auf diese Option, um die Versionshinweise für die neueste Version von Tenable Identity Exposure zu öffnen.
20	Ausloggen	Klicken Sie auf diese Option, um sich aus Tenable Identity Exposure auszuloggen.

Bei Tenable Identity Exposure einloggen

Sie greifen über eine Client-URL auf die Webanwendung von Tenable Identity Exposure zu.

Wählen Sie eine der folgenden Optionen aus, um sich bei Tenable Identity Exposure einzuloggen:

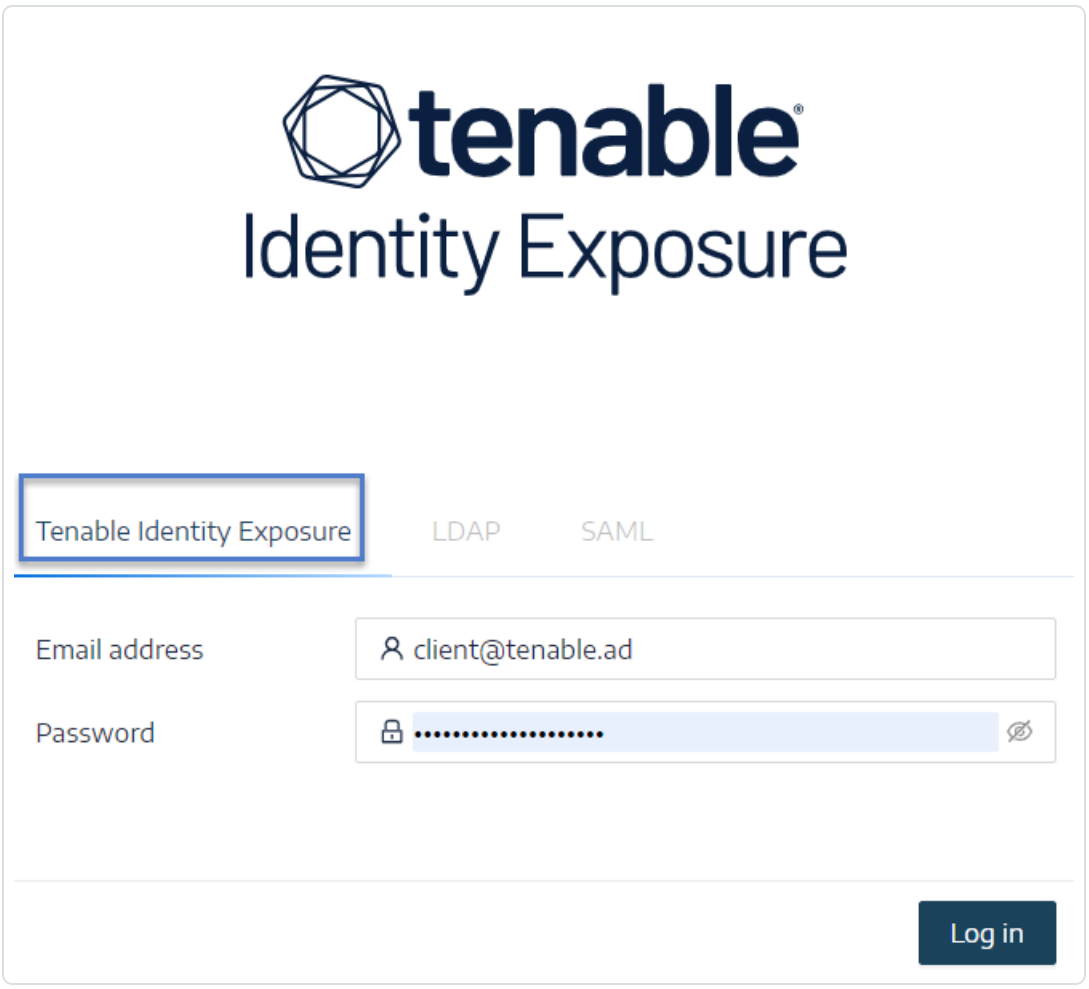
- ◦ Verwenden eines Tenable Identity Exposure-Kontos
  ◦ LDAP-Konto verwenden
  ◦ SAML verwenden

Verwenden eines Tenable Identity Exposure-Kontos

So loggen Sie sich mit Ihrem Tenable Identity Exposure-Konto ein:

1. Geben Sie in einem beliebigen Browser Ihre Client-URL (zum Beispiel: client.tenable.ad) in die Adresszeile ein.

   Das Fenster **Einloggen** wird angezeigt.



2. Klicken Sie auf die Registerkarte **Tenable Identity Exposure**.
3. Geben Sie Ihre E-Mail Adresse ein.
4. Geben Sie Ihr Passwort ein.
5. Klicken Sie auf **Einloggen**.

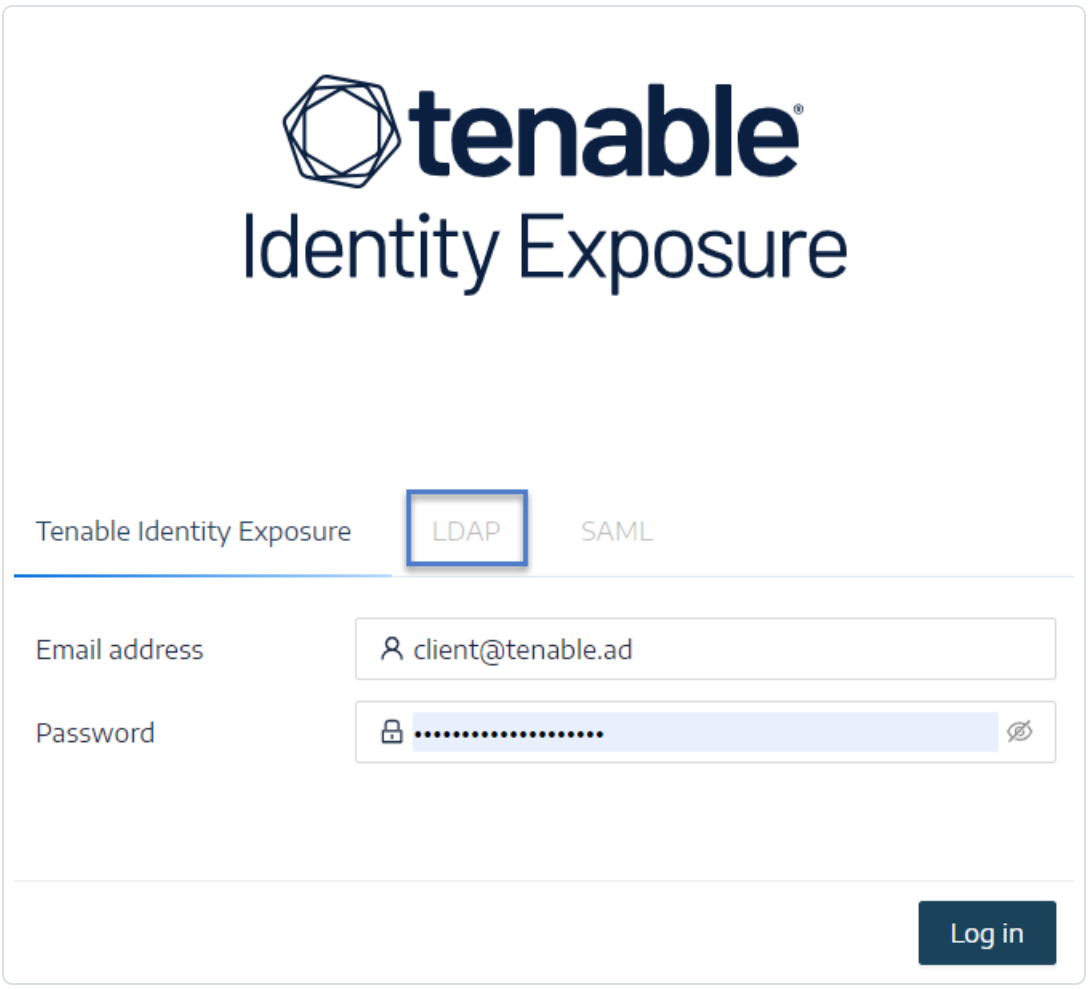
   Die Seite Tenable Identity Exposure wird geöffnet.

LDAP-Konto verwenden

So melden Sie sich mit LDAP an:

1. Geben Sie in einem beliebigen Browser Ihre Client-URL (zum Beispiel: client.tenable.ad) in die Adresszeile ein.

   Das Fenster **Einloggen** wird angezeigt.



2. Klicken Sie auf die Registerkarte **LDAP**.
3. Geben Sie den Namen Ihres LDAP-Kontos ein.
4. Geben Sie Ihr LDAP-Passwort ein.
5. Klicken Sie auf **Einloggen**.

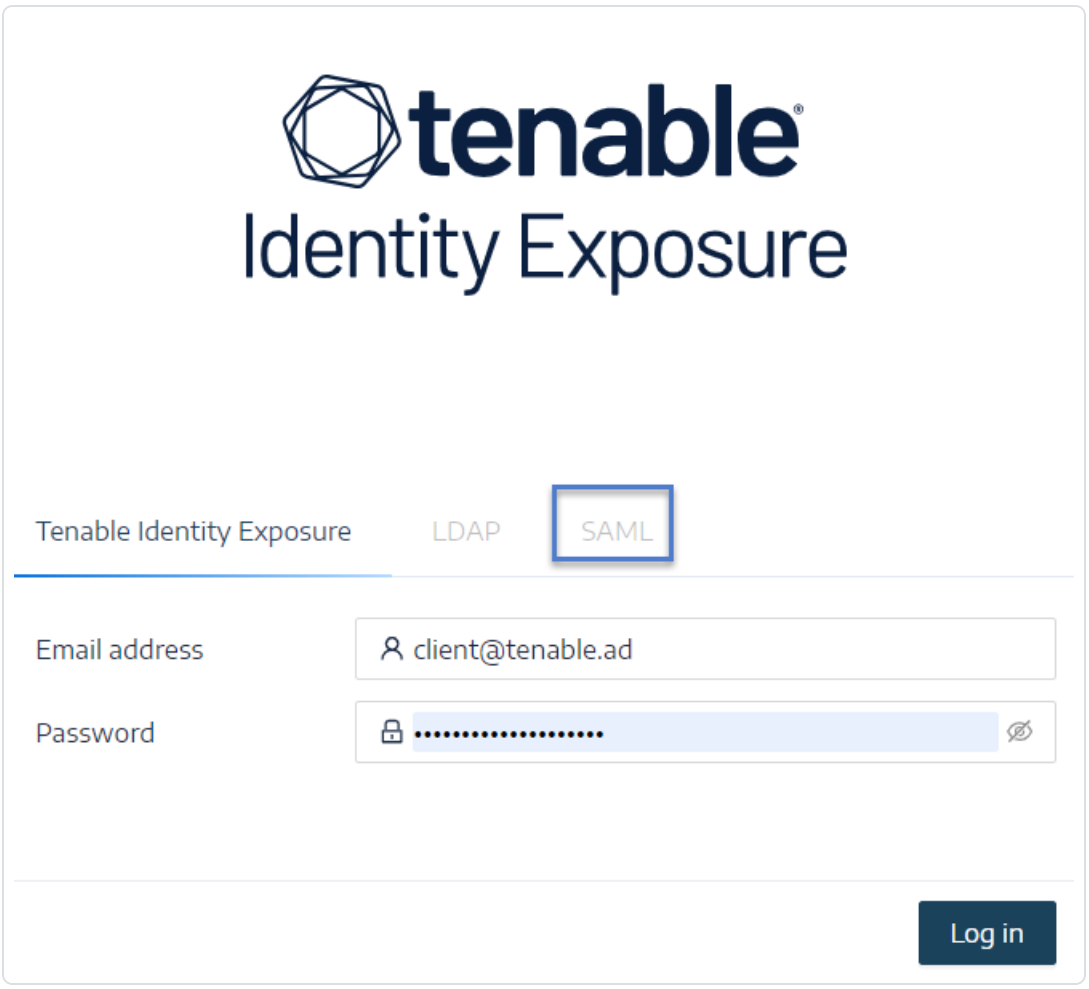
   Die Tenable Identity Exposure-Seite wird geöffnet.

SAML verwenden

So melden Sie sich mit SAML an:

1. Geben Sie in einem beliebigen Browser Ihre Client-URL (zum Beispiel: client.tenable.ad) in die Adresszeile ein.

   Das Fenster **Einloggen** wird angezeigt.



2. Klicken Sie auf die Registerkarte **SAML**.
3. Klicken Sie auf den Link zu Ihrem Identitätsanbieter (IDP).

   Tenable Identity Exposure leitet Sie zur Authentifizierung an Ihren SAML-Server weiter.
4. Geben Sie Ihre Unternehmensanmeldeinformationen bei Ihrem IDP ein.

   Sie werden als eingeloggter Benutzer zu Tenable Identity Exposure weitergeleitet.

Achtung: Wenn das Einloggen wiederholt fehlschlägt, sperrt Tenable Identity Exposure Ihr Konto. Wenden Sie sich an Ihren Administrator.

So melden Sie sich von Tenable Identity Exposure ab:

1. Klicken Sie in Tenable Identity Exposure auf Ihr Benutzersymbol.

   Ein Untermenü wird angezeigt.

2. Klicken Sie auf **Ausloggen**.

   Tenable Identity Exposure zeigt wieder die Login-Seite an.

Auf den Workspace zugreifen

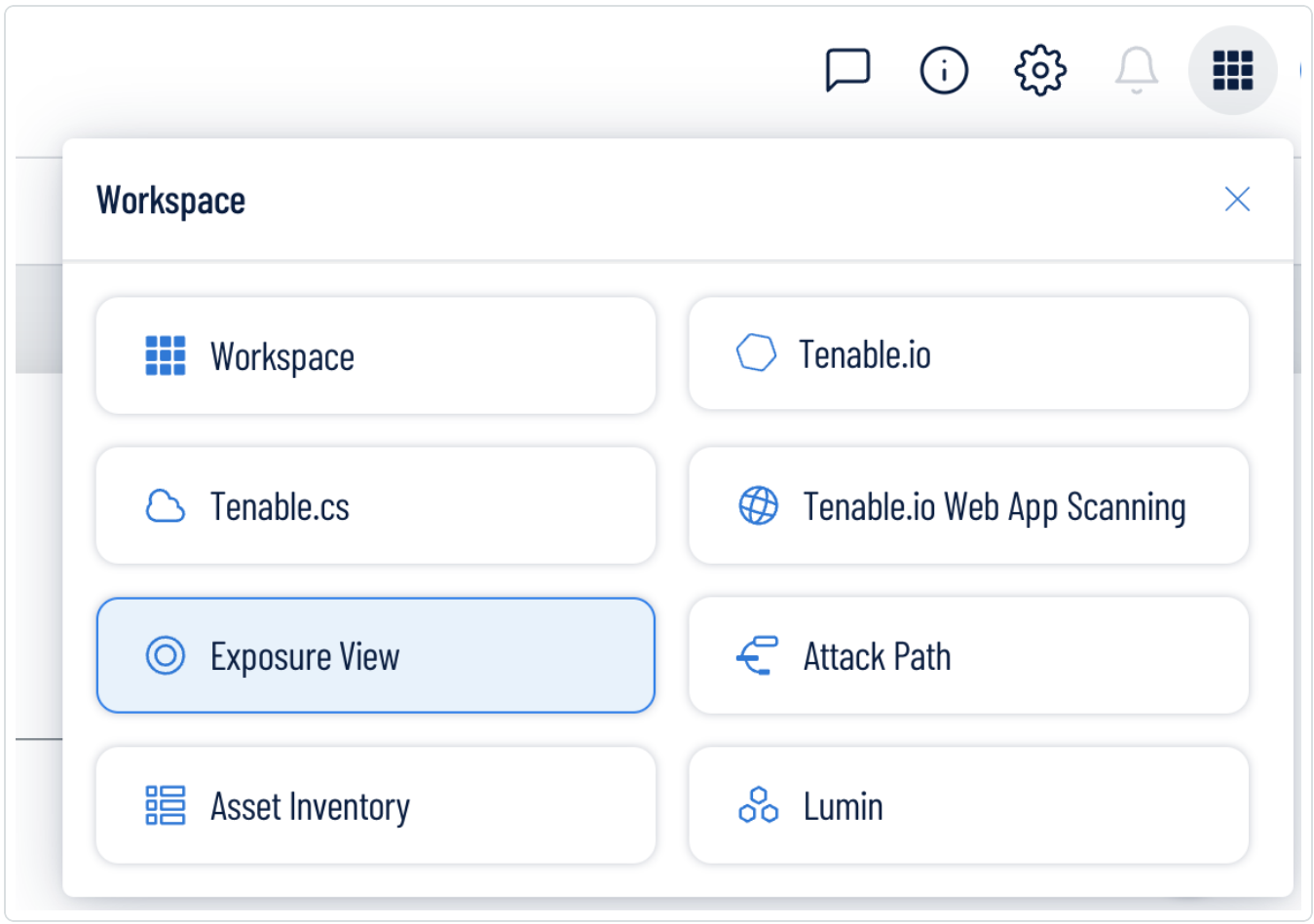
Wenn Sie sich bei Tenable einloggen, wird standardmäßig die Seite **Workspace** angezeigt. Auf der Seite **Workspace** können Sie zwischen den Tenable-Anwendungen wechseln oder eine Standardanwendung festlegen, um die Seite **Workspace** in Zukunft zu überspringen. Zum Wechseln zwischen Anwendungen können Sie auch das Menü **Workspace** in der oberen Navigationsleiste verwenden.

Menü „Workspace“ öffnen

So öffnen Sie das Menü **Workspace**:

1. Klicken Sie in einer beliebigen Tenable-Anwendung in der oberen rechten Ecke auf die Schaltfläche  .

   Das Menü **Workspace** wird angezeigt.



2. Klicken Sie auf eine Anwendungskachel, um die betreffende Anwendung zu öffnen.

Seite „Workspace“ anzeigen

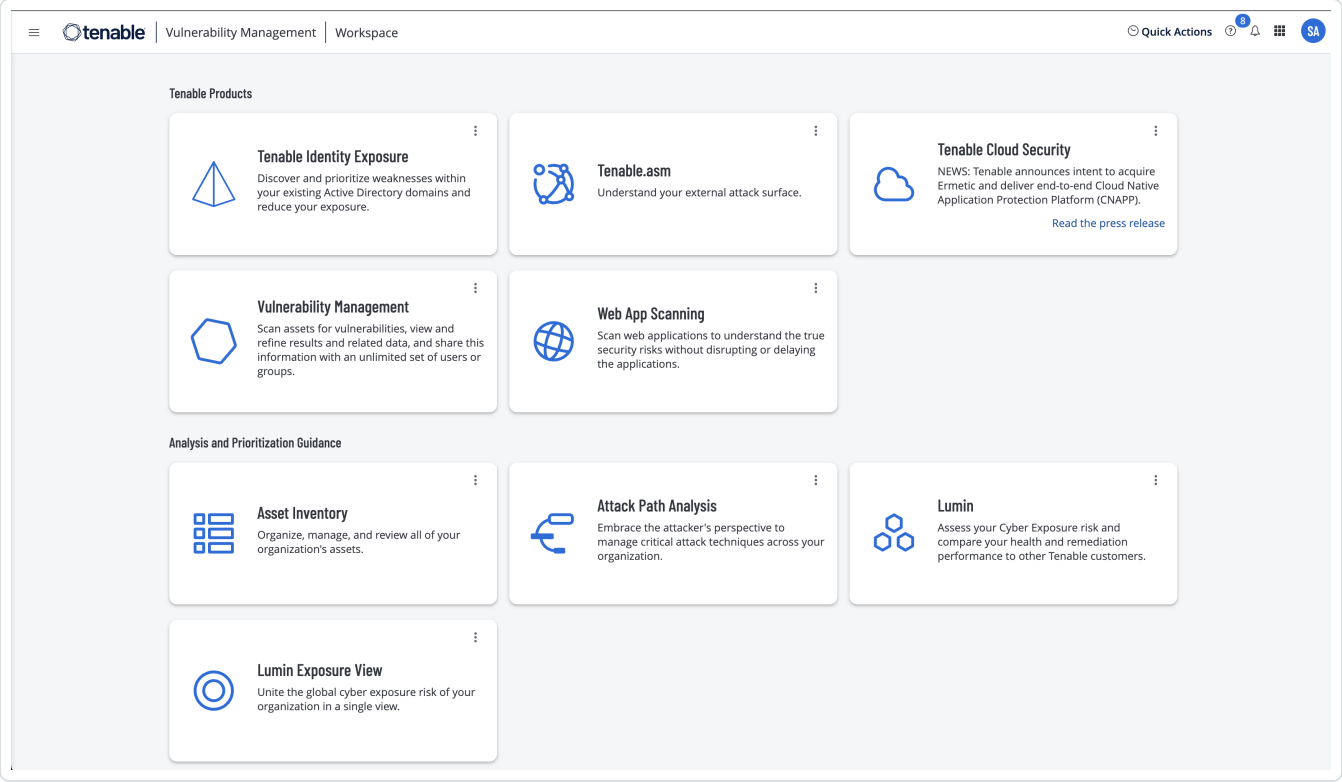
So zeigen Sie die Seite „Workspace“ an:

1. Klicken Sie in einer beliebigen Tenable-Anwendung in der oberen rechten Ecke auf die Schaltfläche .

   Das Menü **Workspace** wird angezeigt.

2. Klicken Sie im Menü **Workspace** auf **Workspace**.

Die Seite **Workspace** wird angezeigt.



Standardanwendung festlegen

Wenn Sie sich bei Tenable einloggen, wird standardmäßig die Seite **Workspace** angezeigt. Sie können jedoch eine Standardanwendung festlegen, um die Seite **Workspace** in Zukunft zu überspringen.

> Standardmäßig können Benutzer mit den Rollen **Administrator**, **Scan Manager**, **Scan Operator**, **Standard** und **Basic** eine Standardanwendung festlegen. Wenn Sie eine andere Rolle haben, wenden Sie sich an Ihren Administrator und fordern Sie unter **Mein Konto** die Berechtigung **Verwalten** an. Weitere Informationen finden Sie unter Benutzerdefinierte Rollen.

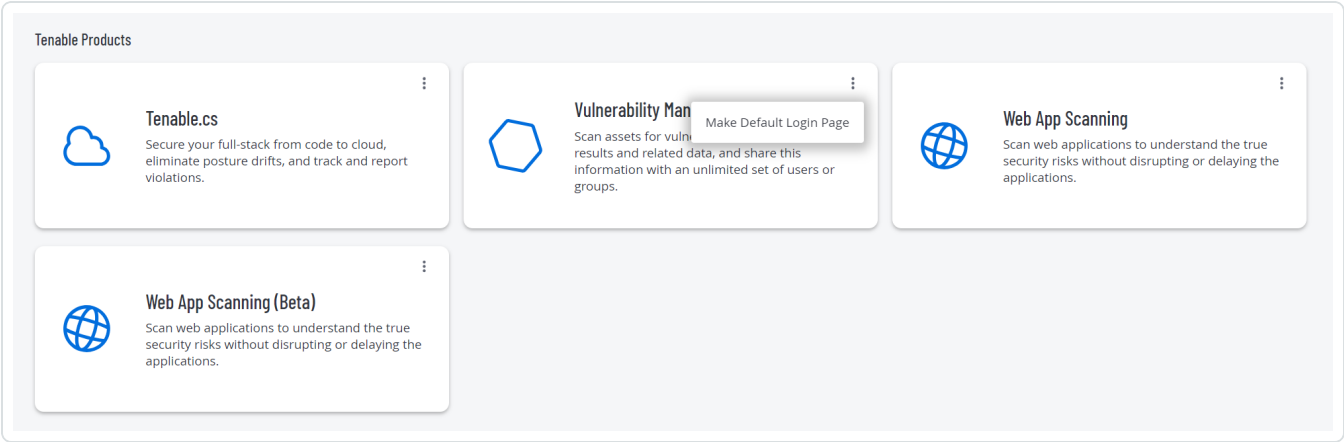
So legen Sie eine Standard-Login-Anwendung fest:

1. Loggen Sie sich bei Tenable ein.

   Die Seite **Workspace** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke der gewünschten Anwendung auf die Schaltfläche ⋮.

Ein Menü wird angezeigt.



3. Klicken Sie im Menü auf **Make Default Login Page** (Als Standard-Login-Seite festlegen).

   Diese Anwendung wird jetzt angezeigt, wenn Sie sich einloggen.

Standardanwendung entfernen

So entfernen Sie eine Standard-Login-Anwendung:

1. Loggen Sie sich bei Tenable ein.

   Die Seite **Workspace** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke der zu entfernenden Anwendung auf die Schaltfläche ⋮.

   Ein Menü wird angezeigt.

3. Klicken Sie auf **Remove Default Login Page** (Standard-Login-Seite entfernen).

   Wenn Sie sich jetzt einloggen, wird die Seite **Workspace** angezeigt.

Benutzervoreinstellungen

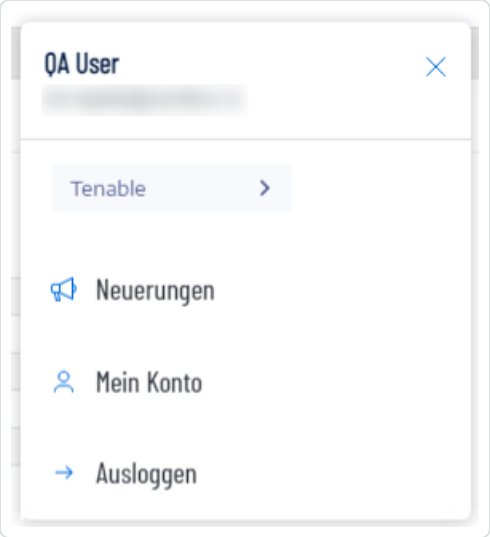
Sie können Ihre Benutzervoreinstellungen in Tenable Identity Exposure festlegen.

- So wählen Sie Ihre Sprache aus:
- So wählen Sie Ihr Profil aus:
- So ändern Sie Ihr Passwort:
- So wählen Sie Ihr Profil aus:

So legen Sie Ihre Voreinstellungen fest:

1. Klicken Sie in Tenable Identity Exposure oben rechts auf Ihr Benutzerprofilsymbol.

   Ein Untermenü wird angezeigt.

2. Wählen Sie **Mein Konto** aus.

   Daraufhin wird die Seite **Voreinstellungen** angezeigt.

So wählen Sie Ihre Sprache aus:

a. Klicken Sie unter **Sprachen** auf den Pfeil der Dropdown-Liste, um Ihre bevorzugte Sprache auszuwählen.

b. Klicken Sie auf **Speichern**.

Eine Meldung bestätigt, dass Tenable Identity Exposure Ihre Voreinstellungen aktualisiert hat. Die Benutzeroberfläche wird in der von Ihnen ausgewählten Sprache angezeigt.

So wählen Sie Ihr Profil aus:

Wenn Sie von einem Sicherheitsprofil zu einem anderen wechseln, ändert sich die Darstellung der Konfiguration der Indikatoren und die Datendarstellung in den Dashboards, Widgets und im Trail Flow in Tenable Identity Exposure.

a. Klicken Sie unter **Voreinstellungen** auf **Profile**.

b. Klicken Sie unter **Bevorzugtes Profil** auf den Dropdown-Pfeil, um Ihr Standardprofil auszuwählen, nachdem Sie eine Verbindung zu Tenable Identity Exposure hergestellt haben.

c. Klicken Sie auf **Speichern**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure Ihre Voreinstellungen aktualisiert hat.

Weitere Informationen finden Sie unter Sicherheitsprofile.

So ändern Sie Ihr Passwort:

> **Hinweis**: Die Passwortinformationen sind nicht verfügbar, wenn Sie über eine Tenable One-Lizenz verfügen. In diesem Fall verwaltet Tenable Vulnerability Management alle Ihre Authentifizierungseinstellungen. Weitere Informationen finden Sie unter „Access Control" im Tenable Vulnerability Management User Guide.

a. Klicken Sie unter **Voreinstellungen** auf **Anmeldeinformationen**.

b. Geben Sie folgende Informationen an:

   - Ihr altes Passwort.
   - Ihr neues Passwort.

c. Geben Sie im Feld **Bestätigung des neuen Passworts** das neue Passwort erneut ein.

d. Klicken Sie auf **Speichern**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure Ihr Passwort geändert hat.

   > **Hinweis**: Es ist nicht möglich, Passwörter für Konten zu ändern, die über externe Anbieter wie LDAP oder SAML in Tenable Identity Exposure verbunden sind.

So verwalten Sie Ihren API-Schlüssel:

a. Klicken Sie unter **Voreinstellungen** auf **API-Schlüssel**.

   Ihr Zugriffstoken wird im Feld **Aktueller API-Schlüssel** angezeigt.

b. Sie haben folgende Möglichkeiten:

c. Klicken Sie auf das ❐-Symbol, um den API-Schlüssel in die Zwischenablage zu kopieren und bei Bedarf zu verwenden.

d. Klicken Sie auf **API-Schlüssel aktualisieren**, um einen neuen Zugriffstoken zu generieren.

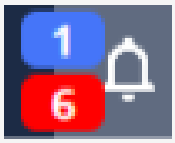
   In einer Meldung werden Sie aufgefordert, den Vorgang zu bestätigen.

   > **Hinweis**: Das Aktualisieren des API-Schlüssels führt dazu, dass Tenable Identity Exposure den aktuellen Token deaktiviert.

Weitere Informationen finden Sie unter Öffentliche API verwenden.

Benachrichtigungen

Oben rechts auf der Startseite von Tenable Identity Exposure werden Sie durch ein Glockensymbol und die Anzahl der Badges über Angriffswarnungen und/oder Exposure-Warnungen informiert, die auf Ihre Bestätigung warten. Wenn neue Warnungen eingehen, erhöht Tenable Identity Exposure die Anzahl des Badge-Zählers.

	**Blau**	Exposure-Warnungen
	Rot	Angriffswarnungen

So zeigen Sie Warnungen an:

1. Klicken Sie in Tenable Identity Exposure auf das Glockensymbol.

   Der Fensterbereich **Warnungen** wird geöffnet.

2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Registerkarte **Exposure-Warnungen**, um Exposure-Warnungen anzuzeigen.
   - Klicken Sie auf die Registerkarte **Angriffswarnungen**, um Angriffswarnungen anzuzeigen.

     Es erscheint eine Liste der zugehörigen Warnungen.

So zeigen Sie das mit der Warnung verbundene Ereignis an:

1. Wählen Sie eine Warnung aus der Liste aus und klicken Sie auf **Aktionen** > **Abweichung anzeigen**.

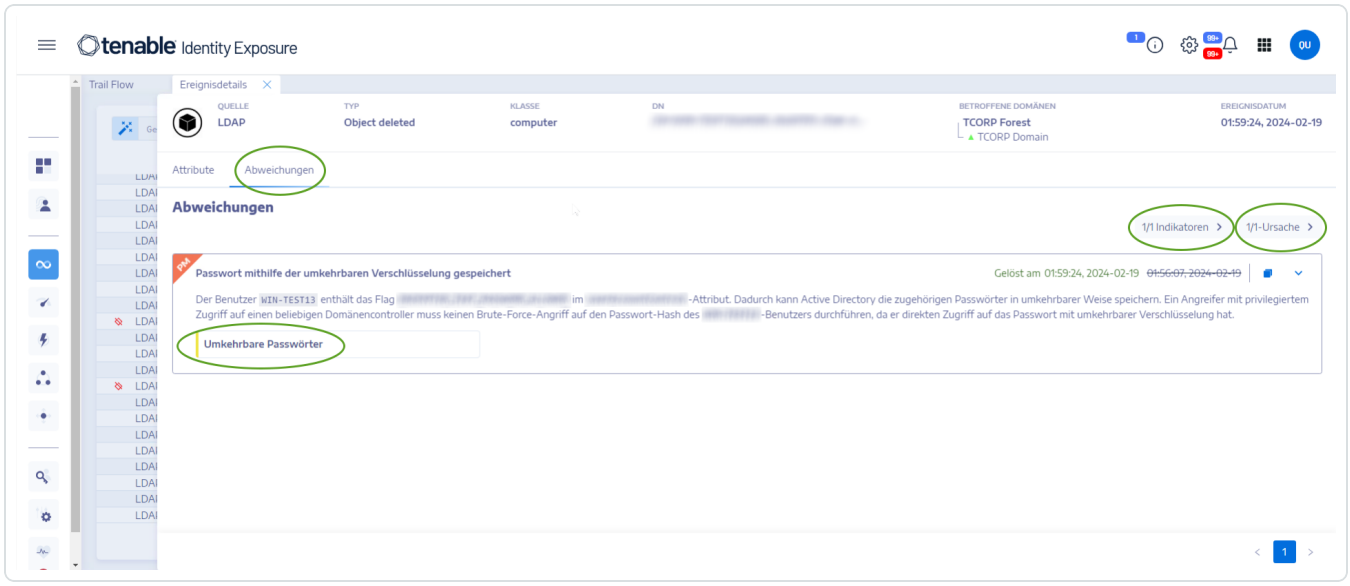
   Der Fensterbereich mit den Ereignisdetails wird mit den folgenden Informationen geöffnet:

   - Quelle (Ereignis-Collector)
   - Objekttyp
   - Datei
   - Pfad

- Betroffene Domänen
- Datum
- Eine Liste von Attributen mit Werten zum Zeitpunkt des Ereignisses und dem aktuellen Wert

2. Klicken Sie auf die Registerkarte **Abweichungen**.

   Der Fensterbereich **Abweichungen** wird mit einer Liste der Abweichungen geöffnet, die mit dem Ereignis verknüpft sind.



3. Klicken Sie auf **n/n Indikatoren**, um den Fensterbereich für den Indicator of Exposure anzuzeigen, der die Warnung ausgelöst hat.
4. Klicken Sie auf **n/n Ursachen**, um die Ursachen für die Warnung anzuzeigen.
5. Klicken Sie auf den Pfeil, um die Informationen zur Warnung zu erweitern oder zu reduzieren.
6. Klicken Sie auf den Namen des Indikators, um die Seite „Indikatordetails“ anzuzeigen.

So archivieren Sie die Warnung:

Nachdem Sie die Warnung angesehen haben, können Sie sie archivieren.

1. Aktivieren Sie im Fensterbereich **Warnungen** in der Liste der Warnungen das Kontrollkästchen für die Warnung, die Sie archivieren möchten.

- Optional können Sie am unteren Rand des Fensterbereichs auf das Kontrollkästchen für **n/n Objekten ausgewählt** klicken, um alle Warnungen auf einmal auszuwählen.

2. Klicken Sie am unteren Rand des Fensterbereichs auf **Aktion auswählen** > **Archivieren**.
3. Klicken Sie auf **OK**.

Dashboards

Mit Dashboards können Sie Daten und Trends visualisieren, die die Sicherheit Ihres Active Directory betreffen. Sie können sie mit Widgets anpassen, um Diagramme und Zähler nach Ihren Wünschen anzuzeigen.

Tenable Identity Exposure bietet Dashboard-Vorlagen, mit denen Sie sich auf Probleme mit hoher Priorität konzentrieren können, die Ihre Organisation betreffen. Dazu gehören die folgenden Vorlagen:

- **AD-Konformität und Hauptrisiken** – Konformitätsbewertung, Entwicklung und Konformität mit Risikokritikalität
- **AD Risk 360** – Abweichungsentwicklung und Probleme nach Schweregrad des Indicator of Exposure
- **Risiko bei Passwortverwaltung** – passwortbezogene Probleme
- **Benutzerüberwachung** – AD-Benutzerentwicklung, Anzahl der Benutzerkategorien
- **Native Administratorüberwachung** – Metriken zu Administratorkonten

So erstellen Sie ein neues Dashboard mithilfe einer Vorlage:

1. Klicken Sie in Tenable Identity Exposure auf  oder **Dashboards**. (Diese Seite wird auch standardmäßig in Tenable Identity Exposure geöffnet.)
2. Sie können einen der folgenden Schritte ausführen:
   - Wenn der Fensterbereich leer ist: Klicken Sie auf **Dashboards hinzufügen**.
   - Wenn der Fensterbereich bereits mindestens ein Dashboard enthält: Klicken Sie in der oberen rechten Ecke auf  > **Neues Dashboard hinzufügen**.

     Der Fensterbereich **Dashboard-Vorlagen konfigurieren** wird geöffnet.
3. Wählen Sie die Dashboards aus, die Sie hinzufügen möchten.
4. Klicken Sie auf **Dashboards hinzufügen**.

5. Eine Meldung bestätigt, dass Tenable Identity Exposure das Dashboard und die Widgets erstellt hat. Die neuen Dashboards werden unter einer Registerkarte im Fensterbereich **Dashboards** angezeigt.

So fügen Sie ein benutzerdefiniertes Dashboard hinzu:

1. Klicken Sie in Tenable Identity Exposure auf  oder **Dashboards**. (Diese Seite wird auch standardmäßig in Tenable Identity Exposure geöffnet.)
2. Klicken Sie oben rechts auf  > **Neues Dashboard hinzufügen**.

   Der Fensterbereich **Dashboard-Vorlagen konfigurieren** wird geöffnet.
3. Wählen Sie unten die Vorlage **Benutzerdefiniertes Dashboard** aus.
4. Geben Sie einen Namen für das Dashboard ein.
5. Klicken Sie auf **Dashboards hinzufügen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure das Dashboard erstellt hat. Die neuen Dashboards werden unter einer Registerkarte im Fensterbereich **Dashboards** angezeigt.
6. Unter Widgets finden Sie Informationen darüber, wie Sie Ihrem Dashboard Widgets hinzufügen können.

So benennen Sie ein Dashboard um:

1. Wählen Sie im Fensterbereich **Dashboards** die Registerkarte für das Dashboard aus, das Sie umbenennen möchten.
2. Klicken Sie oben rechts auf > **Name bearbeiten**.

   Der Fensterbereich **Dashboard konfigurieren** wird geöffnet.
3. Geben Sie im Feld **Name** einen anderen Namen für das Dashboard ein.
4. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure das Dashboard aktualisiert hat.

So löschen Sie ein Dashboard:

1. Wählen Sie im Fensterbereich **Dashboards** die Registerkarte für das Dashboard aus, das Sie löschen möchten.
2. Klicken Sie oben rechts auf ··· > **Dashboard löschen**.

   Der Fensterbereich **Dashboard löschen** öffnet sich und Sie werden aufgefordert, den Löschvorgang zu bestätigen.
3. Klicken Sie auf **Löschen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure das Dashboard gelöscht hat.

Widgets

Mit Widgets in Dashboards können Sie Ihre Active Directory-Daten in Form von Balken- und Liniendiagrammen sowie Zählern visualisieren. Sie können die Widgets so anpassen, dass sie bestimmte Informationen anzeigen, und sie durch Ziehen auf dem Dashboard neu positionieren.

Sie können Widgets zu einem neu erstellten Dashboard oder einem bestehenden Dashboard hinzufügen.

So fügen Sie ein Widget zu einem Dashboard hinzu:

1. Klicken Sie in Tenable Identity Exposure auf  oder **Dashboards**. (Diese Seite wird auch standardmäßig in Tenable Identity Exposure geöffnet.)
2. Wählen Sie im Fensterbereich „Dashboards“ die Registerkarte für das Dashboard aus.
3. Sie können einen der folgenden Schritte ausführen:
   - Wenn das Dashboard leer ist: Klicken Sie auf **Widgets hinzufügen**.
   - Wenn das Dashboard bereits Widgets enthält: Klicken Sie oben rechts auf  > **Widget zum aktuellen Dashboard hinzufügen**.

     Der Fensterbereich **Widget hinzufügen** wird geöffnet.
4. Klicken Sie auf eine Kachel, um eine der folgenden Optionen auszuwählen:
   - Balkendiagramm
   - Liniendiagramm
   - Zähler
5. Geben Sie im Feld **Name des Widgets** einen Namen für das Widget ein.
6. Klicken Sie unter **Widget-Konfiguration** im Feld **Datentyp** auf den Pfeil in der Dropdown-Liste, um eine der folgenden Optionen auszuwählen:

- Benutzeranzahl: Die Anzahl der aktiven Benutzer für die Domäne.
- Anzahl an Abweichungen: Die Anzahl der festgestellten Abweichungen oder Sicherheitsverstöße.
- Konformitätsbewertung: Eine Punktzahl von 0–100, die Tenable Identity Exposure anhand der Anzahl der festgestellten Abweichungen und deren Schweregrad berechnet.
- Dauer (für Liniendiagramm): Klicken Sie auf den Pfeil in der Dropdown-Liste, um die anzuzeigende Dauer auszuwählen.

7. Unter **Dataset-Konfiguration**:

Dataset-Konfiguration	
Status (Anzahl Benutzer)	Wählen Sie „Aktiv", „Inaktiv" oder „Alle" aus.
Indikatoren	a. Klicken Sie auf **Indikatoren**, um mindestens einen Indikator auszuwählen. Der Fensterbereich **Indicators of Exposure** wird geöffnet. b. Wählen Sie einen oder mehrere Indikatoren aus der Liste aus. Optional können Sie auch folgendermaßen vorgehen: ■ Geben Sie einen Indikatornamen in das Suchfeld ein. ■ Wählen Sie alle Indikatoren aus. ■ Wählen Sie alle Indikatoren mit einem bestimmten Schweregrad (Kritisch, Hoch, Mittel oder Gering) aus. c. Klicken Sie auf **Auswahlbasierter Filter**.
Domänen	a. Klicken Sie auf **Domänen**, um mindestens eine Domäne auszuwählen. Der Fensterbereich **Gesamtstrukturen und Domänen** wird geöffnet. b. Wählen Sie eine Domäne aus der Liste aus. Optional können Sie auch folgendermaßen vorgehen: ■ Geben Sie einen Domänennamen in das Suchfeld ein. ■ Wählen Sie alle Domänen aus.

	c. Klicken Sie auf **Auswahlbasierter Filter**.

8. Geben Sie im Feld **Name des Datasets** einen Namen für das Dataset ein.
9. Wählen Sie die Domäne für das Widget aus.

   Optional können Sie einen Domänennamen in das Suchfeld eingeben.
10. Klicken Sie auf **Auswahlbasierter Filter**.
11. Optional können Sie auf **Neues Dataset hinzufügen** klicken, um ein weiteres Dataset mit anderen Optionen für das Widget hinzuzufügen.
12. Klicken Sie auf **Hinzufügen**.

    Eine Meldung bestätigt, dass Tenable Identity Exposure das Widget hinzugefügt hat.

So ändern Sie ein Widget:

1. Klicken Sie in Tenable Identity Exposure auf **Dashboards**.
2. Wählen Sie das Dashboard mit dem Widget aus, das Sie ändern möchten.
3. Wählen Sie das Widget aus.
4. Klicken Sie in der oberen rechten Ecke des Widgets auf das Symbol .

   Der Fensterbereich **Widget ändern** wird geöffnet.
5. Ändern Sie diese nach Bedarf.
6. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure das Widget aktualisiert hat.

So aktualisieren Sie ein Widget:

1. Wählen Sie das Widget aus.
2. Klicken Sie in der oberen rechten Ecke des Widgets auf das Symbol .

   Das Widget wird aktualisiert.

So löschen Sie ein Widget:

1. Klicken Sie in Tenable Identity Exposure auf **Dashboards**.
2. Wählen Sie das Dashboard mit dem Widget aus, das Sie löschen möchten.
3. Wählen Sie das Widget aus.
4. Klicken Sie auf das Symbol  .

   Der Fensterbereich „Widget entfernen" wird geöffnet. In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.
5. Klicken Sie auf **OK**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure das Widget vom Dashboard gelöscht hat.

Siehe auch

- Dashboards

Identitäts-Explorer

Berechtigungen: Um auf die Konfiguration und Datenvisualisierung für Microsoft Entra ID zuzugreifen, muss Ihre Benutzerrolle über die entsprechenden Berechtigungen verfügen. Weitere Informationen finden Sie unter Berechtigungen für eine Rolle festlegen.

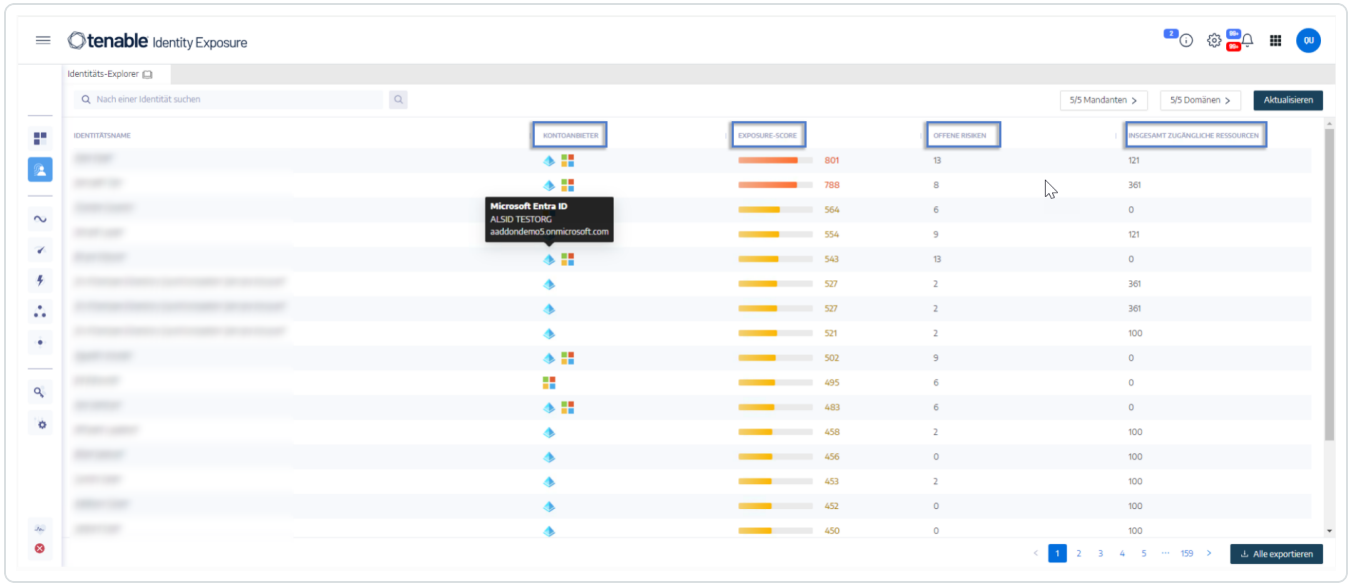
Die Identitäts-Explorer-Ansicht von Tenable Identity Exposure vereinheitlicht Identitäten über Active Directory und Microsoft Entra ID hinweg. Die Ansicht zeigt den Identitätsrisiko-Score (Beta) für jedes aufgelistete Asset und die potenzielle Reichweite kompromittierter Identitäten.

So greifen Sie auf den Identitäts-Explorer zu:

Hinweis: Der Identitäts-Explorer ist nur sichtbar, wenn Sie die Microsoft Entra ID-Funktion verwenden. Weitere Informationen finden Sie unter Microsoft Entra ID-Unterstützung.

- Klicken Sie in Tenable Identity Exposure auf das Identitäts-Explorer-Symbol in der linken Navigationsleiste.

  Der Bereich **Identitäts-Explorer** wird geöffnet.



Im Bereich **Identitäts-Explorer** werden die folgenden Informationen zu den insgesamt zugänglichen Ressourcen angezeigt:

- **Identitätsname** – Name des Benutzerkontos unter dem Identitätsanbieter.
- **Kontoanbieter** – Identitätsanbieter.
- **Exposure Score** – Tenable Identity Exposure berechnet diese Metrik, indem die Kritikalität eines Assets oder einer Identität und ihrer Schwachstellen für jeden Identitätsanbieter bewertet wird, und aggregiert sie, um einen Gesamt-Score für die Exposure einer bestimmten Identität bereitzustellen.

  > **Hinweis**: Tenable Identity Exposure zeigt den Exposure-Score nur an, wenn Sie über die Tenable One-Lizenz verfügen.

- **Offene Risiken** – Anzahl der Ergebnisse, die ein Microsoft Entra ID-Indicator of Exposure erkennt, wenn er das Asset scannt. Weitere Informationen finden Sie unter Indicators of Exposure in Zusammenhang mit Microsoft Entra ID.
- **Insgesamt zugängliche Ressourcen** – Anzahl der Ressourcen jeglicher Art, auf die dieses Asset Zugriff hat (Lesen, Schreiben usw.)

So suchen Sie nach einer Identität:

1. Geben Sie im Feld **Suchen** des Bereichs **Identitäts-Explorer** den Namen des Benutzers oder Kontos ein.
2. Klicken Sie auf das Symbol .

   Tenable Identity Exposure zeigt die passenden Ergebnisse.

So exportieren Sie Identitäten:

1. Klicken Sie unten im Bereich **Identitäts-Explorer** auf **Alle exportieren**.

   Der Bereich **Identitäten exportieren** wird geöffnet.
2. Klicken Sie auf **Alle exportieren**.

   Tenable Identity Exposure lädt die Datei auf den lokalen Computer herunter.

Trail Flow

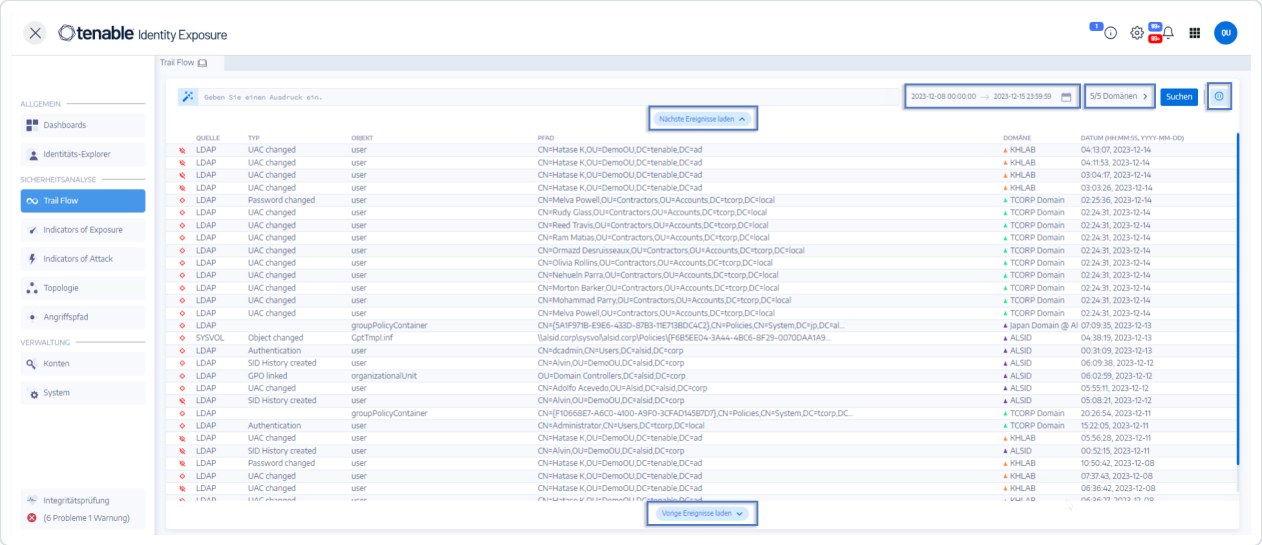
Im Trail Flow in Tenable Identity Exposure wird die Echtzeitüberwachung und Analyse der Ereignisse angezeigt, die Ihre AD-Infrastruktur betreffen. Sie können damit kritische Schwachstellen und die empfohlenen Behebungsmaßnahmen identifizieren.

Auf der Seite **Trail Flow** können Sie in der Zeit zurückgehen und frühere Ereignisse laden oder nach bestimmten Ereignissen suchen. Sie können auch das Suchfeld oben auf der Seite verwenden, um nach Bedrohungen zu suchen und bösartige Muster zu erkennen.

So greifen Sie auf den Trail Flow zu:

- Klicken Sie in Tenable Identity Exposure in der Navigationsleiste auf der linken Seite auf **Trail Flow**.

  Die Trail Flow-Seite wird mit einer Liste von Ereignissen geöffnet. Weitere Informationen finden Sie unter Trail Flow-Tabelle.



So wählen Sie einen Zeitrahmen aus:

1. Klicken Sie oben auf der **Trail Flow**-Seite auf das Kalenderfeld.
2. Wählen Sie ein Start- und ein Enddatum aus.
3. Klicken Sie auf **Suchen**.

   Tenable Identity Exposure aktualisiert die Trail Flow-Tabelle mit dem ausgewählten Zeitrahmen.

So wählen Sie eine Domäne aus:

1. Klicken Sie oben auf der **Trail Flow**-Seite auf **n/n Domäne >**.

   Der Fensterbereich **Gesamtstrukturen und Domänen** wird geöffnet.

2. Wählen Sie die Gesamtstrukturen und Domänen aus.
3. Klicken Sie auf **Auswahlbasierter Filter**.

   Tenable Identity Exposure aktualisiert die Trail Flow-Tabelle mit Informationen für die ausgewählte Gesamtstruktur und Domäne.

So zeigen Sie ein Ereignis an:

- Klicken Sie in der Trail Flow-Tabelle auf eine Zeile, die das Ereignis enthält, das Sie untersuchen möchten.

  Der Fensterbereich „Ereignisdetails" wird geöffnet. Weitere Informationen finden Sie unter Ereignisdetails.

So halten Sie den Trail Flow an und starten ihn neu:

- Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf das Symbol ⏸, um den Trail Flow anzuhalten.

    Wenn Sie den Trail Flow anhalten, wird das automatische vertikale Scrollen der neuesten Ereignisse gestoppt, während die Analyse im Hintergrund weiterläuft. Sie können dann eine Suche nach Ereignissen durchführen.
  - Klicken Sie auf das Symbol ▶, um den Trail Flow neu zu starten.

So laden Sie die nächsten oder vorherigen Ereignisse:

- Führen Sie auf der Trail Flow-Seite einen der folgenden Schritte aus:
  - Klicken Sie auf „Nächste Ereignisse laden".
  - Klicken Sie auf „Vorherige Ereignisse laden".

Trail Flow-Tabelle

Tenable Identity Exposure listet die Ereignisse in Ihrem Active Directory in der Trail Flow-Tabelle kontinuierlich auf, sobald sie auftreten. Sie enthält die folgenden Informationen:

Informationen	Beschreibung
Quelle	Hier wird der Ursprung jeder sicherheitsrelevanten Änderung an Ihren AD-Infrastrukturen aufgeführt. Es gibt zwei mögliche Quellen: • Das Lightweight Directory Access Protocol (LDAP), das für die Kommunikation mit Ihrer AD-Infrastruktur verwendet wird. • Das SMB-Protokoll (Server Message Block), das für die gemeinsame Nutzung von Dateien, Druckern usw. verwendet wird. **Tenable Identity Exposure** führt sorgfältige Analysen des LDAP- und SMB-Datenverkehrs in Ihrem Netzwerk durch, um Anomalien und potenzielle Bedrohungen zu erkennen. **Hinweis**: Mit Active Directory (AD) können Administratoren Gruppenrichtlinien erstellen, die Einstellungen für Benutzer- und Computerkonten steuern. Das Gruppenrichtlinienobjekt (Group Policy Object, GPO) speichert diese Steuerungseinstellungen. GPO-Dateien werden im Sysvol-Ordner auf dem Domänencontroller gespeichert. Es ist wichtig, den Inhalt von GPOs im Hinblick auf die Sicherheit Ihres AD zu überwachen, da jedes Domänenmitglied mit hohen Berechtigungen sie anwenden oder ausführen kann.
Typ	Zeigt die charakteristischen Elemente eines Ereignisses an, zum Beispiel: • ACL geändert • SPN geändert • Mitglied entfernt • Neues Mitglied • Neue Vertrauensstellung • Unbekannter Dateityp hinzugefügt

	• Neues Objekt • Objekt entfernt • Passwort geändert • UAC geändert • Neues GPO verlinkt • GPO-Link entfernt • Besitzerwechsel • Datei umbenannt • SPN erstellt • Zurücksetzen der Authentifizierung fehlgeschlagen • Authentifizierung fehlgeschlagen
Objekt	Gibt die Klasse oder Dateierweiterung an, die mit einem AD-Objekt verknüpft ist. Sie können nach einem Verzeichnisobjekt (Benutzer, Computer usw.) oder nach einer Datei mit einer bestimmten Dateinamenerweiterung (INI, XML, CSV) suchen.
Pfad	Gibt den vollständigen Pfad zu einem AD-Objekt an, um den eindeutigen Standort dieses Objekts im AD zu identifizieren.
Verzeichnis	Gibt an, aus welchem Verzeichnis die Änderung in Ihrer AD-Infrastruktur stammt.
Datum	Gibt den Zeitpunkt des Ereignisses an.

Suche im Trail Flow mit dem Assistenten

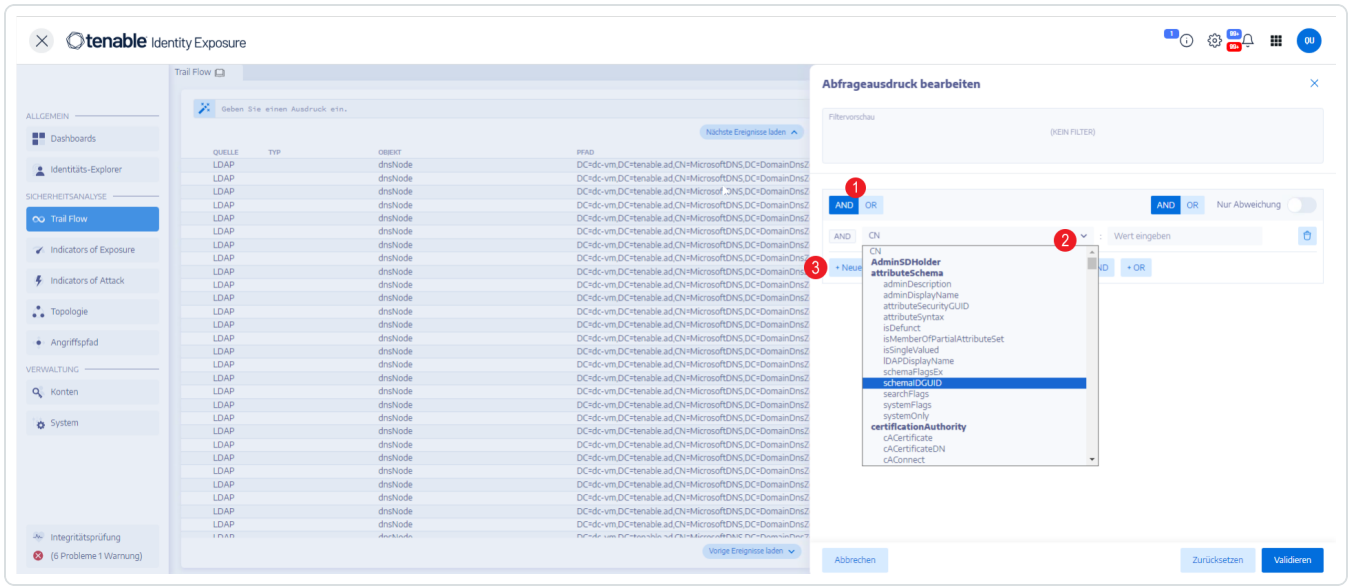
Mit dem Suchassistenten können Sie Abfrageausdrücke erstellen und kombinieren.

- Wenn Sie häufige Ausdrücke im Suchfeld verwenden, können Sie diese für eine spätere Verwendung zu einer Liste von Lesezeichen hinzufügen.
- Wenn Sie einen Ausdruck in das Suchfeld eingeben, speichert Tenable Identity Exposure diesen Ausdruck im Fensterbereich „Verlauf“, damit Sie ihn wiederverwenden können.

So suchen Sie mit dem Assistenten:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow“ zu öffnen.
2. Klicken Sie auf das Symbol .

   Der Fensterbereich **Abfrageausdruck bearbeiten** wird geöffnet. Weitere Informationen finden Sie unter Trail Flow-Abfragen anpassen.



3. Um den Abfrageausdruck im Bereich zu definieren, klicken Sie zunächst auf die **AND**- oder **OR**-Operatorschaltfläche (1), um die erste Bedingung anzuwenden.
4. Wählen Sie ein Attribut aus dem Dropdown-Menü und geben Sie den Wert ein (2).
5. Führen Sie einen der folgenden Schritte aus:

- Um ein Attribut hinzuzufügen, klicken Sie auf **+ Neue Regel hinzufügen** (3).
- Um eine weitere Bedingung hinzuzufügen, klicken Sie auf **Neue Bedingung hinzufügen+AND**- oder **+OR**-Operator. Wählen Sie ein Attribut aus dem Dropdown-Menü und geben Sie den Wert ein.
- Um die Suche auf abweichende Objekte einzuschränken, klicken Sie zum Aktivieren auf den Schalter **Nur Abweichungen**. Wählen Sie den Operator **+AND** oder **+OR** aus, um die Bedingung zur Abfrage hinzuzufügen.
- Um eine Bedingung oder Regel zu löschen, klicken Sie auf das Symbol 🗑.

6. Klicken Sie auf **Validieren**, um die Suche auszuführen, oder auf **Zurücksetzen**, um die Abfrageausdrücke zu ändern.

Siehe auch

- Trail Flow manuell durchsuchen
- Suche im Trail Flow mit dem Assistenten
- Trail Flow-Abfragen anpassen
- Lesezeichen-Abfragen
- Verlauf abfragen

Trail Flow manuell durchsuchen

Um Ereignisse zu filtern, die mit bestimmten Zeichenfolgen oder Mustern übereinstimmen, können Sie einen Ausdruck in das Suchfeld eingeben, um die Ergebnisse mit den booleschen Operatoren *****, **AND** und **OR** zu präzisieren. Sie können **OR**-Anweisungen in Klammern einschließen, um die Suchpriorität zu ändern. Bei der Suche wird nach einem bestimmten Wert in einem Active Directory-Attribut gesucht.

So können Sie den Trail Flow manuell durchsuchen:

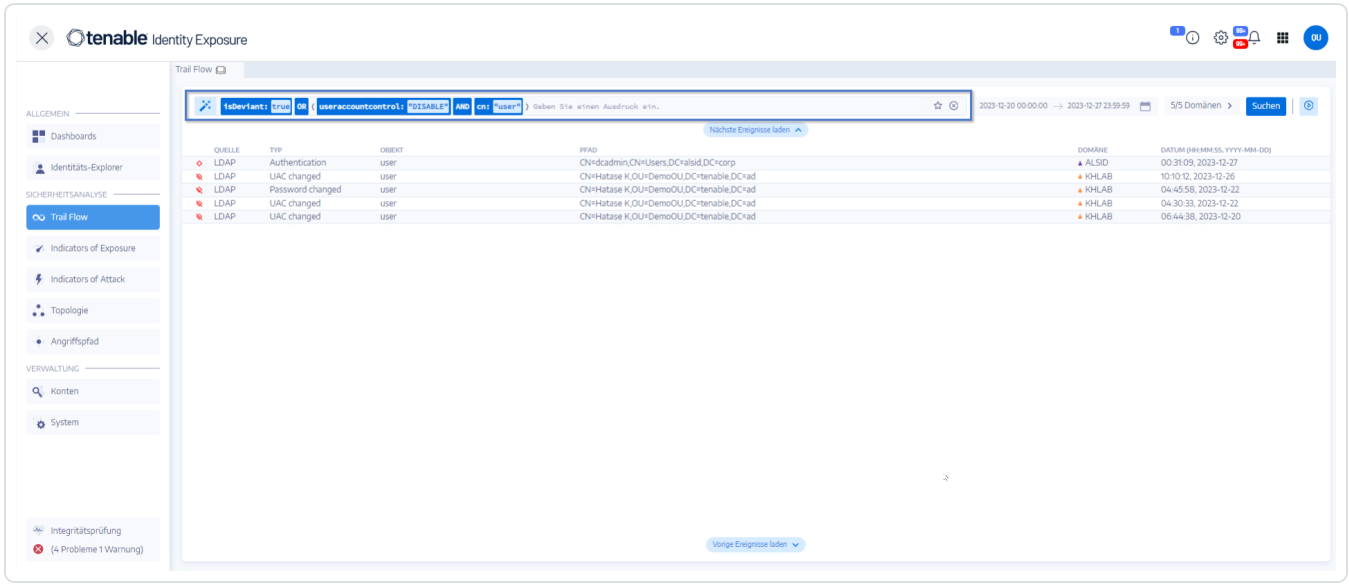
1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Geben Sie im Suchfeld einen Abfrageausdruck ein.
3. Sie können die Suchergebnisse wie folgt filtern:
    - Klicken Sie auf das Feld **Kalender**, um ein Start- und ein Enddatum auszuwählen.
    - Klicken Sie auf **n/n Domänen**, um Gesamtstrukturen und Domänen auszuwählen.
4. Klicken Sie auf **Suchen**.

    Tenable Identity Exposure aktualisiert die Liste mit den Ergebnissen, die Ihren Suchkriterien entsprechen.

Beispiel:

In diesem Beispiel wird nach Folgendem gesucht:

- Deaktivierte Benutzerkonten, die überwachte AD-Infrastrukturen gefährden können.
- Verdächtige Aktivitäten und anormale Kontonutzung.



Grammatik und Syntax

Ein manueller Abfrageausdruck verwendet die folgende Grammatik und Syntax:

- Grammatik: `EXPRESSION [OPERATOR EXPRESSION]*`
- Syntax: `__KEY__ __SELECTOR__ __VALUE__`

  Bedeutung:

  - `__KEY__` bezieht sich auf das zu durchsuchende AD-Objektattribut (wie `CN`, `userAccountControl`, `members` usw.)
  - `__SELECTOR__` bezieht sich auf den Operator: `:`, `>`, `<`, `>=`, `<=`.
  - `__VALUE__` bezieht sich auf den zu suchenden Wert.

    Sie können mehr Schlüsselwörter verwenden, um nach bestimmten Inhalten zu suchen:

  - `isDeviant` sucht nach Ereignissen, die eine Abweichung verursacht haben

Sie können mehrere Trail Flow-Abfrageausdrücke mit den Operatoren **AND** und **OR** kombinieren.

Beispiele:

- Suche nach allen Objekten, die die Zeichenfolge `alice` im Attribut für den allgemeinen Namen enthalten: `cn:"alice"`
- Suche nach allen Objekten, die die Zeichenfolge `alice` im Attribut für den allgemeinen Namen enthalten und zu einer konkreten Abweichung geführt haben: `isDeviant:"true" and cn:"alice"`
- Suche nach einem GPO mit dem Namen „Default Domain Policy“: `objectClass: "groupPolicyContainer" and displayname: "Default Domain Policy"`
- Suche nach allen deaktivierten Konten mit einer SID, die S-1-5-21 enthält: `userAccountControl: "DISABLE" und objectSid: "S-1-5-21"`
- Suche nach allen `script.ini`-Dateien in Sysvol: `globalpath: "sysvol" and types: "SCRIPTSini"`

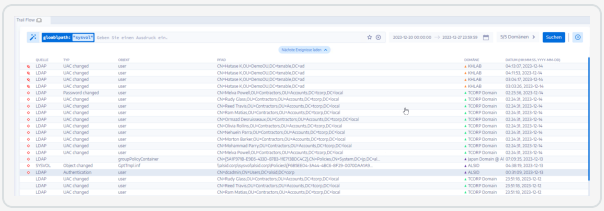
> **Hinweis**: Hier bezieht sich `types` auf das Objektattribut und nicht auf die Spaltenüberschrift.

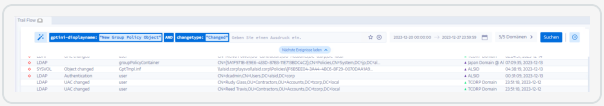
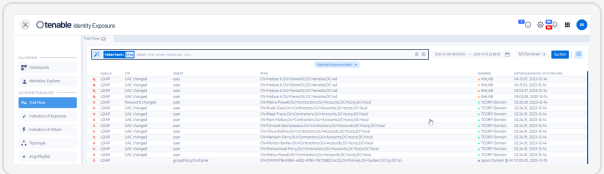
Trail Flow-Abfragen anpassen

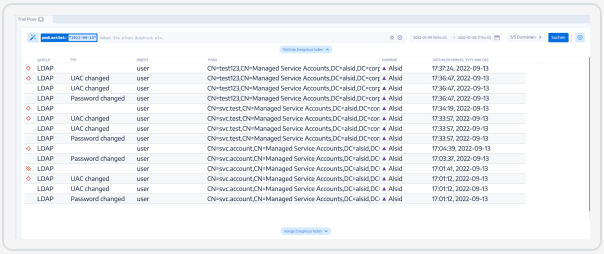
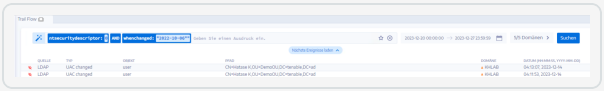
Mit dem Trail Flow können Sie die Funktionen von Tenable Identity Exposure über die standardmäßige Überwachung von Indicators of Exposure und Indicators of Attack hinaus erweitern. Sie können benutzerdefinierte Abfragen erstellen, um Daten schnell abzurufen. Außerdem können Sie die Abfrage als benutzerdefinierte Warnung verwenden, die Tenable Identity Exposure an Ihr Security Information and Event Management (SIEM)-System senden kann.

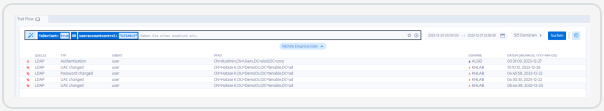
Die folgenden Beispiele zeigen praktische benutzerdefinierte Abfragen in Tenable Identity Exposure.

Anwendungsfall	Beschreibung

Überwachung von Binärdateien zum Starten und Herunterfahren von GPOs und Überwachung des globalen SYSVOL-Pfads	Überwacht auf Skripts im Systemstartpfad und/oder im globalen SYSVOL-Replikationspfad. Angreifer nutzen diese Skripte häufig, um native AD-Dienste zu missbrauchen und Ransomware schnell in einer Umgebung zu verbreiten.
	• **Abfrage für Skripts im Startpfad:**
	`globalpath: "sysvol" AND types: "Scriptsini"`
	Hinweis: Hier bezieht sich `types` auf das Objektattribut und nicht auf die Spaltenüberschrift.
	• **Abfrage für SYSVOL-Überwachung**:
	`globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")`
	 

Änderungen der GPO-Konfiguration	Überwacht auf Änderungen an GPO-Konfigurationen. Angreifer verwenden diese Methode häufig, um Sicherheitseinstellungen herunterzustufen und so eine Persistenz und/oder Kontoübernahme zu ermöglichen. • **Abfrage für GPO-Überwachung:** `gptini-displayname:"Neues Gruppenrichtlinienobjekt" AND changetype:"Geändert"` 
Fehlgeschlagene Authentifizierung und Passwortrücksetzung	Überwacht auf mehrere fehlgeschlagene Authentifizierungsversuche, die zu einer Sperre führen, was als Frühwarnkennzeichen für Brute-Force-Versuche dienen kann. **Hinweis**: Sie müssen die Sperrrichtlinie und die Datums-/Uhrzeitvariablen festlegen. Weitere Informationen finden Sie unter Authentifizierung über ein Tenable Identity Exposure-Konto. • **Abfrage für fehlgeschlagene Authentifizierung:** `useraccountcontrol:"Normal" AND badpwdcount:"<SCHWELLENWERT_FÜR_KONTOSPERRE>" AND badpasswordtime:"<DATUMS-/UHRZEITSTEMPEL>"` 

	• **Abfrage für Passwortrücksetzung:** `pwdlastset:" <DATUMS-/UHRZEITSTEMPEL>"` 
Objektberechtigungen hinzugefügt, entfernt oder geändert	Überwacht auf nicht autorisierte Änderungen an ACL-Rechten und zugehörigen Objektberechtigungssätzen. Angreifer missbrauchen diese Methode, um Berechtigungen zu erhöhen. **Hinweis**: Sie müssen die Datums-/Uhrzeitvariable angeben. • **Abfrage für Objektberechtigungen:** `ntsecuritydescriptor:0 AND whenchanged:"DATUMS-/UHRZEITSTEMPEL"` 
Änderungen an Administratoren, die zu einer Abweichung führen	Integrierte Administratorgruppen und benutzerdefinierte Gruppen sind sensible Gruppen, die eine genaue Überwachung auf Abweichungen oder Konfigurationsänderungen erfordern, die ein Risiko darstellen können. Mit dieser Abfrage können Sie schnell die letzten Änderungen überprüfen, die sich negativ auf die Sicherheitseinstellungen in der Administratorengruppe ausgewirkt haben könnten. • **Abfrage für Änderungen an Administratoren:**

	`isDeviant:true AND cn:"admins"` 

Siehe auch

- Trail Flow manuell durchsuchen
- Suche im Trail Flow mit dem Assistenten
- Lesezeichen-Abfragen
- Verlauf abfragen
- Trail Flow-Anwendungsfälle

Lesezeichen-Abfragen

Wenn Sie häufige Abfrageausdrücke verwenden, können Sie diese zu einer Liste von benutzerdefinierten Lesezeichen hinzufügen, um sie erneut zu verwenden.

So wird ein Abfrageausdruck mit einem Lesezeichen versehen:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie neben dem Suchfeld auf das Symbol  .

   Der Fensterbereich **Abfrageausdruck bearbeiten** wird geöffnet.
3. Geben Sie im Suchfeld einen Abfrageausdruck ein.
4. Klicken Sie neben dem Suchfeld auf das Symbol  .

   Das Feld **Zu Ihren Lesezeichen hinzufügen** wird angezeigt.
5. Klicken Sie im Feld **Ordner wählen** auf den Dropdown-Pfeil, um einen Ordner aus der Liste auszuwählen.
6. (Optional) Stellen Sie den Umschalter **Neuen Ordner erstellen** auf **Ja** um. Geben Sie im Feld **Name des Ordners** einen Namen für den Lesezeichenordner ein.
7. Geben Sie im Feld **Name des Lesezeichens** einen Namen für das Lesezeichen ein.
8. Klicken Sie auf **Hinzufügen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure das Lesezeichen zur Liste hinzugefügt hat.

So verwenden Sie einen mit Lesezeichen versehenen Abfrageausdruck:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie in das Suchfeld.

   Die Registerkarten **Verlauf** und **Lesezeichen** werden unter dem Suchfeld angezeigt.
3. Klicken Sie auf die Registerkarte **Lesezeichen**.

   Die Liste der Lesezeichen wird angezeigt.

4. Klicken Sie auf das Lesezeichen, um es auszuwählen.

   Tenable Identity Exposure lädt den Abfrageausdruck und führt die Suche aus.

So verwalten Sie Ihre Lesezeichen:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie in das Suchfeld.

   Die Registerkarten **Verlauf** und **Lesezeichen** werden unter dem Suchfeld angezeigt.
3. Klicken Sie auf die Registerkarte **Lesezeichen**.

   Die Liste der Lesezeichen wird angezeigt.
4. Klicken Sie auf **Lesezeichen verwalten**.

   Der Fensterbereich **Lesezeichen** wird geöffnet.
5. Führen Sie einen der folgenden Schritte aus:
   - Nach einem Lesezeichen suchen:
     a. Geben Sie den Namen des Lesezeichens in das Suchfeld ein.
     b. Wählen Sie einen Ordner aus der Dropdown-Liste aus.
   - Namen eines Lesezeichens oder eines Lesezeichenordners bearbeiten:
     a. Klicken Sie auf das Symbol für das Lesezeichen oder den Lesezeichenordner.
     b. Geben Sie im Feld **Name des Lesezeichens** oder **Name des Ordners** einen Namen für das Lesezeichen bzw. den Lesezeichenordner ein.
     c. Klicken Sie auf **Bearbeiten**.

        Eine Meldung bestätigt, dass Tenable Identity Exposure den Namen des Lesezeichens oder des Lesezeichenordners aktualisiert hat.
   - Ein Lesezeichen oder einen Lesezeichenordner löschen:
     - Klicken Sie auf das Symbol für das Lesezeichen oder den Lesezeichenordner.

Siehe auch

- Trail Flow manuell durchsuchen
- Suche im Trail Flow mit dem Assistenten
- Trail Flow-Abfragen anpassen
- Verlauf abfragen
- Trail Flow-Anwendungsfälle

Verlauf abfragen

Wenn Sie einen Ausdruck in das Suchfeld eingeben, speichert Tenable Identity Exposure diesen Ausdruck im Fensterbereich „Verlauf“, damit Sie ihn wiederverwenden können.

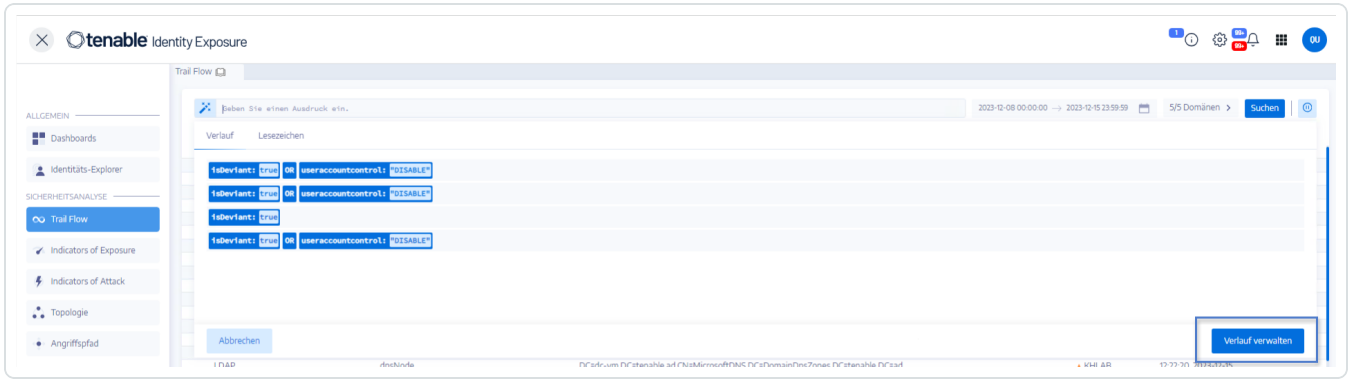
So verwenden Sie einen Abfrageausdruck im Verlauf:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow“ zu öffnen.
2. Klicken Sie in das Suchfeld.

   Die Registerkarten **Verlauf** und **Lesezeichen** werden unter dem Suchfeld angezeigt.
3. Klicken Sie auf die Registerkarte **Verlauf**.

   Die Liste der Abfrageausdrücke wird angezeigt.
4. Klicken Sie, um einen Abfrageausdruck auszuwählen, den Sie verwenden möchten.

   Tenable Identity Exposure lädt den Abfrageausdruck und führt die Suche aus.



So verwalten Sie den Verlauf Ihrer Abfrageausdrücke:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow“ zu öffnen.
2. Klicken Sie in das Suchfeld.

   Die Registerkarten **Verlauf** und **Lesezeichen** werden unter dem Suchfeld angezeigt.
3. Klicken Sie auf die Registerkarte **Verlauf**.

   Die Liste der Abfrageausdrücke wird angezeigt.
4. Klicken Sie auf **Verlauf verwalten**.

Der Fensterbereich **Verlauf** wird geöffnet.

5. Führen Sie einen der folgenden Schritte aus:

- Nach einem Abfrageausdruck suchen:
    a. Geben Sie im Suchfeld einen Abfrageausdruck ein.
    b. Klicken Sie auf das Kalenderfeld, um ein Start- und ein Enddatum auszuwählen.
    c. Klicken Sie auf **Suchen**.
- So löschen Sie einen Abfrageausdruck aus dem Verlauf:
    - Klicken Sie auf das Symbol  .
- So entfernen Sie alle Abfrageausdrücke aus dem Verlauf:
    a. Klicken Sie auf **Auswahl löschen**.

    In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.

    b. Klicken Sie auf **Bestätigen**.

Siehe auch

- Trail Flow manuell durchsuchen
- Suche im Trail Flow mit dem Assistenten
- Trail Flow-Abfragen anpassen
- Lesezeichen-Abfragen
- Trail Flow-Anwendungsfälle

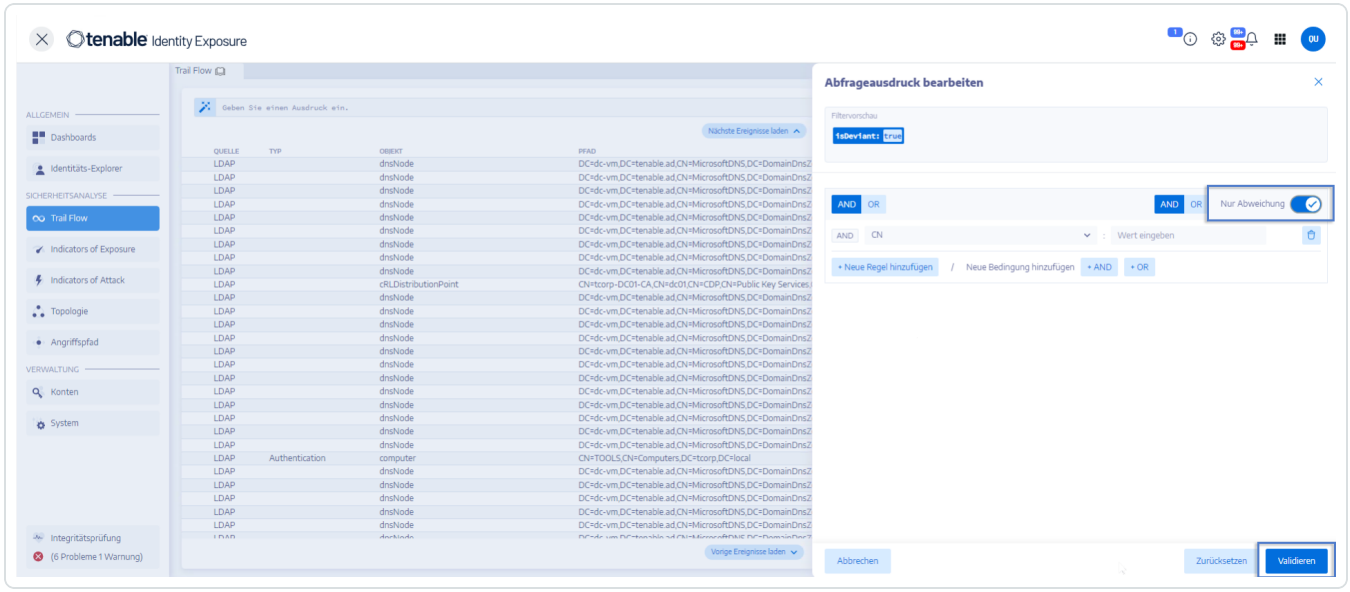
Abweichende Ereignisse anzeigen

Sie können abweichende Ereignisse direkt in der Trail Flow-Tabelle ausfindig machen.

So zeigen Sie nur abweichende Ereignisse an:

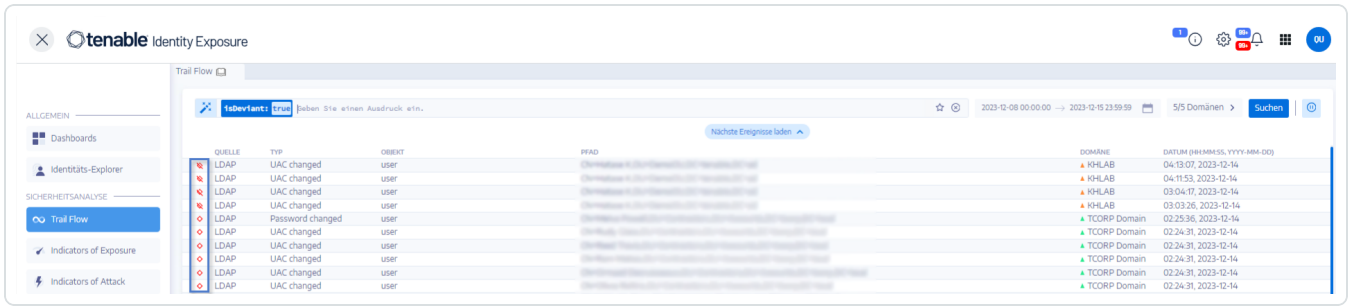
1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie neben dem Suchfeld auf das Symbol .

   Der Fensterbereich **Abfrageausdruck bearbeiten** wird geöffnet.



3. Klicken Sie zum Aktivieren auf den Schalter **Nur Abweichung**.
4. Klicken Sie auf **Validieren**.

   Tenable Identity Exposure aktualisiert die Trail Flow-Tabelle mit einer Liste von Ereignissen mit einer roten Raute neben der Quelle.



Bedeutung:

- ◇ Der Trail Flow hat eine Abweichung im Tenable Identity Exposure-Sicherheitsprofil festgestellt.
- ◆ Der Trail Flow hat eine Abweichung in anderen Sicherheitsprofilen festgestellt.
- Zeigt, dass die Abweichung durch Änderungen behoben wurde.

Ereignisdetails

Der Trail Flow in Tenable Identity Exposure liefert detaillierte Informationen zu jedem Ereignis, das Ihr Active Directory (AD) betrifft. Anhand der Details zu einem bestimmten Ereignis können Sie die technischen Informationen überprüfen und die jeweiligen Maßnahmen ergreifen, die der Schweregrad des Indicator of Exposure (IoE) erfordert.

Ereignisdetails anzeigen:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie, um einen Eintrag aus der Tabelle „Trail Flow" auszuwählen.

   Der Fensterbereich **Ereignisdetails** wird geöffnet.

IoE, Ereignis und abweichendes Objekt

- Ein **Indicator of Exposure** (IoE) beschreibt eine Bedrohung, die das AD betrifft. Die IoEs von Tenable Identity Exposure bewerten das Sicherheitsniveau nach Erhalt eines Ereignisses in Echtzeit. IoEs können verschiedene technische Schwachstellen umfassen. IoEs liefern Informationen über erkannte Schwachstellen, zugehörige abweichende Objekte und Empfehlungen für Behebungsmaßnahmen.
- Ein **Ereignis** zeigt eine sicherheitsrelevante Änderung an, die in einem AD auftreten kann. Dabei kann es sich um eine Passwortänderung, die Erstellung eines Benutzers, ein neues oder geändertes GPO, ein neues delegiertes Recht usw. handeln. Ein Ereignis kann den Compliance-Status eines IoE ändern, von konform zu nicht konform.
- Ein **abweichendes Objekt** ist ein technisches Element, das (allein oder in Verbindung mit einem anderen abweichenden Objekt) das Funktionieren des Angriffsvektors eines IoE ermöglicht.

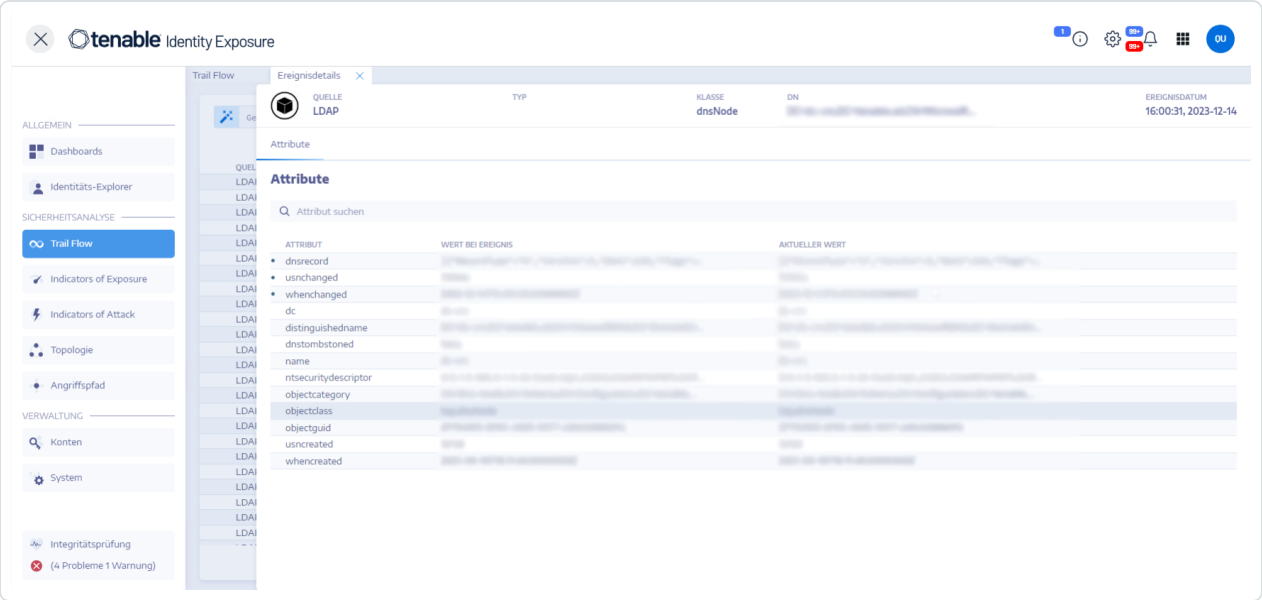


Tabelle „Attribute“

Die Tabelle „Attribute“ enthält die folgenden Spalten:

Spalte	Beschreibung
Attribute	Zeigt die Attribute des AD-Objekts an, das mit dem Ereignis verknüpft ist, das Sie in der Tabelle „Trail Flow“ ausgewählt haben. Attribute beschreiben die Merkmale des Objekts. Für die Beschreibung eines einzelnen AD-Objekts können mehrere Objekte verwendet werden.
Wert bei Ereignis	Gibt den Attributwert zum Zeitpunkt des Eintretens des Ereignisses an.
Aktueller Wert	Zeigt den Wert des Attributs im AD zu dem Zeitpunkt an, zu dem der Benutzer es betrachtet.

Tipp: Um den Wert des Attributs vor dem Eintreten des Ereignisses anzuzeigen, bewegen Sie den Mauszeiger über den blauen Punkt auf der linken Seite (falls vorhanden).

So suchen Sie nach einem Attribut:

- Geben Sie im Fensterbereich **Ereignisdetails** eine Zeichenfolge in das Suchfeld ein.

  Tenable Identity Exposure grenzt die Liste auf Attribute ein, die dem Suchbegriff entsprechen.

Weitere Informationen finden Sie unter Attributänderungen.

Abweichungen

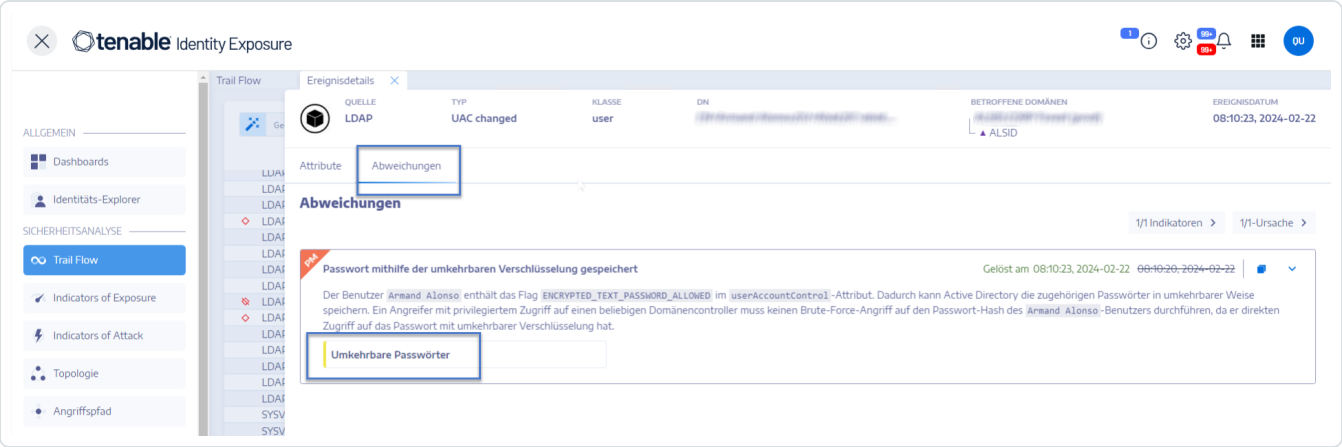
Wenn ein Ereignis im Trail Flow Abweichungen enthält, werden diese auch im Fensterbereich „Ereignisdetails" angezeigt, damit Sie die Ursache des Problems aufschlüsseln können.

So zeigen Sie Abweichungen an:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie, um einen Eintrag aus der Tabelle „Trail Flow" auszuwählen.

   Der Fensterbereich **Ereignisdetails** wird geöffnet.
3. Wählen Sie die Registerkarte **Abweichungen** aus.

   Tenable Identity Exposure zeigt die Liste der Abweichungen an sowie die IoEs, die sie ausgelöst haben.



So schlüsseln Sie die IoE-Details auf:

1. Klicken Sie auf der Registerkarte **Abweichungen** auf die IoE-Kachel unter der Ursache für die Abweichung.

Der Fensterbereich **Indikatordetails** wird mit einer Liste der abweichenden Objekte und den folgenden Informationen geöffnet:

- Name des IoE
- Schweregrad des IoE (Kritisch, Hoch, Mittel, Gering)
- IoE-Status
- Zeitstempel der letzten Erkennung

2. Klicken Sie auf eine der folgenden Registerkarten:
   - **Informationen**: Enthält die internen und externen Ressourcen im IoE.
   - **Details zum Sicherheitsrisiko**: Bietet Erläuterungen zur Schwachstelle, die in Ihrer AD-Infrastruktur erkannt wurde.
   - **Abweichende Objekte**: Enthält technische Details und ein Suchfeld zum Filtern nach Objekten.
   - **Empfehlungen**: Enthält Tipps zur Lösung des Problems.

Attributänderungen

Wenn sich der Wert eines Attributs ändert, wird im Trail Flow ein blauer Punkt vor der Spalte **Attribut** angezeigt.

So zeigen Sie die Attributänderung an:

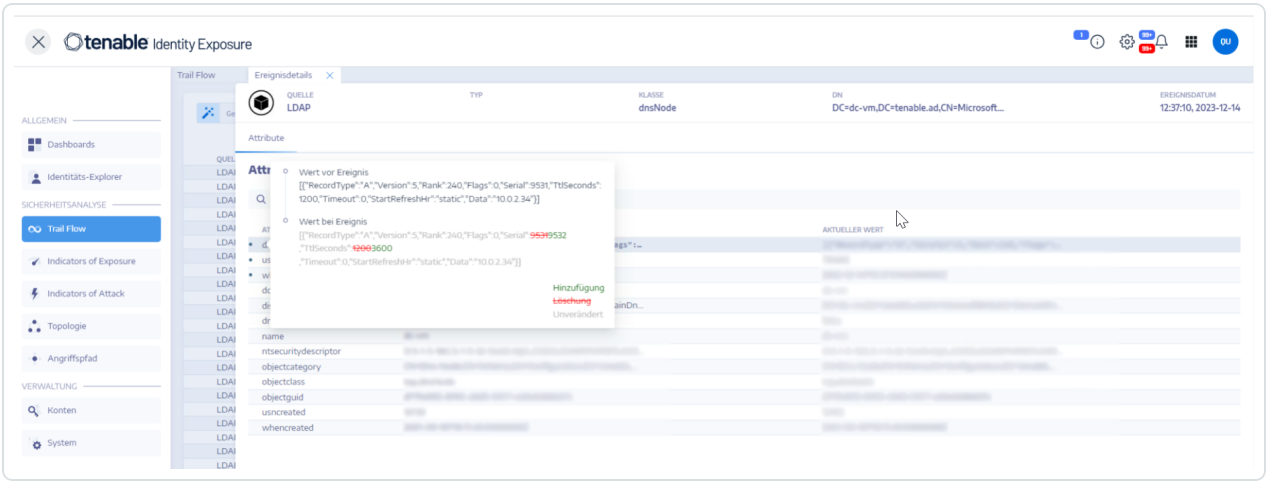
1. Klicken Sie in Tenable Identity Exposure in der Navigationsleiste auf der linken Seite auf **Trail Flow**.

   Die Seite **Trail Flow** öffnet sich mit einer Liste von Ereignissen.

2. Bewegen Sie den Mauszeiger über den blauen Punkt vor der Ereigniszeile, um die Änderungen anzuzeigen.

   Die Farbe der Beschriftung von **Wert bei Ereignis** hängt von den Änderungen ab, die auf das Attribut angewendet wurden:

   - Grün: **Hinzufügung**
   - Rot: **Löschung**
   - Grau: **Unverändert**



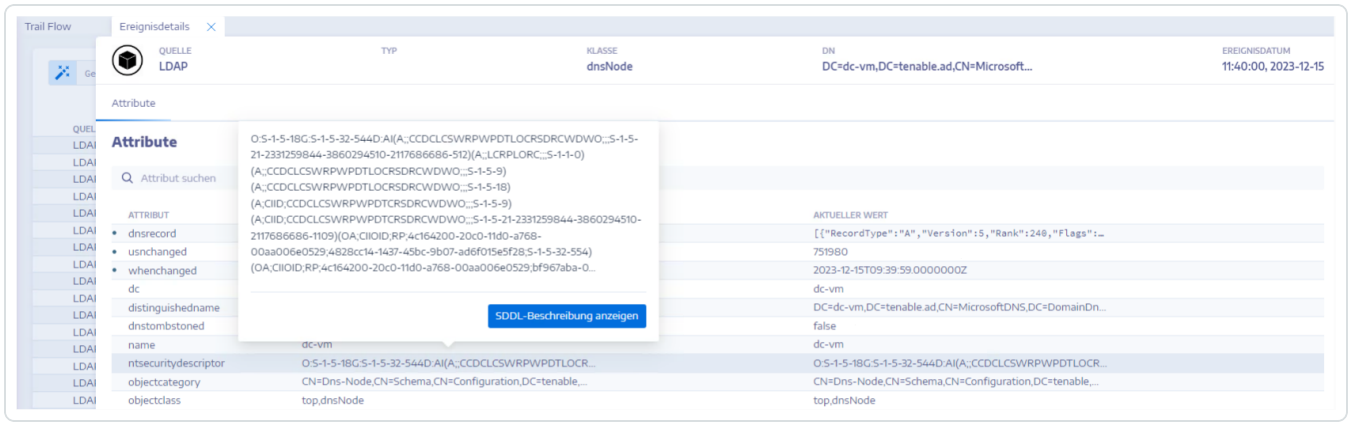
Attribut „ntsecuritydescriptor“

Eine Sicherheitsbeschreibung ist eine Datenstruktur, die Sicherheitsinformationen über ein AD-Objekt enthält, wie z. B. die Besitzerschaft und Berechtigungen. Weitere Einzelheiten finden Sie in der Online-Dokumentation von Microsoft.

So zeigen Sie Details zu einer Objekt-Sicherheitsbeschreibung an:

1. Klicken Sie in Tenable Identity Exposure auf **Trail Flow**, um die Seite „Trail Flow" zu öffnen.
2. Klicken Sie, um einen Eintrag aus der Tabelle „Trail Flow" auszuwählen.

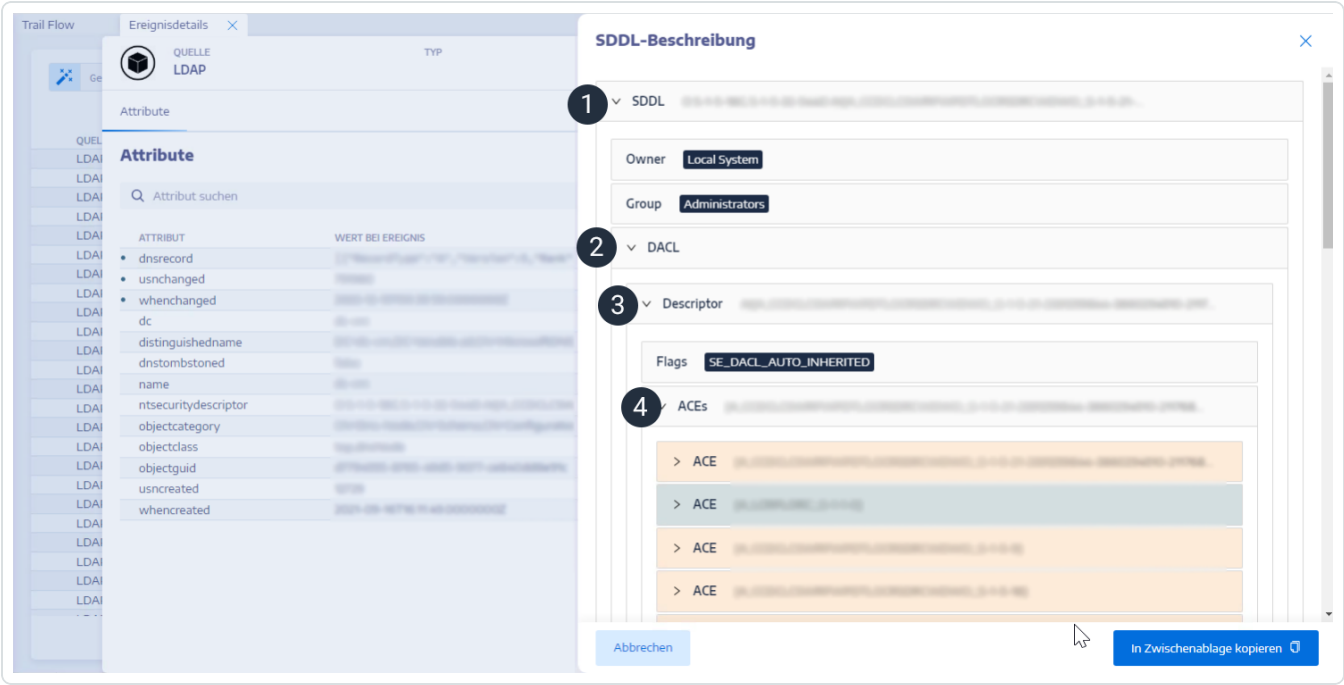
   Der Fensterbereich **Ereignisdetails** wird geöffnet.
3. Bewegen Sie den Mauszeiger über den Attributeintrag `ntsecuritydescriptor` (Spalte „Wert bei Ereignis" oder „Aktueller Wert") **.



4. Klicken Sie auf **SDDL-Beschreibung anzeigen**.

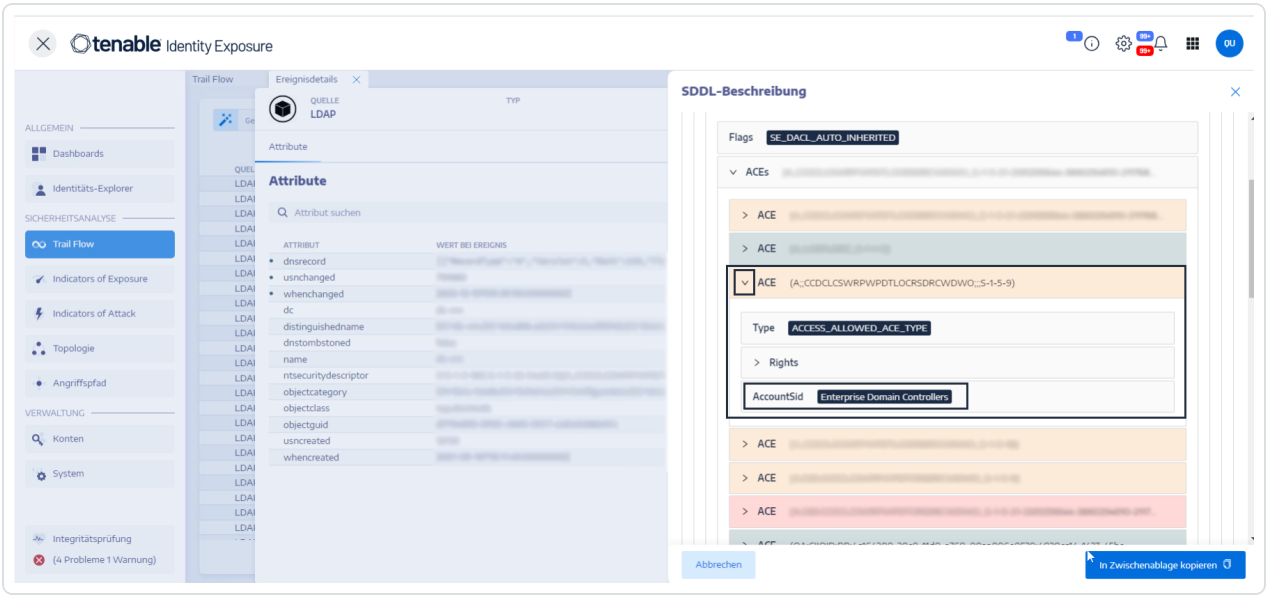
   Der Fensterbereich **SDDL-Beschreibung** wird geöffnet.
5. Klicken Sie auf die Pfeile links von SDDL (1), DACL (2) und Beschreibung (3), um die

Beschreibung zu erweitern:



6. Blättern Sie zu einem farblich hervorgehobenen Zugriffssteuerungseintrag (Access Control Entry, ACE) (4), um die Zugriffsrechte des Objekts anzuzeigen. Die Farbcodes bedeuten:
    - **Rot**: Benutzern wurden gefährliche Rechte zugewiesen, doch sie dürfen keine Zugriffsrechte auf das Objekt haben.
    - **Orange**: Privilegierten Benutzern wurden gefährliche Rechte zugewiesen, doch sie verfügen im Allgemeinen über diese Art von Rechten (z. B. Domänenadministratoren).

- **Grün**: Es sind keine gefährlichen Rechte vorhanden.



7. Klicken Sie zum Kopieren der SDDL-Beschreibung auf **In Zwischenablage kopieren**.

Trail Flow-Anwendungsfälle

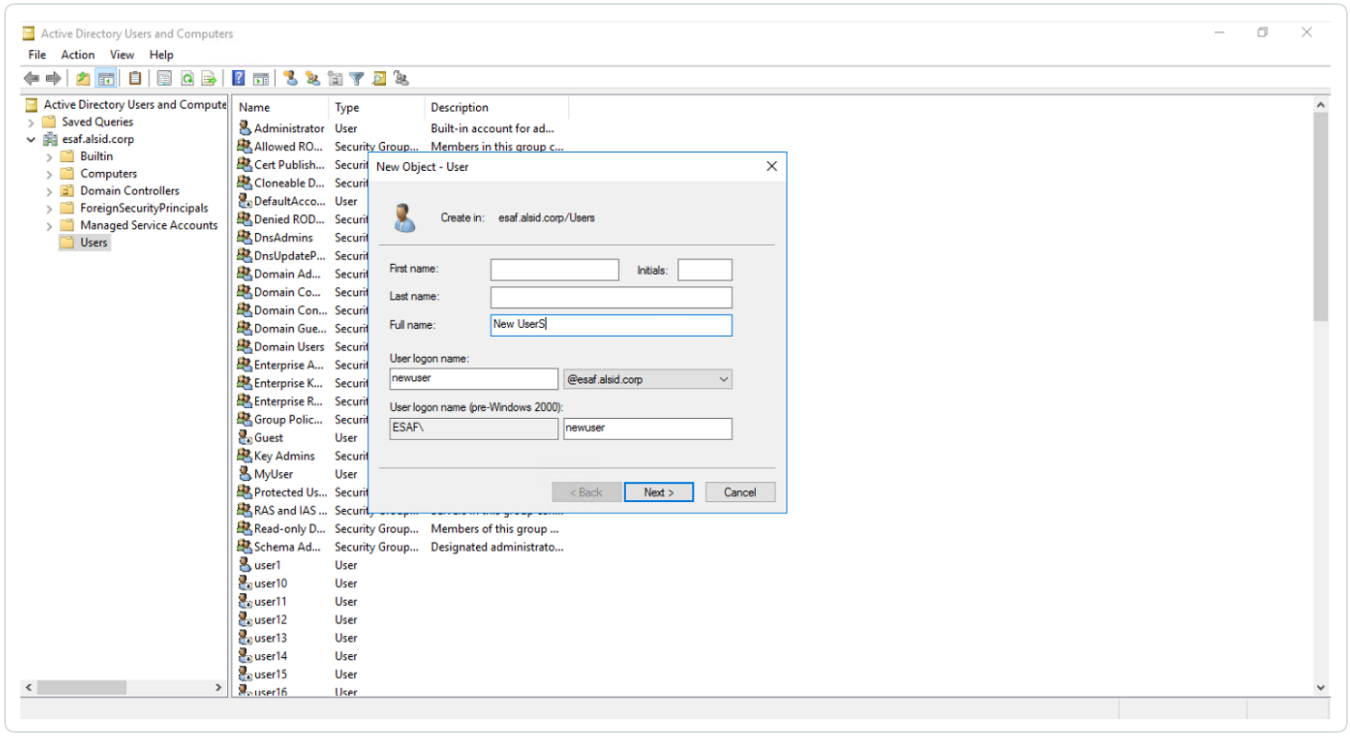
Um das Verhalten von Trail Flow zu verstehen, veranschaulichen zwei Beispiele, wie ein Vorgang, den Sie in der Oberfläche von Active Directory (AD) durchführen, auf der Seite „Trail Flow“ dargestellt wird.

In jedem Beispiel werden Daten auf der Seite des Administrators (in der AD-Oberfläche) mit den Daten auf der Seite des Endbenutzers (in Tenable Identity Exposure) verglichen. Unabhängig davon, ob Sie eine Anwendung, eine API oder einen Dienst verwenden, um einen Vorgang in Ihrem AD auszuführen, ist das Ergebnis im Trail Flow das gleiche.

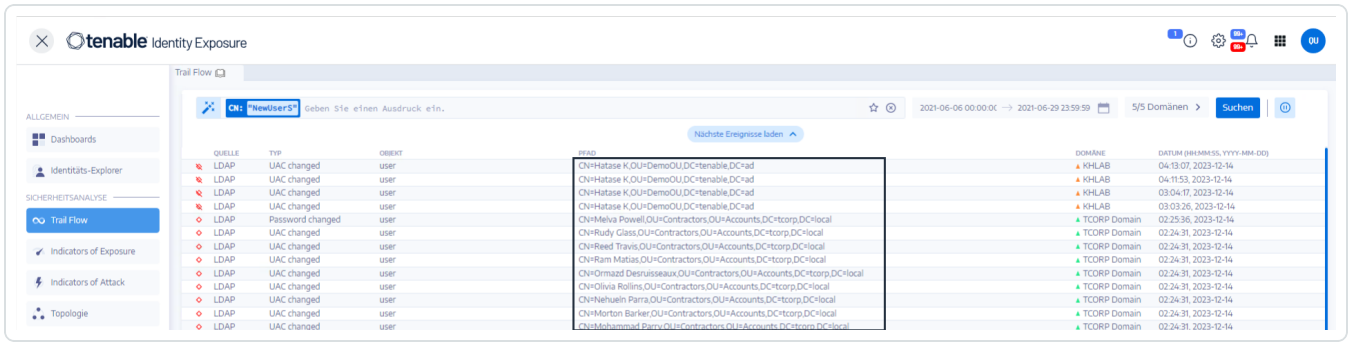
Hinweis: Diese Beispiele sind nicht vollständig und können nicht alle möglichen Situationen abdecken.

Was passiert im Trail Flow, wenn Sie ein neues AD-Benutzerkonto erstellen?

- Auf Seiten des Administrators geben Sie verschiedene Informationen für das neue Benutzerkonto ein.

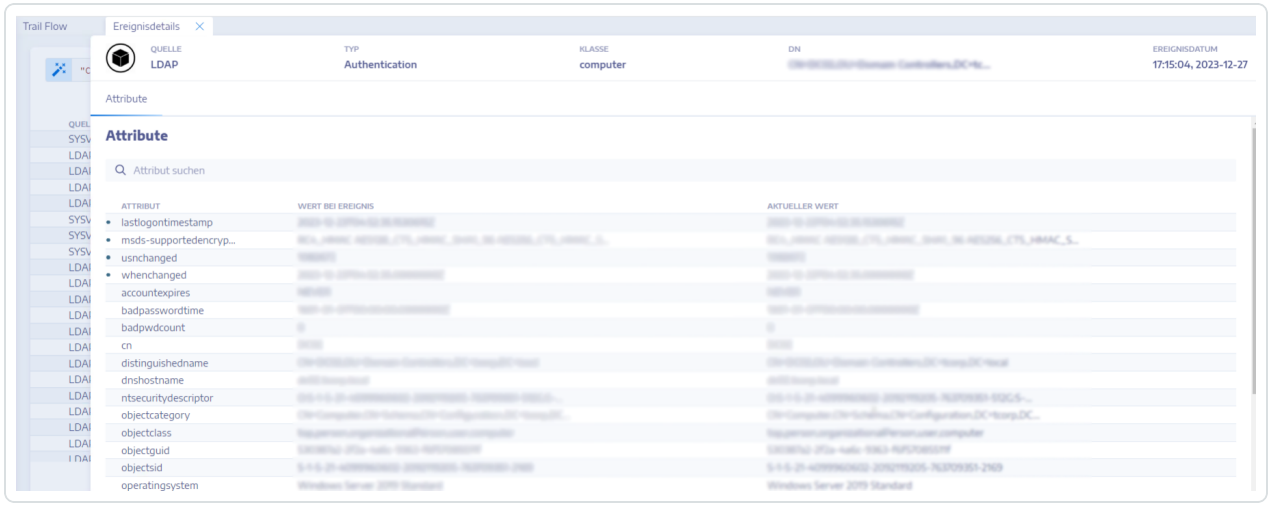


- Auf Seiten des Endbenutzers aktualisiert Tenable Identity Exposure die Seite **Trail Flow**. Sehen Sie sich dazu die Spalte **Typ** mit der Angabe *Neues Objekt* an.



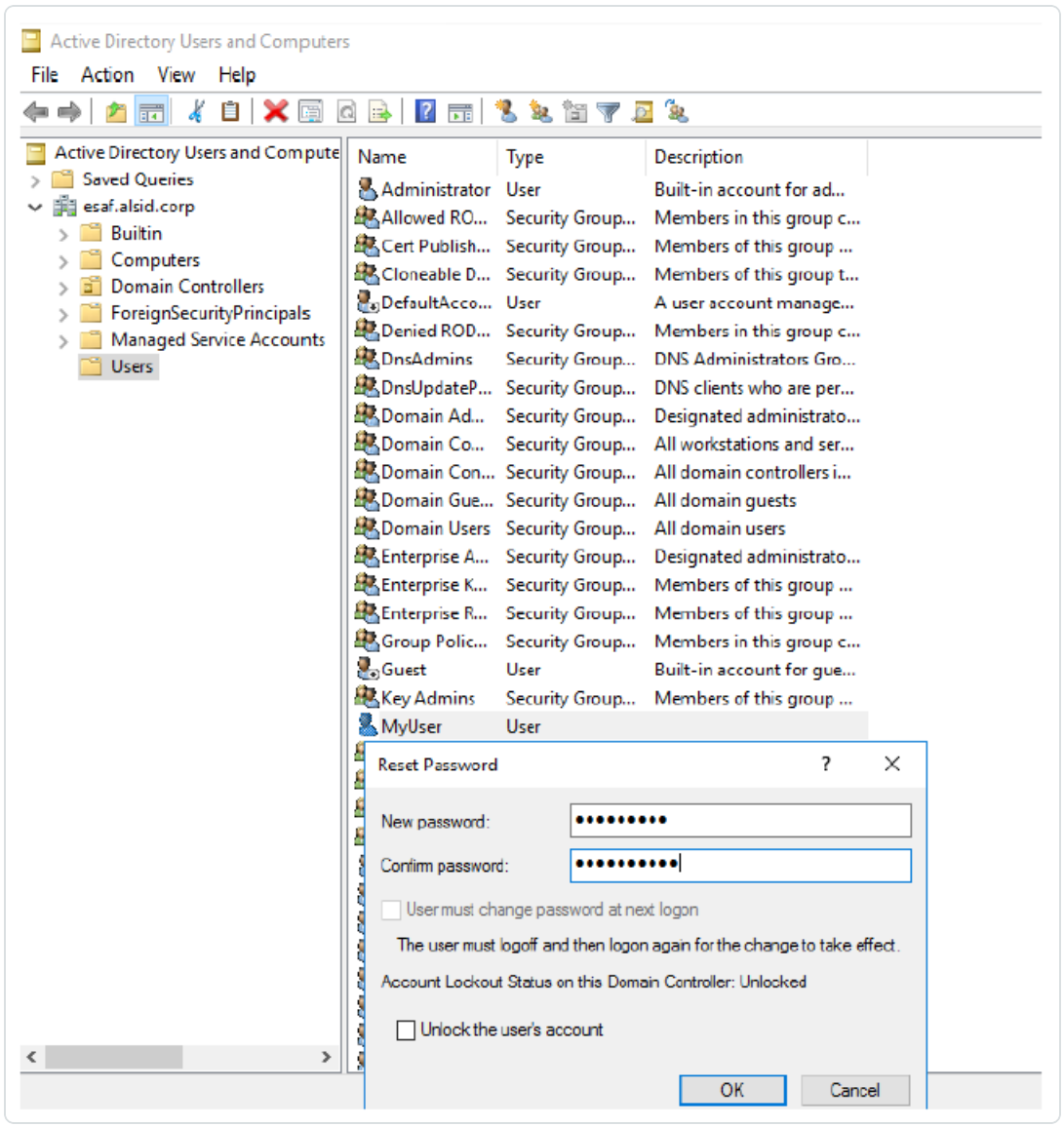
- Die Seite **Ereignisdetails** spiegelt diese Änderung ebenfalls wider. Die blauen Punkte links neben den Attributnamen zeigen an, dass eine Aktualisierung stattgefunden hat.

  Weitere Einzelheiten zu Attributen finden Sie unter Ereignisdetails anzeigen.

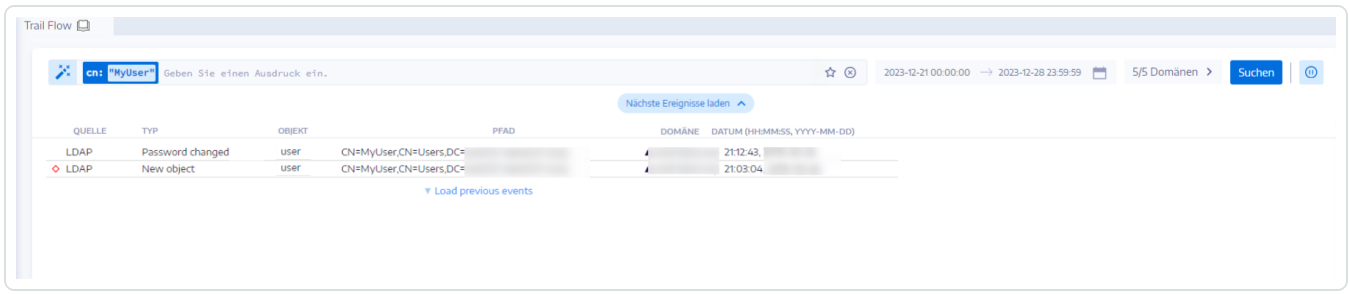


Was passiert im Trail Flow, wenn Sie das Passwort eines AD-Benutzers ändern?

- Auf Seiten des Administrators werden Sie in einem neuen Fenster aufgefordert, verschiedene Informationen einzugeben, um das Passwort eines Benutzers zurückzusetzen.

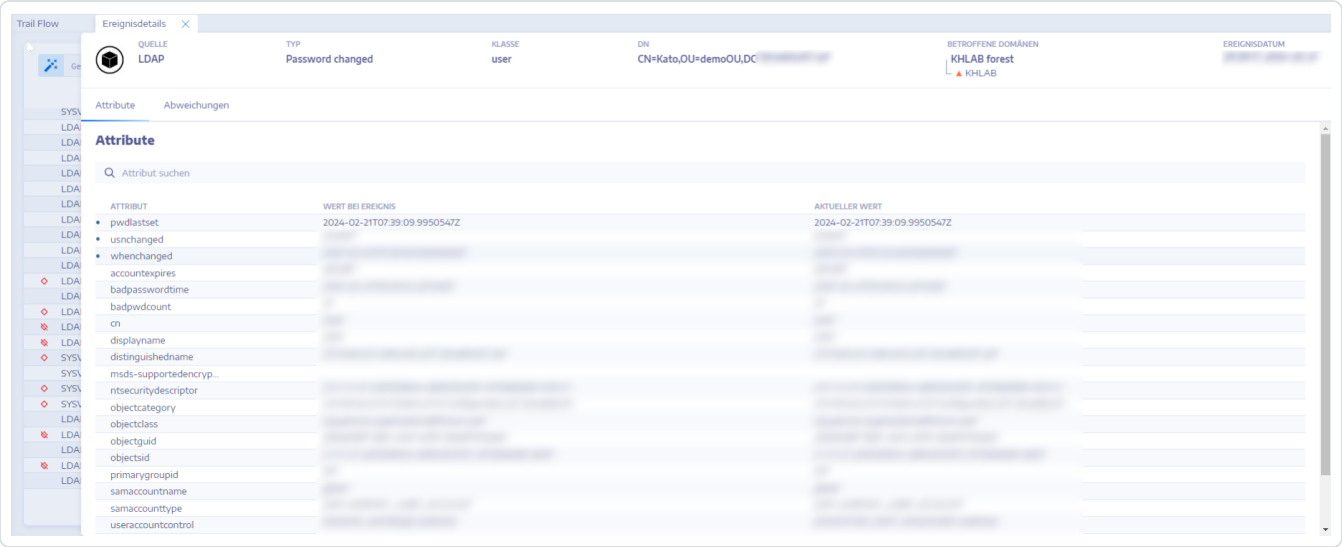


- Auf Seiten des Endbenutzers aktualisiert Tenable Identity Exposure die Seite **Trail Flow**. In der Spalte **Typ** steht „Passwort geändert".



- Auf der Seite **Ereignisdetails** wird diese Änderung durch einen blauen Punkt links neben dem Attribut whenchanged ebenfalls angezeigt.

  Weitere Einzelheiten über die Tabelle „Attribute“ finden Sie unter Ereignisdetails.



Siehe auch

- Trail Flow manuell durchsuchen
- Suche im Trail Flow mit dem Assistenten
- Trail Flow-Abfragen anpassen
- Lesezeichen-Abfragen
- Verlauf abfragen

Indicators of Exposure

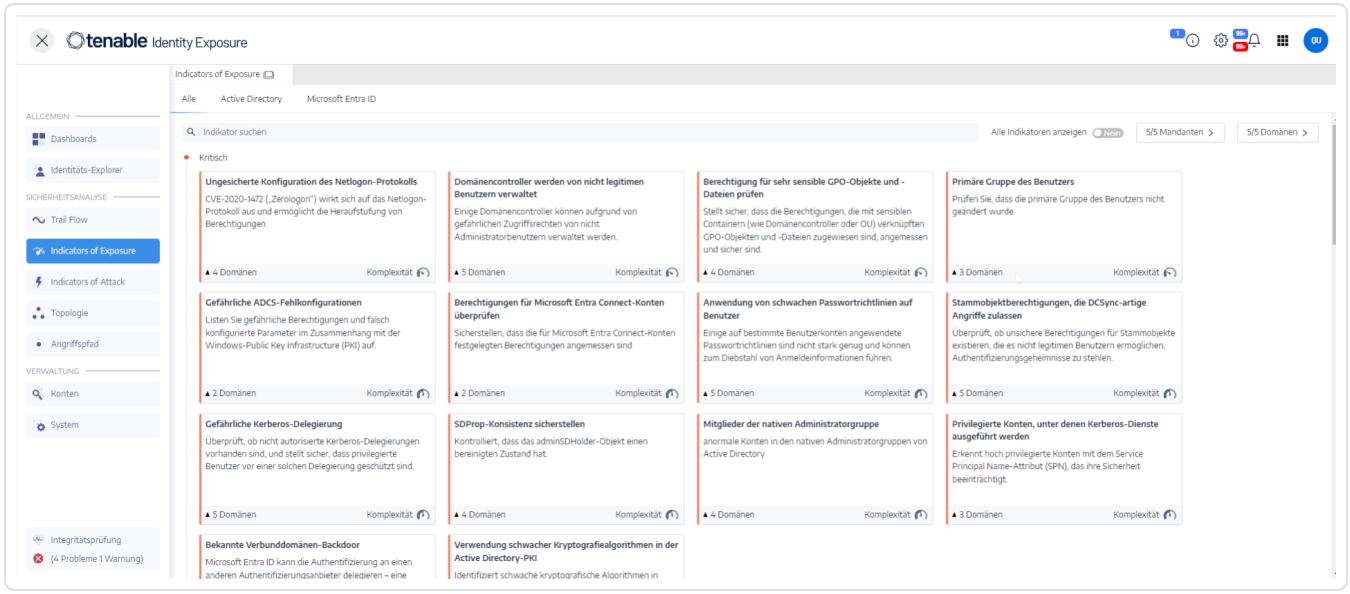
Tenable Identity Exposure misst den Sicherheitsreifegrad Ihrer AD-Infrastrukturen anhand von Indicators of Exposure (IoEs) und weist dem Strom von Ereignissen, der überwacht und analysiert wird, Schweregradestufen zu. Tenable Identity Exposure löst Warnungen aus, wenn es Sicherheitsmängel feststellt.

So zeigen Sie IoEs an:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**.

   Der Fensterbereich **Indicators of Exposure** wird geöffnet. Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die Abweichungen enthalten.

2. (Optional) Wenn Sie alle IoEs anzeigen möchten, stellen Sie den Schalter **Alle Indikatoren anzeigen** auf **Ja**.



So suchen Sie nach einem IoE:

1. Geben Sie oben auf der Seite **Indicators of Exposure** eine Zeichenfolge in das Suchfeld ein. Dies kann ein beliebiger Begriff im Zusammenhang mit einem IoE sein, z. B. Passwort, Benutzer, Anmeldung usw.

2. Drücken Sie die Eingabetaste.

Die IoE-Seite wird mit den Indikatoren aktualisiert, die mit Ihrem Suchbegriff verbunden sind.

So filtern Sie IoEs für eine bestimmte Gesamtstruktur oder Domäne:

1. Klicken Sie auf **n/n Domäne**.

   Der Fensterbereich **Gesamtstrukturen und Domänen** wird geöffnet.
2. Wählen Sie die Gesamtstruktur oder Domäne aus.
3. Klicken Sie auf **Auswahlbasierter Filter**.

Schweregradstufe

Anhand der Schweregradstufen können Sie auf einen Blick den Schweregrad der entdeckten Schwachstellen beurteilen und Prioritäten für Behebungsmaßnahmen setzen.

Im Fensterbereich **Indicators of Exposure** werden die IoEs wie folgt angezeigt:

- Nach Schweregrad unter Verwendung von Farbcodes.
- Vertikal: vom höchsten Schweregrad bis zum niedrigsten (rot für höchste Priorität und blau für niedrigste Priorität).
- Horizontal: vom komplexesten zum am wenigsten komplexen. Tenable Identity Exposure berechnet den Komplexitätsindikator dynamisch, um den Schwierigkeitsgrad der Behebung des abweichenden IoE anzuzeigen.

Schweregrad	Beschreibung
Kritisch – Rot	Zeigt, wie man Angriffe und Kompromittierungen des Active Directory durch bestimmte unprivilegierte Benutzer verhindern kann.
Hoch – Orange	Befasst sich entweder mit Techniken nach der Ausnutzung, die zum Diebstahl von Zugangsdaten oder zur Umgehung der Sicherheit führen, oder mit Ausnutzungstechniken, die eine Verkettung erfordern, um gefährlich zu sein.
Mittel – Gelb	Gibt ein begrenztes Risiko für die Active Directory-Infrastruktur an.
Gering – Blau	Zeigt gute Sicherheitspraktiken. In bestimmten geschäftlichen Zusammenhängen können Abweichungen mit geringen Auswirkungen

	zulässig sein, die die AD-Sicherheit nicht unbedingt beeinträchtigen. Diese Abweichungen wirken sich nur dann auf das AD aus, wenn ein Administrator einen Fehler macht, indem er beispielsweise ein inaktives Konto aktiviert.

Siehe auch

- Indicator of Exposure-Details
- Abweichende Objekte
- Abweichende Objekte suchen
- Abweichende Objekte ignorieren
- Belastende Attribute

Indicator of Exposure-Details

Die Details zu einem bestimmten Indicator of Exposure ermöglichen es Ihnen, technische Informationen zu erkannten Schwachstellen, zugehörigen abweichenden Objekten und Empfehlungen zur Abhilfe zu prüfen.

So werden Indicator of Exposure-Details angezeigt:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**.

   Der Fensterbereich **Indicators of Exposure** wird geöffnet. Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die Abweichungen enthalten.

2. (Optional) Wenn Sie alle IoEs anzeigen möchten, stellen Sie den Schalter **Alle Indikatoren anzeigen** auf **Ja**.

3. Klicken Sie auf eine beliebige **Indicators of Exposure**-Kachel auf der Seite.

   Der Fensterbereich **Indikatordetails** wird geöffnet.

   Oben im Fensterbereich **Indikatordetails** werden die bereits in der Trail Flow-Tabelle enthaltenen Informationen zusammengefasst:

   - Der **Name** des IoE.
   - Die **Schweregradstufe** (Kritisch, Hoch, Mittel oder Gering).
   - Der **Compliance-Status**, der das Ergebnis der letzten von Tenable Identity Exposure ausgeführten Analyse anzeigt.
   - Die **Letzte Erkennung** gibt an, wann die Analyse zum letzten Mal von Tenable Identity Exposure durchgeführt wurde.

4. Klicken Sie auf eine der folgenden Registerkarten, um weitere Details zum IoE zu erhalten:

Registerkarte	Beschreibung
Informationen	Enthält interne und externe Ressourcen zum IoE wie: • Kurzzusammenfassung: Ein Überblick über das Problem, damit Sie die richtigen Entscheidungen treffen können. • Dokumente: Links zu externen Ressourcen über den IoE. • Bekannte Tools des Angreifers: Name der Hacking-Tools. • Eine Baumstruktur der betroffenen Domänen.
Details zum Sicherheitsrisiko	Enthält Erklärungen zu den in Ihrem Active Directory (AD) entdeckten Schwachstellen und den Risiken für Ihr AD, wenn Sie keine Behebungsmaßnahmen ergreifen.
Abweichende Objekte	Abweichende Objekte zeigen Schwachstellen oder potenziell gefährliche Verhaltensweisen in Ihrem AD auf. Sie können Filter auf abweichende Objekte anwenden, um kritische Probleme ausfindig zu machen. Wenn ein IoE-Status nicht konform ist und abweichende Objekte enthält, können Sie Behebungsmaßnahmen ergreifen, um die von Tenable Identity Exposure festgestellten Sicherheitsmängel zu beheben. Weitere Informationen finden Sie unter Abweichende Objekte.
Empfehlungen	Tipps, wie Sie die Compliance mit Ihren Sicherheitsanforderungen wiederherstellen und die Sicherheit Ihrer AD verbessern können: • Eine Kurzzusammenfassung gibt einen Überblick über die von Tenable Identity Exposure vorgeschlagene Lösung. • Der Teilbereich „Details“ bietet Tipps für die Umsetzung des Aktionsplans und hilft den Verantwortlichen, die notwendigen Änderungen an ihren AD-Infrastrukturen

	einzuleiten. • Der Unterabschnitt „Dokumente“ enthält Links zu externen Ressourcen zur vorgeschlagenen Lösung oder Bedrohung.

Siehe auch

- Indicators of Exposure
- Abweichende Objekte
- Abweichende Objekte suchen
- Abweichende Objekte ignorieren
- Belastende Attribute

Abweichende Objekte

Die Indicators of Exposure (IoE) von Tenable Identity Exposure können abweichende Objekte kennzeichnen, die Schwachstellen oder potenziell gefährliche Verhaltensweisen in einem Active Directory (AD) aufzeigen. Die Untersuchung dieser abweichenden Objekte kann Ihnen helfen, kritische Probleme zu erkennen und zu beheben. Sie können eine der folgenden Möglichkeiten nutzen:

- Nach einem abweichenden Objekt suchen.
- Ein abweichendes Objekt für eine bestimmte Zeit ignorieren.
- Gesamtstrukturen und Domänen auswählen, um nach abweichenden Objekten zu suchen.
- Erklärungen zu den belastenden Attributen abrufen, die den IoE betreffen.
- Einen Bericht mit allen abweichenden Objekten herunterladen.

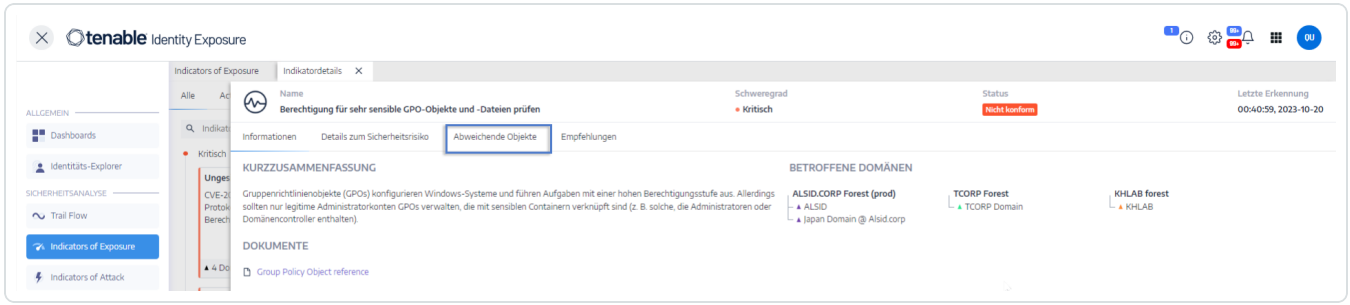
So zeigen Sie abweichende Objekte an:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**.

   Die Seite für **Indicators of Exposure** wird geöffnet. Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die Abweichungen enthalten.

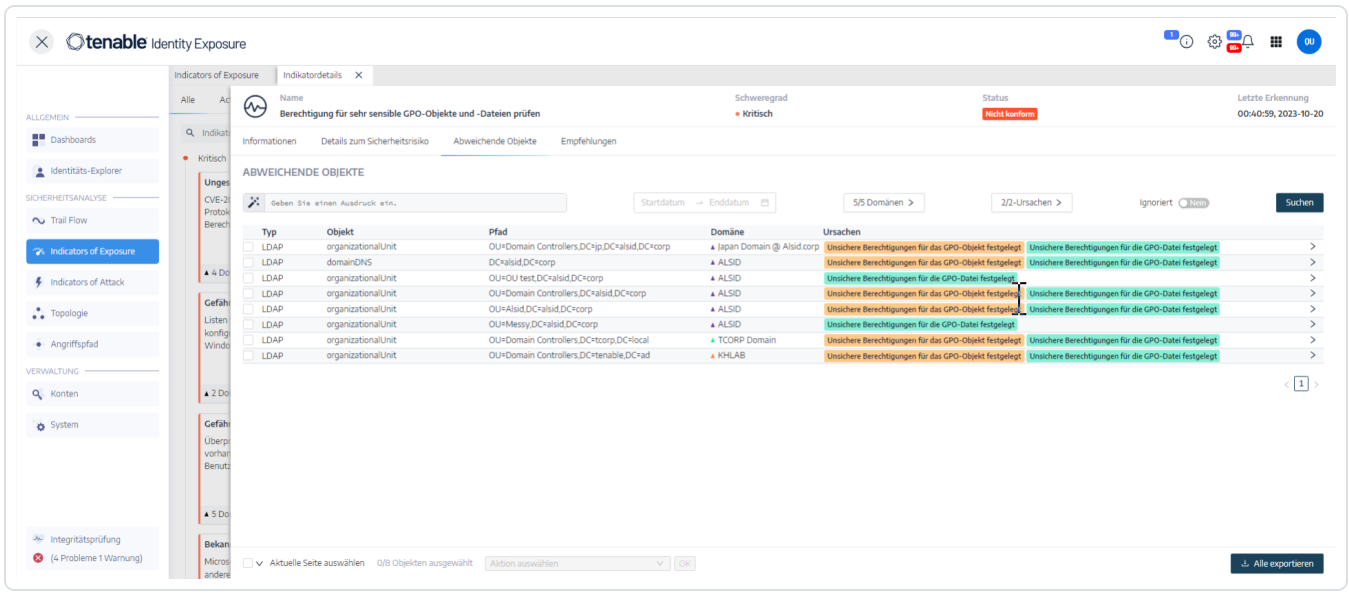
2. Klicken Sie auf eine beliebige **Indicators of Exposure**-Kachel auf der Seite.

   Der Fensterbereich **Indikatordetails** wird geöffnet.



3. Klicken Sie auf die Registerkarte **Abweichende Objekte**.

   Die Liste der abweichenden Objekte, die mit dem IoE verbunden sind, wird angezeigt.



Die Tabelle der abweichenden Objekte enthält die folgenden Informationen:

- **Typ**: Gibt den Ursprung jeder sicherheitsrelevanten Änderung im AD an (LDAP- oder SMB-Protokolle).
- **Objekt**: Hier wird die Klasse oder Dateierweiterung aufgeführt, die einem AD-Objekt zugewiesen ist.
- **Pfad**: Gibt den vollständigen Pfad zu einem AD-Objekt an, um den eindeutigen Standort dieses Objekts im AD zu identifizieren.
- **Domäne**: Gibt die Domäne an, aus der die Änderung in Ihrem AD stammt.
- **Ursachen**: Hier werden die belastenden Attribute aufgeführt, die abweichende Objekte betreffen.

So exportieren Sie den Bericht zu abweichenden Objekten:

1. Klicken Sie unten auf der Seite **Abweichende Objekte** auf **Alle exportieren**.

   Der Fensterbereich **Abweichende Objekte exportieren** wird geöffnet.

2. Klicken Sie im Feld **Exportformat** auf den Dropdown-Pfeil, um ein Format auszuwählen.
3. Klicken Sie auf **Alle exportieren**.

Tenable Identity Exposure lädt den Bericht über abweichende Objekte auf Ihren Computer herunter.

Siehe auch

- Indicators of Exposure
- Indicator of Exposure-Details
- Abweichende Objekte suchen
- Abweichende Objekte ignorieren
- Belastende Attribute

Abweichende Objekte suchen

Sie können manuell oder mit Hilfe des Assistenten nach abweichenden Objekten suchen.

Assistentensuche

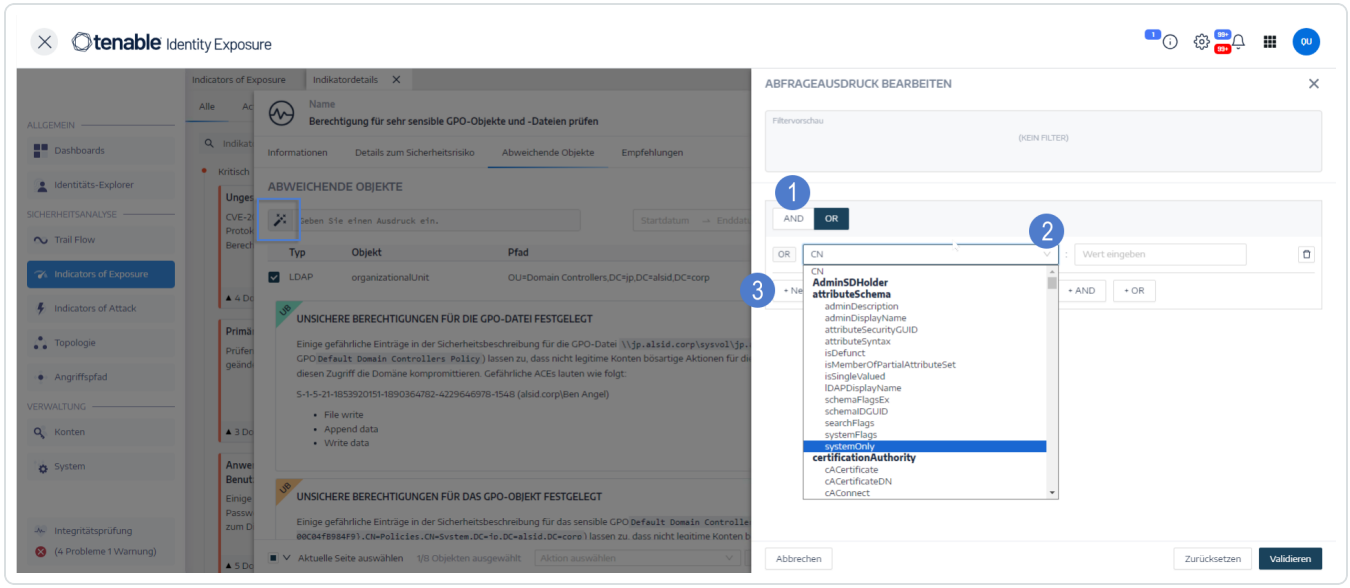
Mit dem Suchassistenten können Sie Abfrageausdrücke erstellen.

- Wenn Sie häufige Ausdrücke im Suchfeld verwenden, können Sie diese für eine spätere Verwendung zu einer Liste von Lesezeichen hinzufügen.
- Wenn Sie einen Ausdruck in das Suchfeld eingeben, speichert Tenable Identity Exposure diesen Ausdruck im Fensterbereich „Verlauf“, damit Sie ihn wiederverwenden können.

So suchen Sie mit dem Assistenten nach einem abweichenden Objekt:

1. Zeigen Sie die Liste Abweichende Objekte an.
2. Klicken Sie auf das Symbol .

   Der Fensterbereich **Abfrageausdruck bearbeiten** wird geöffnet.



3. Um den Abfrageausdruck im Bereich zu definieren, klicken Sie zunächst auf die **AND**- oder **OR**-Operatorschaltfläche (1), um die erste Bedingung anzuwenden.
4. Wählen Sie ein Attribut aus dem Dropdown-Menü und geben Sie den Wert ein (2).
5. Führen Sie einen der folgenden Schritte aus:

- Um ein Attribut hinzuzufügen, klicken Sie auf **+ Neue Regel hinzufügen** (3).
- Um eine weitere Bedingung hinzuzufügen, klicken Sie auf **Neue Bedingung hinzufügen+AND**- oder **+OR**-Operator. Wählen Sie ein Attribut aus dem Dropdown-Menü und geben Sie den Wert ein.
- Um die Suche auf abweichende Objekte einzuschränken, klicken Sie zum Aktivieren auf den Schalter **Nur Abweichungen**. Wählen Sie den Operator **+AND** oder **+OR** aus, um die Bedingung zur Abfrage hinzuzufügen.
- Um eine Bedingung oder Regel zu löschen, klicken Sie auf das Symbol 🗑.

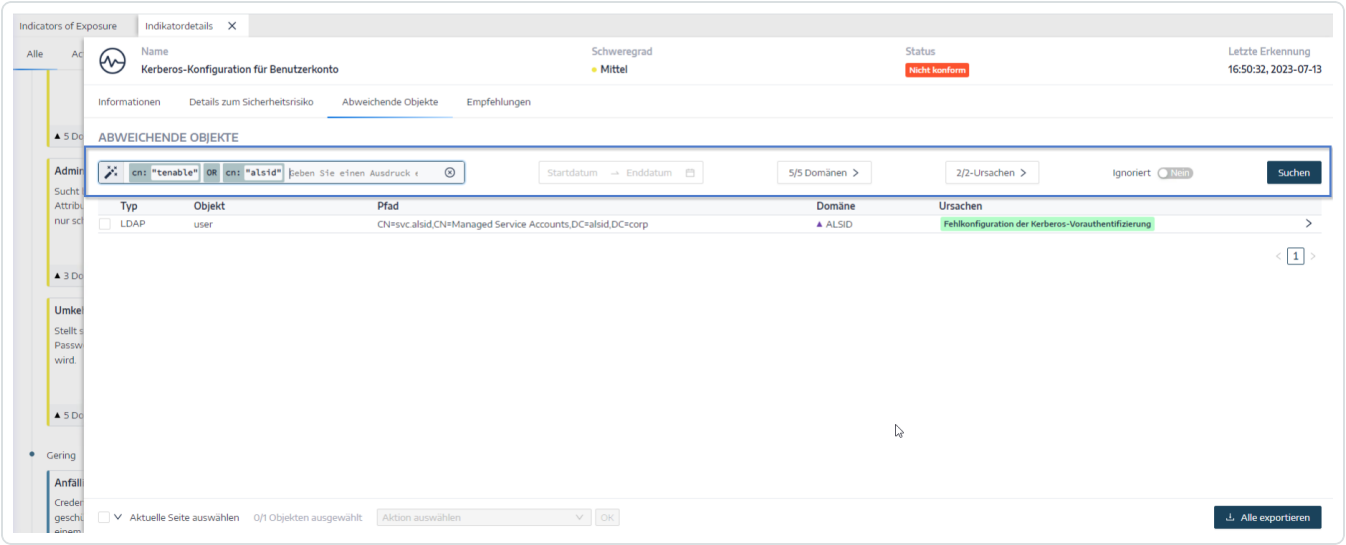
6. Klicken Sie auf **Validieren**, um die Suche auszuführen, oder auf **Zurücksetzen**, um die Abfrageausdrücke zu ändern.

Manuelle Suche

Um abweichende Objekte zu filtern, die mit bestimmten Zeichenfolgen oder Mustern übereinstimmen, können Sie einen Ausdruck in das Suchfeld eingeben und so die Ergebnisse mit den booleschen Operatoren *****, **AND** und **OR** präzisieren. Sie können **OR**-Anweisungen in Klammern einschließen, um die Suchpriorität zu ändern. Bei der Suche wird nach einem bestimmten Wert in einem Active Directory-Attribut gesucht. So können Sie den Trail Flow manuell durchsuchen:

So suchen Sie manuell nach einem abweichenden Objekt:

1. Zeigen Sie die Liste der Abweichende Objekte an.



2. Geben Sie im Suchfeld einen Abfrageausdruck ein.
3. Sie können die Suchergebnisse wie folgt filtern:
    - Klicken Sie auf das Feld **Kalender**, um ein Start- und ein Enddatum auszuwählen.
    - Klicken Sie auf **n/n Domänen**, um Gesamtstrukturen und Domänen auszuwählen.
4. Klicken Sie auf **Suchen**.

    Tenable Identity Exposure aktualisiert die Liste mit den Ergebnissen, die Ihren Suchkriterien entsprechen.

Grammatik und Syntax

Ein manueller Abfrageausdruck verwendet die folgende Grammatik und Syntax:

- Grammatik: `EXPRESSION [OPERATOR EXPRESSION]*`
- Syntax: `__KEY__ __SELECTOR__ __VALUE__`

  Bedeutung:
    - `__KEY__` bezieht sich auf das zu durchsuchende AD-Objektattribut (wie `CN`, `userAccountControl`, `members` usw.)
    - `__SELECTOR__` bezieht sich auf den Operator: `:`, `>`, `<`, `>=`, `<=`.
    - `__VALUE__` bezieht sich auf den zu suchenden Wert.

      Sie können mehr Schlüsselwörter verwenden, um nach bestimmten Inhalten zu suchen:
    - `isDeviant` sucht nach Ereignissen, die eine Abweichung verursacht haben

Sie können mehrere Trail Flow-Abfrageausdrücke mit den Operatoren **AND** und **OR** kombinieren.

Beispiele:

- Suche nach allen Objekten, die die Zeichenfolge `alice` im Attribut für den allgemeinen Namen enthalten: `cn:"alice"`
- Suche nach allen Objekten, die die Zeichenfolge `alice` im Attribut für den allgemeinen Namen enthalten und zu einer konkreten Abweichung geführt haben: `isDeviant:"true" and cn:"alice"`

- Suche nach einem GPO mit dem Namen „Default Domain Policy“: `objectClass: "groupPolicyContainer" and displayname: "Default Domain Policy"`
- Suche nach allen deaktivierten Konten mit einer SID, die S-1-5-21 enthält: `userAccountControl: "DISABLE" und objectSid: "S-1-5-21"`
- Suche nach allen `script.ini`-Dateien in Sysvol: `globalpath: "sysvol" and types: "SCRIPTSini"`

> **Hinweis**: Hier bezieht sich `types` auf das Objektattribut und nicht auf die Spaltenüberschrift.

Siehe auch

- Indicators of Exposure
- Indicator of Exposure-Details
- Abweichende Objekte
- Abweichende Objekte ignorieren
- Belastende Attribute

Abweichende Objekte ignorieren

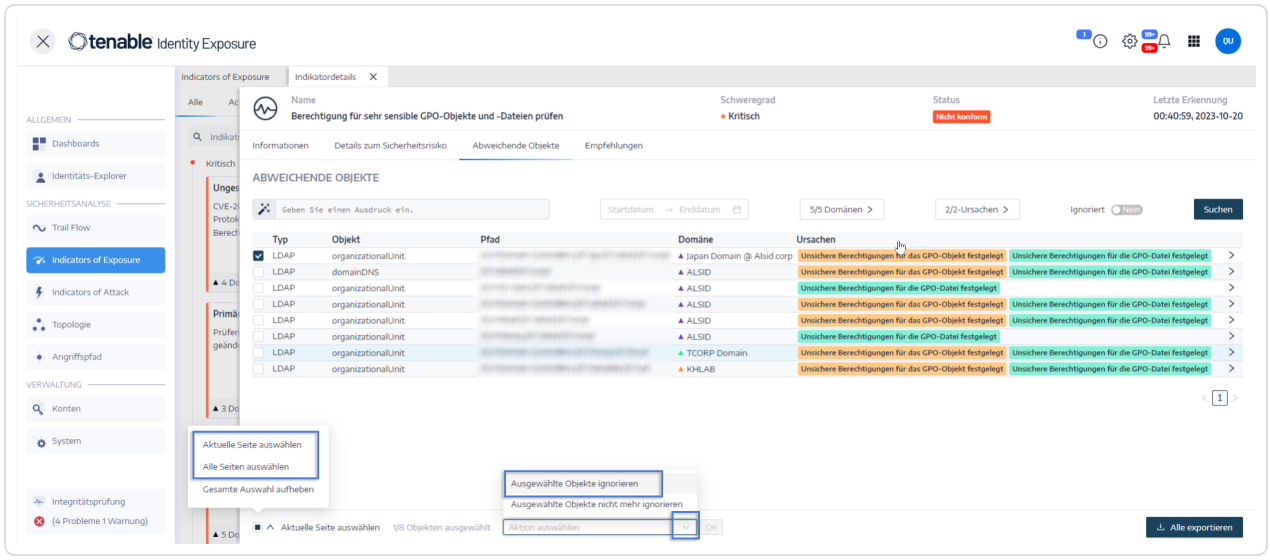
Damit der Bildschirm für Untersuchungs- oder Berichtszwecke nicht unübersichtlich wird, können Sie einige abweichende Objekte herausfiltern und Tenable Identity Exposure zwingen, diese für eine bestimmte Zeit zu ignorieren. Sie können wählen, ob Sie ein oder mehrere abweichende Objekte ignorieren wollen. Es ist möglich, einen benutzerdefinierten Filter sofort anzuwenden oder einen Zeitrahmen für die Aktivierung des Filters festzulegen.

Hinweis: Ein Objekt zu ignorieren bedeutet nicht, dass es in Tenable Identity Exposure aufgelöst ist.

So ignorieren Sie abweichende Objekte:

1. Zeigen Sie in Tenable Identity Exposure die Liste Abweichende Objekte an.
2. Aktivieren Sie die Kontrollkästchen vor den zu ignorierenden abweichenden Objekten.
3. Optional können Sie auch nach abweichenden Objekten filtern, die ignoriert werden sollen:
    - Klicken Sie auf das Feld **Kalender**, um ein Start- und ein Enddatum auszuwählen.
    - Klicken Sie auf **n/n Domänen**, um Gesamtstrukturen und Domänen auszuwählen.

Tipp: Um die Auswahl zu beschleunigen, können Sie unten auf der Seite das Kästchen **Alle Seiten auswählen** oder **Aktuelle Seite auswählen** aktivieren.



4. Wählen Sie in der Dropdown-Liste am unteren Bildschirmrand die Option **Ausgewählte Objekte ignorieren** aus.
5. Klicken Sie auf **OK**.

   Der Fensterbereich **Ausgewählte Objekte ignorieren** wird angezeigt.
6. Klicken Sie auf das Feld **Ignorieren bis**, um den Kalender anzuzeigen und ein Datum auszuwählen, bis zu dem Tenable Identity Exposure das abweichende Objekt ignorieren muss.
7. Klicken Sie auf **OK**.

   Tenable Identity Exposure zeigt eine Bestätigungsmeldung an und aktualisiert die Liste der verbleibenden abweichenden Objekte.

So zeigen Sie ignorierte abweichende Objekte an:

1. Klicken Sie auf die Schaltfläche **Ignoriert**, um auf **Ja** umzuschalten.
2. Klicken Sie unten auf der Seite auf **Alle Seiten auswählen**.
3. Wählen Sie in der Dropdown-Liste die Option **Ausgewählte Objekte nicht mehr ignorieren** aus.
4. Klicken Sie auf **OK**.

   Daraufhin wird ein Konfigurationsfenster angezeigt.
5. Klicken Sie auf **OK**, um Ihre Änderungen zu bestätigen.

   Tenable Identity Exposure zeigt die ignorierten abweichenden Objekte an.

Siehe auch

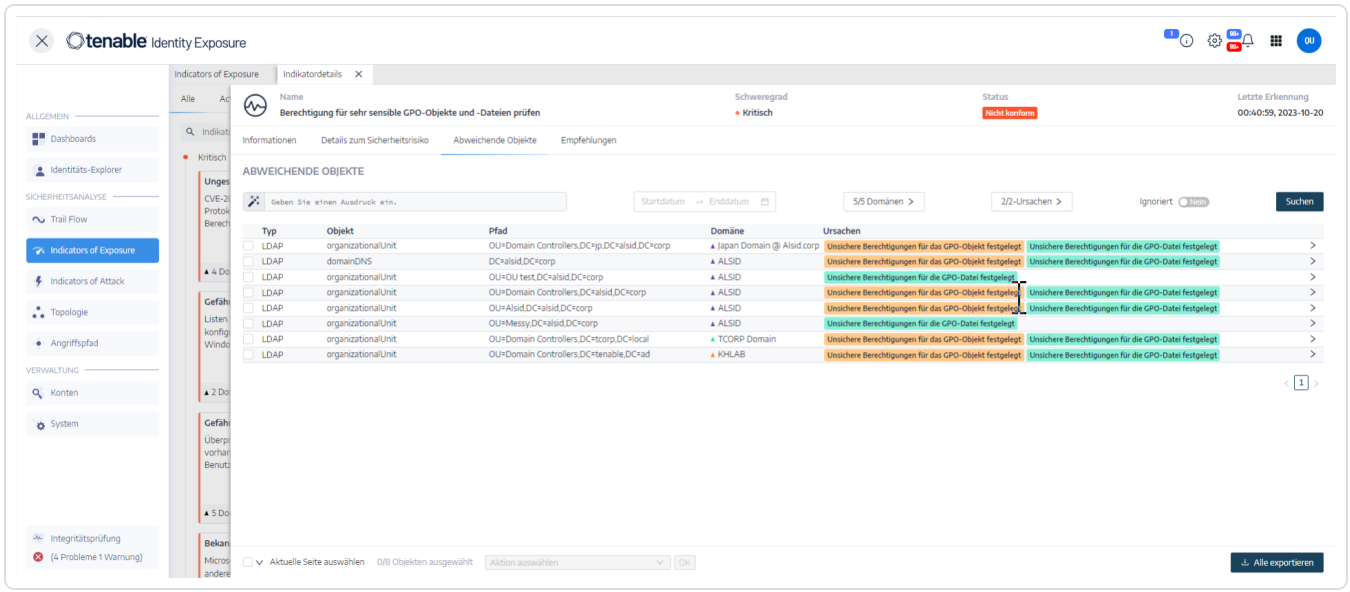
- Indicators of Exposure
- Indicator of Exposure-Details
- Abweichende Objekte
- Abweichende Objekte suchen
- Belastende Attribute

Belastende Attribute

Tenable Identity Exposure zeigt in einem Indicator of Exposure (IoE) die belastenden Attribute an, die abweichende Objekte auslösen, und nennt die Ursachen dafür, damit Sie die Abweichung verstehen und beheben können.

So zeigen Sie belastende Attribute an:

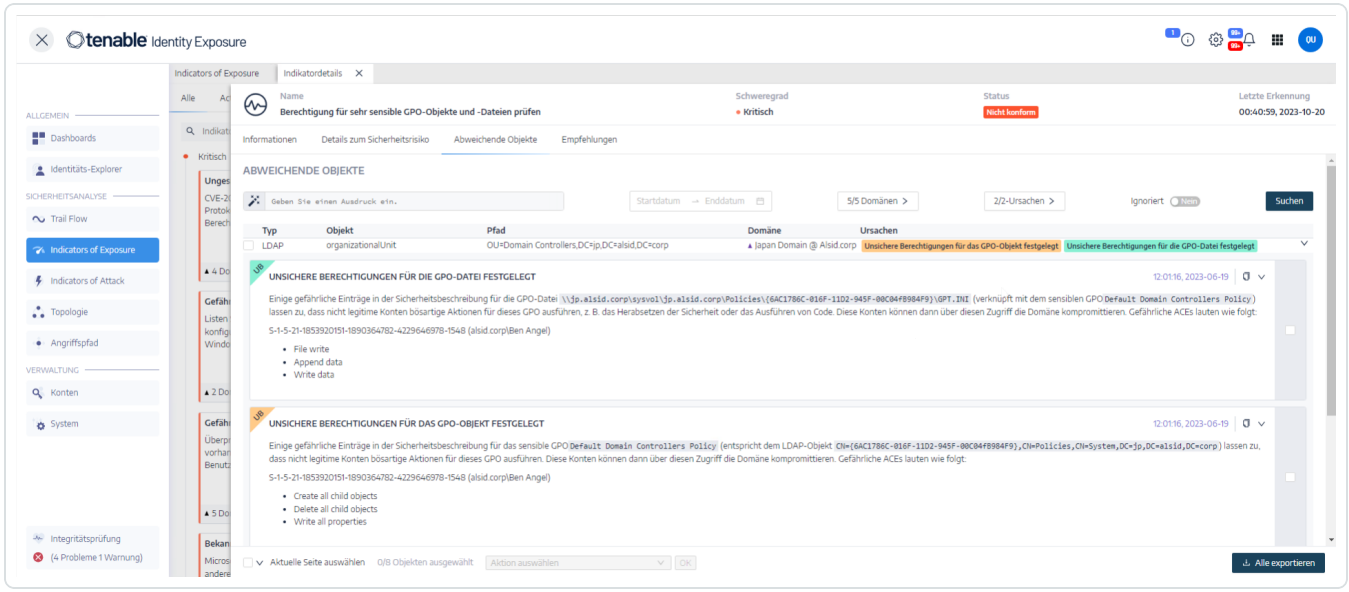
1. Zeigen Sie die Liste Abweichende Objekte an.



2. Klicken Sie auf einen Eintrag in der Liste der abweichenden Objekte.

   Tenable Identity Exposure zeigt eine Liste mit belastenden Attributen für das abweichende

Objekt an:



Die Liste enthält die folgenden Informationen:

- **Farbcodierte Markierungen** zur Unterscheidung der verschiedenen Ursachen, wenn es mehrere gibt.
- Werte:
  - `?` – Ein fehlender (leerer) Attributwert, der ein abnormales Verhalten anzeigt.
  - `Für diese Abweichung ist keine Beschreibung verfügbar`: Die Erkennung stammt aus der Version 2.6 und Tenable Identity Exposure verwaltet dieses Attribut nicht mehr.

So kopieren Sie das belastende Attribut:

- Wählen Sie das Attribut aus und klicken Sie auf das Symbol .

Siehe auch

- Indicators of Exposure
- Indicator of Exposure-Details
- Abweichende Objekte

- Abweichende Objekte suchen
- Abweichende Objekte ignorieren

RSoP-basierte Indicators of Exposure

Tenable Identity Exposure verwendet eine Reihe von Indicators of Exposure (IoEs), die auf einem resultierenden Richtliniensatz (Resultant Set of Policy, RSoP) basieren, um die Sicherheit und Compliance verschiedener Aspekte zu bewerten und sicherzustellen. Dieser Abschnitt enthält Informationen über das aktuelle Verhalten bestimmter RSoP-basierter IoEs und darüber, wie Tenable Identity Exposure Leistungsprobleme im Zusammenhang mit den Berechnungen dieser IoEs angeht.

Die folgenden RSoP-basierten IoEs spielen im Sicherheits-Framework von Tenable Identity Exposure eine Rolle:

- Login-Beschränkungen für privilegierte Benutzer
- Gefährliche sensible Berechtigungen
- Anwendung von schwachen Passwortrichtlinien auf Benutzer
- Unzureichende Härtung gegen Ransomware
- Nicht abgesicherte Konfiguration des Netlogon-Protokolls

Diese IoEs stützen sich auf einen Cache mit RSoP-Berechnungsergebnissen, der bei Bedarf initialisiert wird. Für die Berechnungen werden auf Anfrage hinzugefügte Werte verwendet, anstatt sich auf bereits vorhandene Werte zu verlassen. Bisher führten Änderungen an `AdObjects` dazu, dass der Cache ungültig gemacht wurde, sodass häufige Neuberechnungen während der RSoP-Ausführungen des IoE erforderlich wurden.

Die mit RSoP-Berechnungen verbundenen Leistungsbeeinträchtigungen werden in Tenable Identity Exposure wie folgt behoben:

1. **Live-IoE-Analyse mit potenziell veralteten Daten** – Die Berechnung (Eingabe-/Ausgabe-Ereignis) von RSoP-basierten IoEs erfolgt in Echtzeit, sobald die Ereignisse eintreten, auch wenn für die Verarbeitung möglicherweise nicht die neuesten Daten verwendet werden. Gepufferte Ereignisse, die den RSoP-Cache potenziell ungültig machen können, bleiben gespeichert, bis sie eine bestimmte Bedingung erfüllen und die erwartete Berechnung veranlassen.
2. **Geplante RSoP-Invalidierung** – Wenn die Bedingung für die Neuberechnung erfüllt ist, macht das System den RSoP-Cache ungültig, wobei gepufferte Ereignisse während der Invalidierung

berücksichtigt werden.

3. **Erneute Ausführung von IoEs mit aktuellem Cache** – Nach der Cache-Invalidierung werden IoEs mit der neuesten Version des `AdObject` aus dem Cache erneut ausgeführt, wobei gepufferte Ereignisse berücksichtigt werden. Tenable Identity Exposure berechnet jeden IoE für jedes gepufferte Ereignis einzeln.

Aus diesen Gründen führt die optimierte Berechnungsdauer für RSoP-basierte IoEs dazu, dass Abweichungen im Zusammenhang mit dem RSoP langsamer berechnet werden.

Indicators of Exposure in Zusammenhang mit Microsoft Entra ID

Spezifische Indicators of Exposure für Microsoft Entra ID

Tenable Identity Exposure verfügt über spezielle Indicators of Exposure (IoEs), die auf potenzielle Schwachstellen für Assets in Microsoft Entra ID aufmerksam machen.

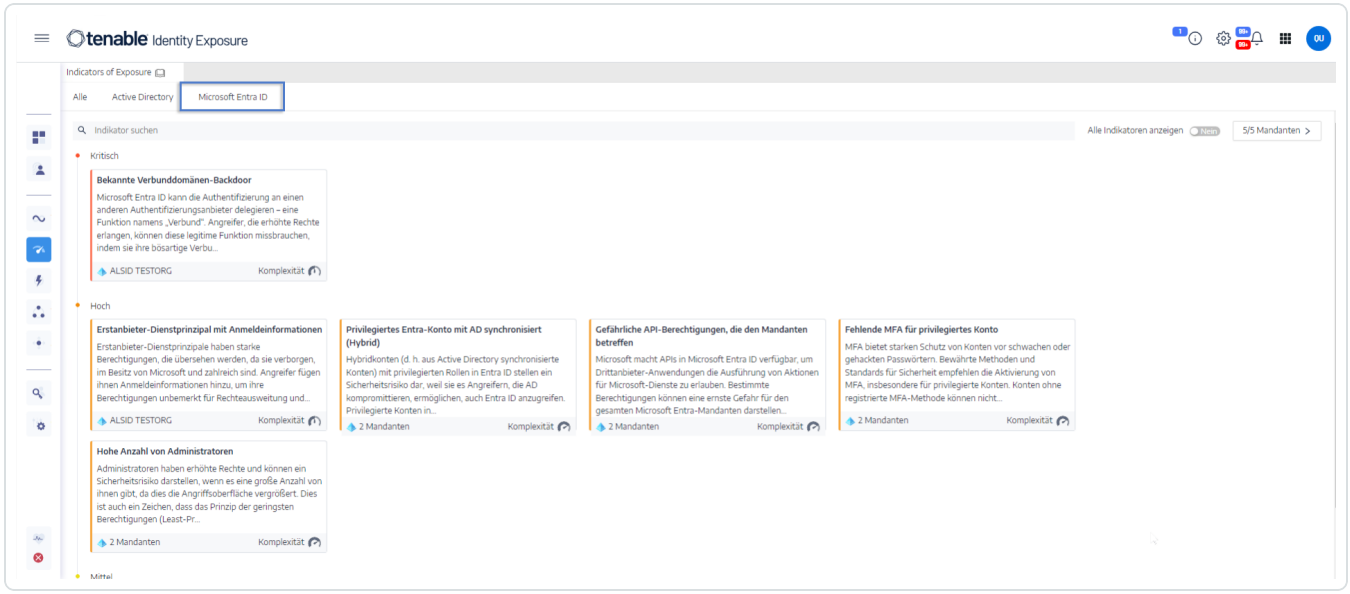
So zeigen Sie Microsoft Entra ID-IoEs an:

1. Klicken Sie in Tenable Identity Exposure auf das IoE-Symbol in der linken Navigationsleiste.

   Der IoE-Fensterbereich wird geöffnet.

2. Klicken Sie auf die Registerkarte **Microsoft Entra ID**.

   Tenable Identity Exposure zeigt IoEs im Zusammenhang mit Microsoft Entra ID an, die Ergebnisse ausgelöst haben.



3. Klicken Sie auf eine Kachel mit dem IoE, das Sie untersuchen möchten.

4. Der Fensterbereich mit den Identitätsdetails für den Indikator wird mit den folgenden Informationen geöffnet:

   - **Informationen zu Sicherheitslücken**: Wie es zu einem potenziellen Angriff kommen kann.

- **Ergebnisse**: Details zum Typ des Identitätsanbieters und eine Beschreibung des Risikos.
- **Empfehlungen**: Schritte zur Behebung der Bedrohung.

Behebungsmaßnahmen für abweichende Objekte aus Indicators of Exposure durchführen

Tenable Identity Exposure löst Warnungen aus, wenn ein Indicator of Exposure (IoE) abweichende Objekte findet, die Behebungsmaßnahmen erfordern.

Im Folgenden finden Sie Beispiele für die Durchführung eines Behebungsverfahrens für drei spezifische IoEs.

- AdminCount-Attribut für Standardbenutzer festgelegt
- Gefährliche Kerberos-Delegierung
- SDProp-Konsistenz sicherstellen

Vollständige Informationen zu IoEs finden Sie in der Dokumentation, die in der Benutzeroberfläche von Tenable Identity Exposure bereitgestellt wird.

AdminCount-Attribut für Standardbenutzer festgelegt

Wenn für ein Benutzerkonto das Attribut `adminCount` festgelegt ist, weist dies auf die frühere Mitgliedschaft des Kontos in einer Administratorgruppe hin. Das Attribut wird nicht zurückgesetzt, wenn das Konto die Gruppe verlässt. Dies führt dazu, dass auch alte Administratorkonten über dieses Attribut verfügen, wodurch die Vererbung von Active Directory-Berechtigungen blockiert wird. Dieses ursprünglich zum Schutz von Administratoren vorgesehene Attribut kann schwer zu behebende Berechtigungsprobleme verursachen.

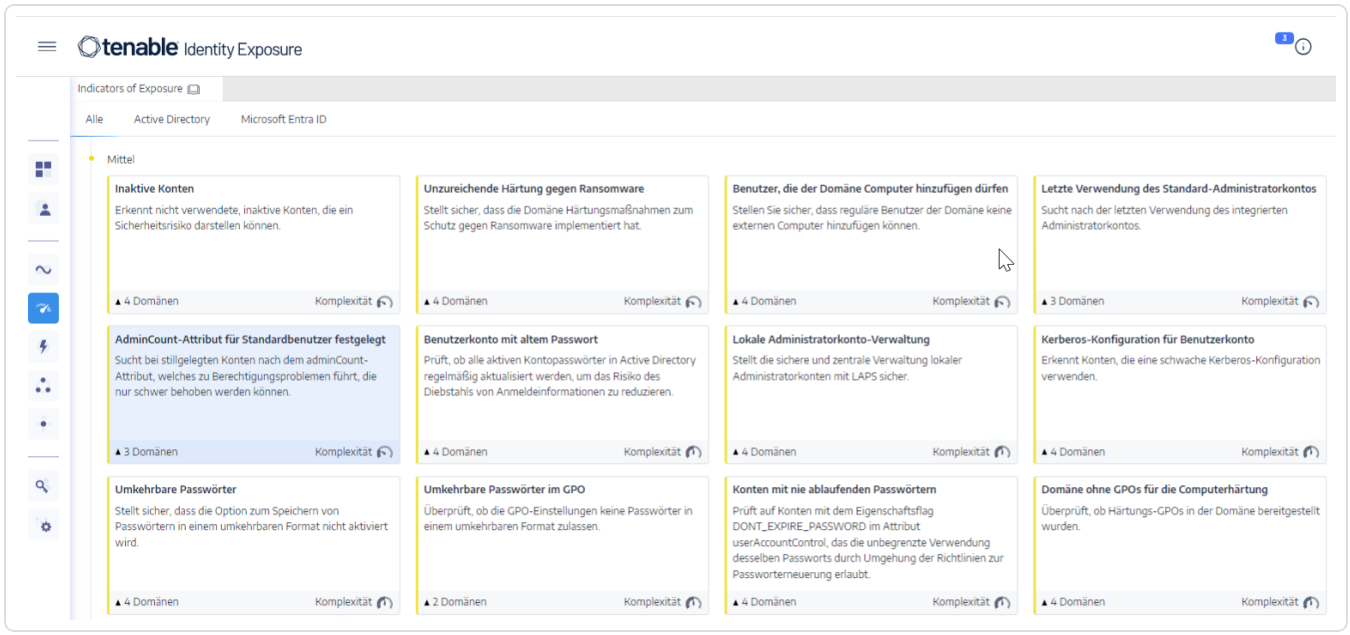
Dieser IoE mit Schweregrad „Mittel" berücksichtigt nur aktive Benutzerkonten und -gruppen mit diesem Attribut und schließt privilegierte Gruppen mit legitimen Mitgliedern aus, bei denen das Attribut `adminCount` auf `1` festgelegt ist.

So führen Sie Behebungsmaßnahmen für ein abweichendes Objekt aus dem IoE **AdminCount-Attribut für Standardbenutzer festgelegt** durch:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**, um dieses Fenster zu öffnen.

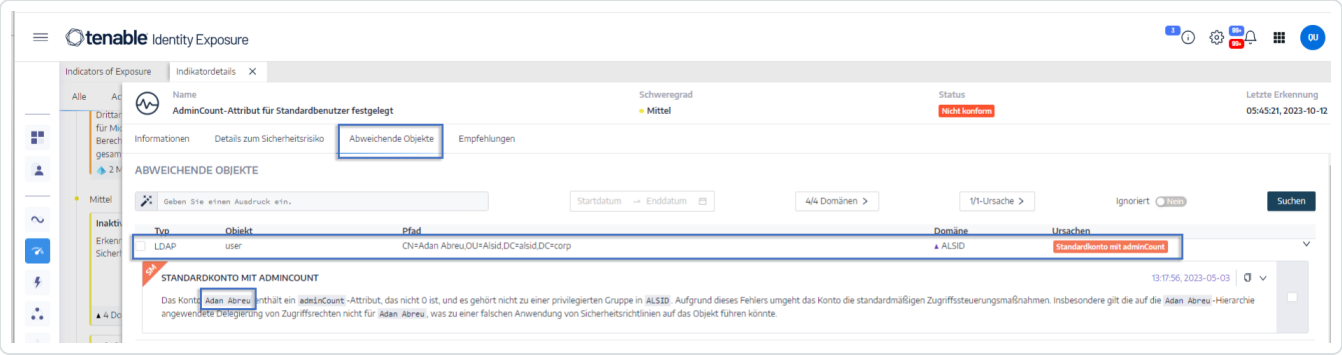
   Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die abweichende Objekte enthalten.

2. Klicken Sie auf die Kachel für den IoE **AdminCount-Attribut für Standardbenutzer festgelegt**.



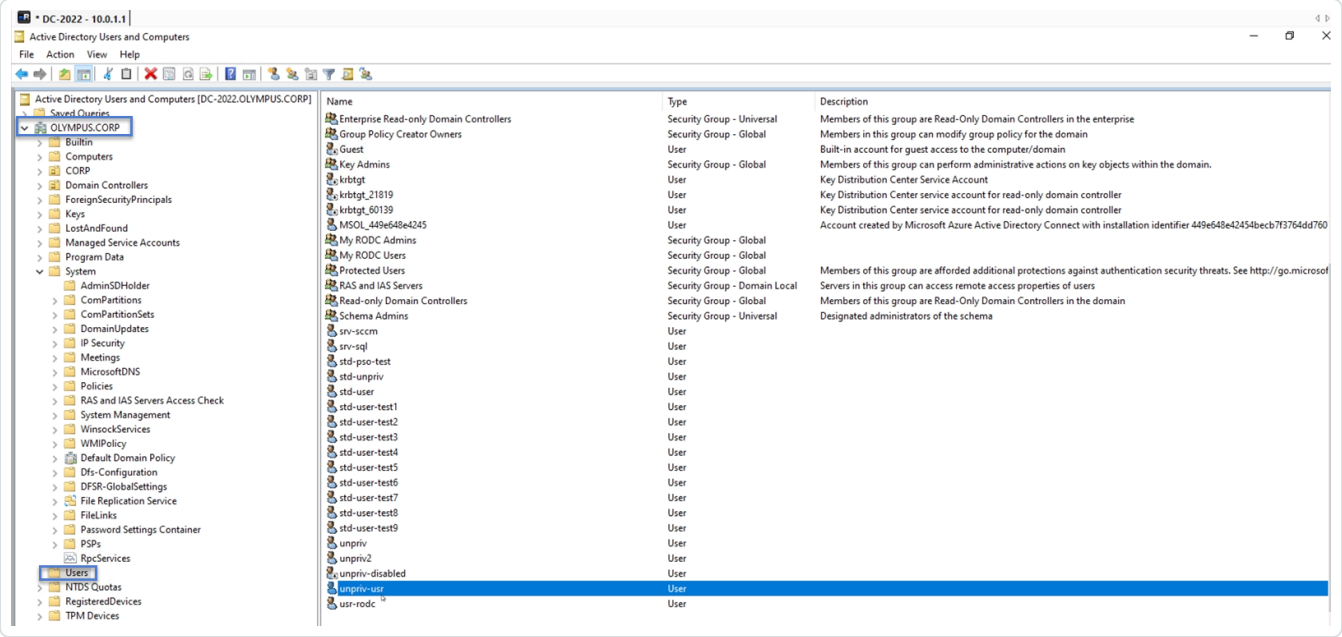
Der Fensterbereich **Indikatordetails** wird geöffnet.

3. Bewegen Sie den Mauszeiger über das abweichende Objekt und klicken Sie darauf, um seine Details anzuzeigen. Notieren Sie sich den Domänennamen und das Konto. (In diesem Beispiel: Domäne = `OLYMPUS.CORP`, das Standardkonto ist `unpriv-usr`)



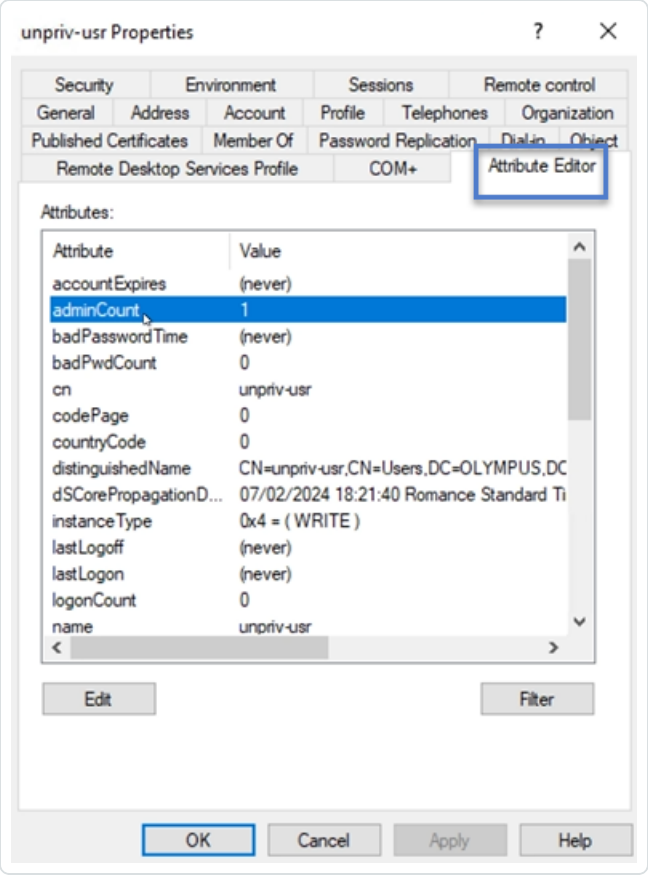
4. Suchen Sie im Remote Desktop Manager (oder einem ähnlichen Tool) nach dem Domänennamen und navigieren Sie zu **Benutzern** und dem von Tenable Identity Exposure gekennzeichneten Konto.

> **Erforderliche Berechtigung**: Sie müssen über ein Administratorkonto in der Domäne verfügen, um das Verfahren durchzuführen.

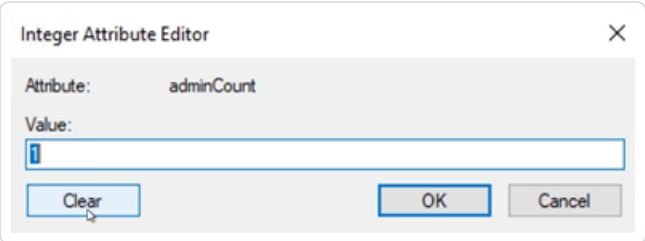


5. Klicken Sie auf den Kontonamen, um das zugehörige Dialogfeld **Eigenschaften** zu öffnen, und wählen Sie die Registerkarte **Attribut-Editor** aus.

6. Klicken Sie in der Liste der Attribute auf `adminCount`, um das Dialogfeld mit dem **Editor für Integer-Attribute** zu öffnen.



7. Klicken Sie im Dialogfeld auf **Löschen** und auf **OK**.



8. Kehren Sie in Tenable Identity Exposure zum Fensterbereich „Indikatordetails“ zurück und aktualisieren Sie die Seite.

   Das abweichende Objekt wird nicht mehr in der Liste angezeigt.

Gefährliche Kerberos-Delegierung

Das Kerberos-Protokoll, das für die Sicherheit von Active Directory von zentraler Bedeutung ist, ermöglicht bestimmten Servern die Wiederverwendung der Anmeldeinformationen von Benutzern. Wenn ein Angreifer solch einen Server kompromittiert, kann er diese Anmeldeinformationen stehlen und sie verwenden, um sich bei anderen Ressourcen zu authentifizieren.

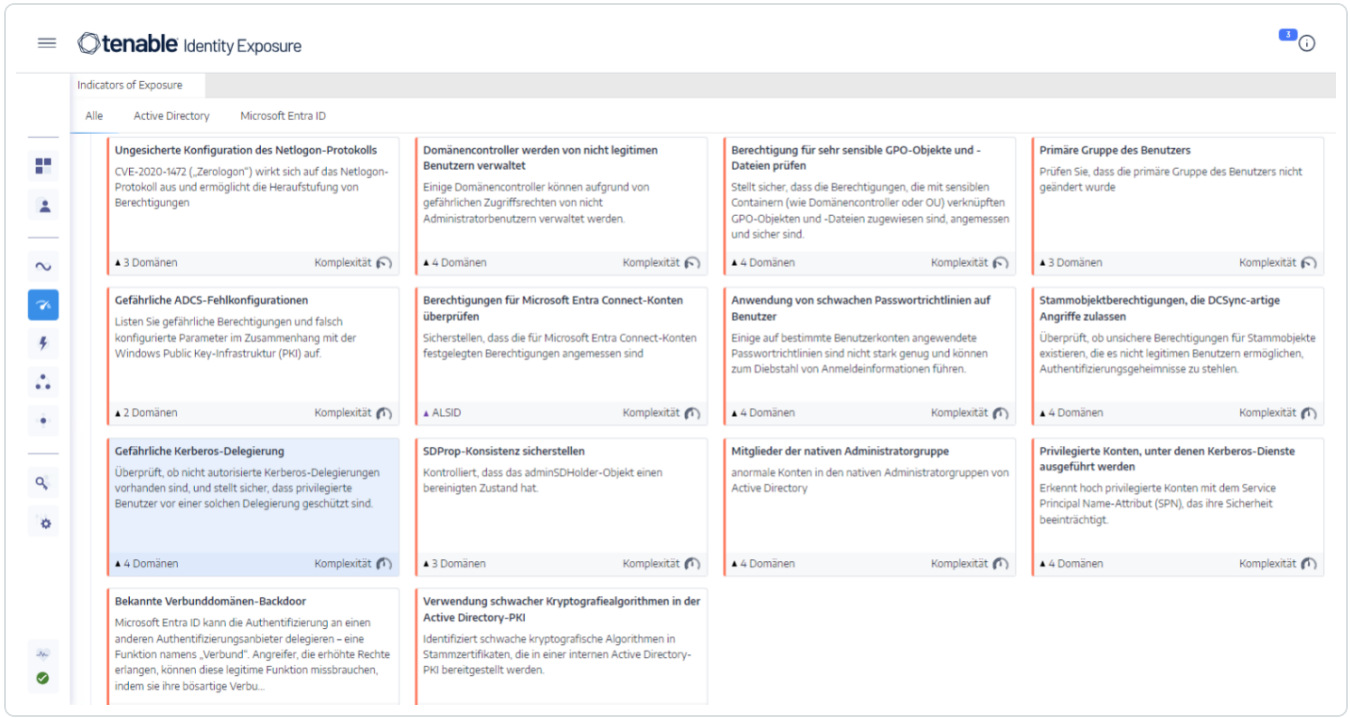
Dieser IoE mit Schweregrad „Kritisch“ meldet alle Konten mit Delegierungsattributen und schließt deaktivierte Konten aus. Privilegierte Benutzer sollten keine Delegierungsattribute haben. Um diese Benutzerkonten zu schützen, fügen Sie sie zur Gruppe „Geschützte Benutzer“ hinzu oder markieren Sie sie als „Konto ist vertraulich und kann nicht delegiert werden“.

So fügen Sie das Konto zur Gruppe „Geschützte Benutzer “ hinzu:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**, um dieses Fenster zu öffnen.

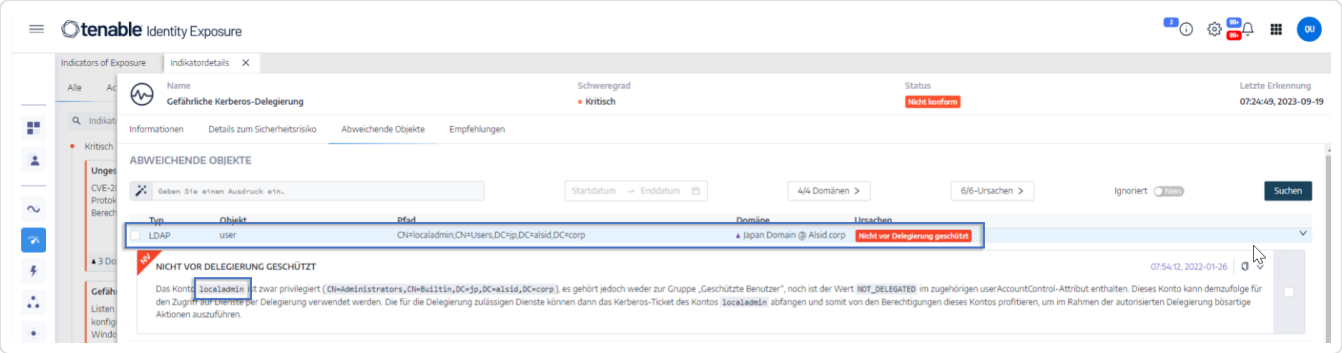
   Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die abweichende Objekte enthalten.

2. Klicken Sie auf die Kachel für den IoE **Gefährliche Kerberos-Delegierung**.



Der Fensterbereich **Indikatordetails** wird geöffnet.

3. Bewegen Sie den Mauszeiger über das abweichende Objekt und klicken Sie darauf, um seine Details anzuzeigen. Notieren Sie sich den Domänennamen und das Konto. (In diesem Beispiel: Domäne = OLYMPUS.CORP und Konto = `adm-t0`)

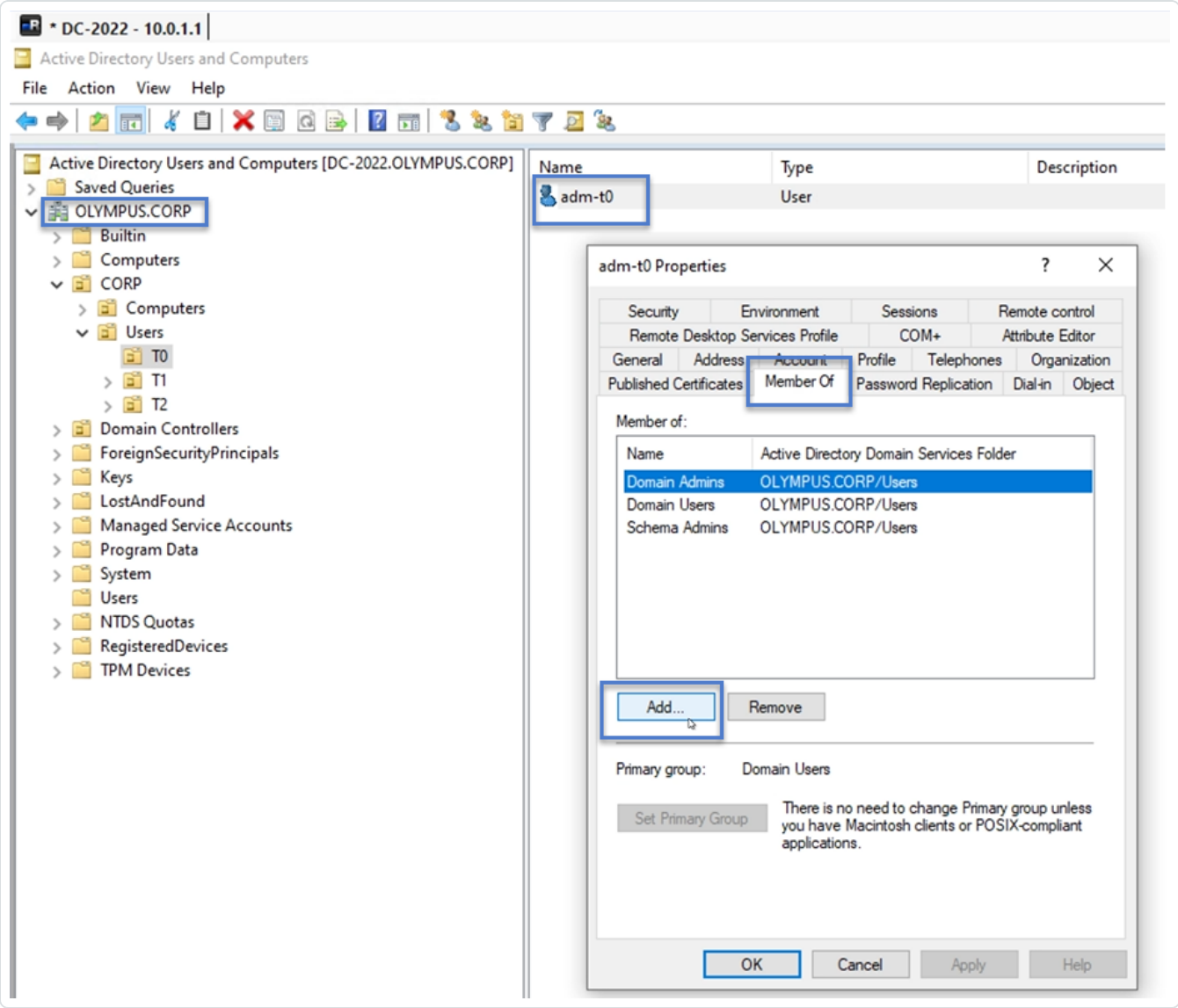


4. Suchen Sie im Remote Desktop Manager (oder einem ähnlichen Tool) nach dem Domänennamen und navigieren Sie zu der Domäne und dem Konto, die von Tenable Identity Exposure gekennzeichnet wurden.

> **Erforderliche Berechtigung**: Sie müssen über ein Administratorkonto in der Domäne verfügen, um das Verfahren durchzuführen.

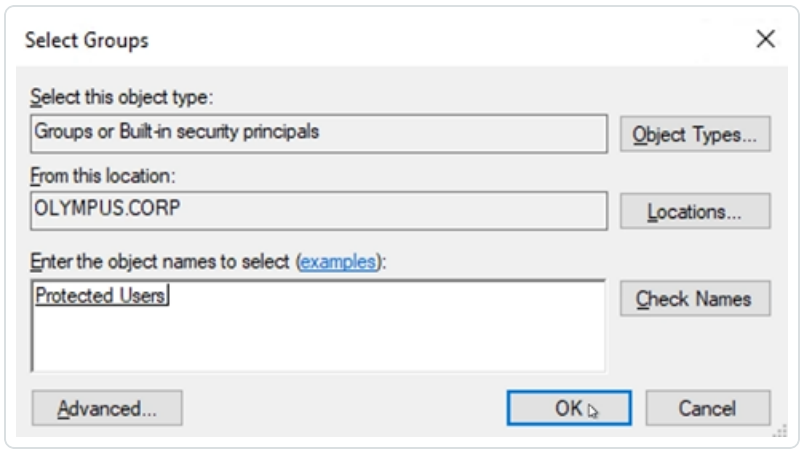
5. Klicken Sie auf den Namen des Kontos, um das zugehörige Dialogfeld **Eigenschaften** zu öffnen, und wählen Sie die Registerkarte **Mitglied von** aus.

6. Klicken Sie in der Mitgliederliste auf **Hinzufügen**.



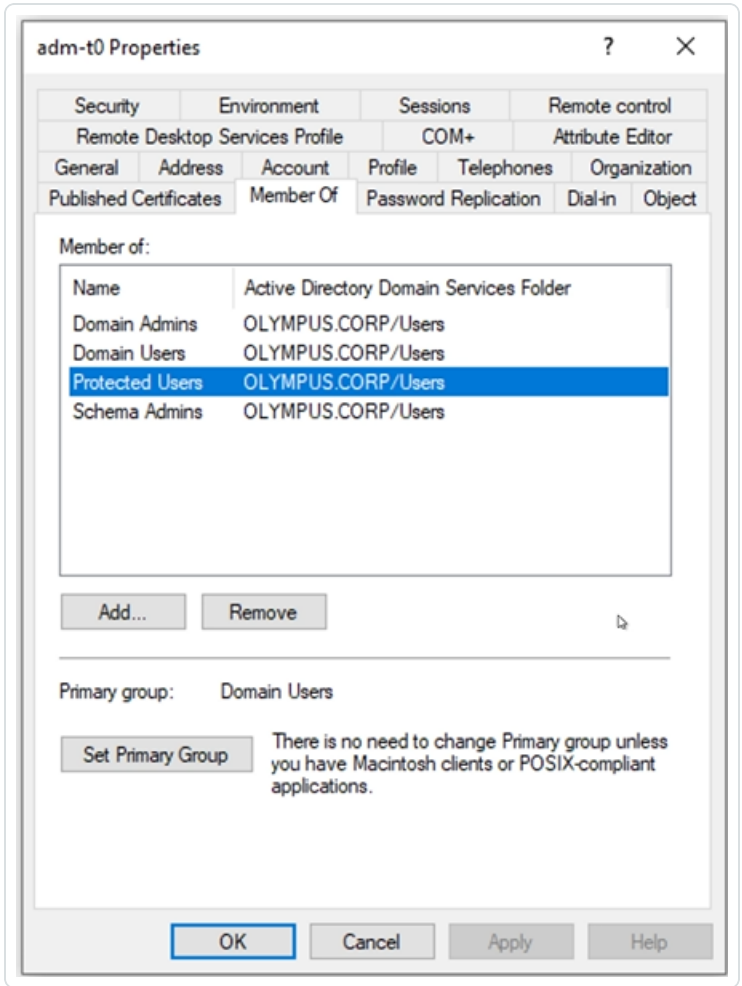
Das Dialogfeld **Gruppen auswählen** wird geöffnet.

7. Geben Sie den Objektnamen „Geschützte Benutzer“ ein und klicken Sie auf **Namen überprüfen**.



8. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
9. Klicken Sie im Dialogfeld **Eigenschaften** auf **Anwenden**.

   Die neue Gruppe wird in der Mitgliederliste angezeigt.



10. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
11. Kehren Sie in Tenable Identity Exposure zum Fensterbereich „Indikatordetails“ zurück und aktualisieren Sie die Seite.

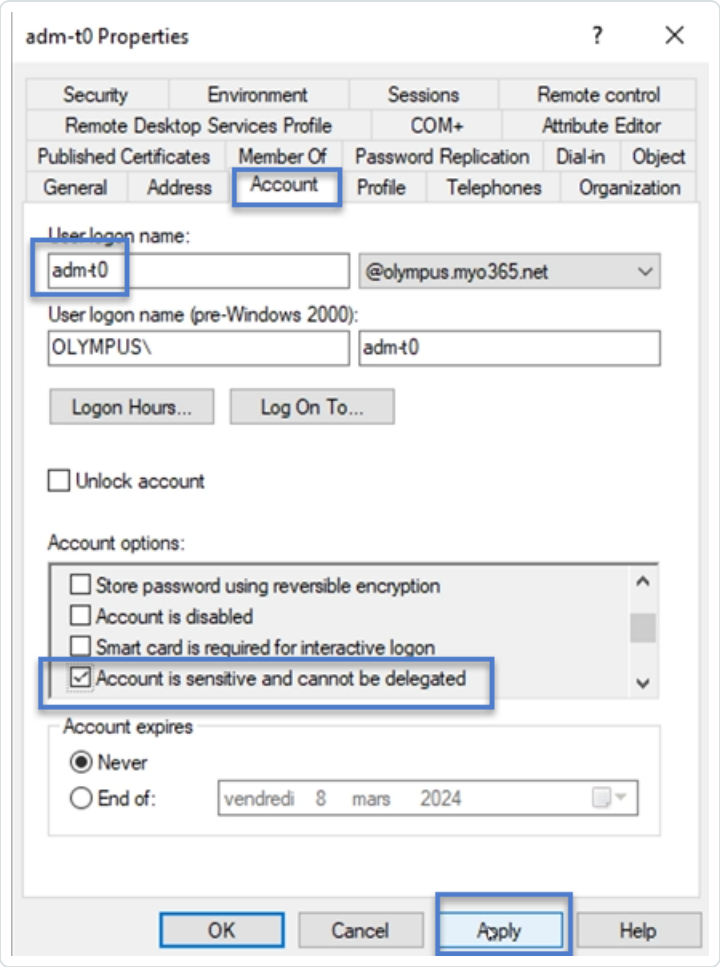
    Das abweichende Objekt wird nicht mehr in der Liste angezeigt.

So legen Sie das Konto als „kann nicht delegiert werden“ fest:

1. Suchen Sie im Remote Desktop Manager nach dem Domänennamen und navigieren Sie zu der Domäne und dem Konto, die von Tenable Identity Exposure gekennzeichnet wurden.

   > **Erforderliche Berechtigung**: Sie müssen über ein Administratorkonto in der Domäne verfügen, um das Verfahren durchzuführen.

2. Klicken Sie auf den Kontonamen, um das zugehörige Dialogfeld **Eigenschaften** zu öffnen, und wählen Sie die Registerkarte **Konto** aus.
3. Wählen Sie in der Liste der Kontooptionen die Option „Konto ist vertraulich und kann nicht delegiert werden“ aus und klicken Sie auf **Anwenden**.



4. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
5. Kehren Sie in Tenable Identity Exposure zum Fensterbereich „Indikatordetails“ zurück und aktualisieren Sie die Seite.

   Das abweichende Objekt wird nicht mehr in der Liste angezeigt.

SDProp-Konsistenz sicherstellen

Angreifer, die eine Active Directory-Domäne kompromittieren, ändern häufig die ACL des `adminSDHolder`-Objekts. Alle Berechtigungen, die sie der ACL hinzufügen, werden für privilegierte Benutzern kopiert, was die Einrichtung von Backdoors einfach macht.

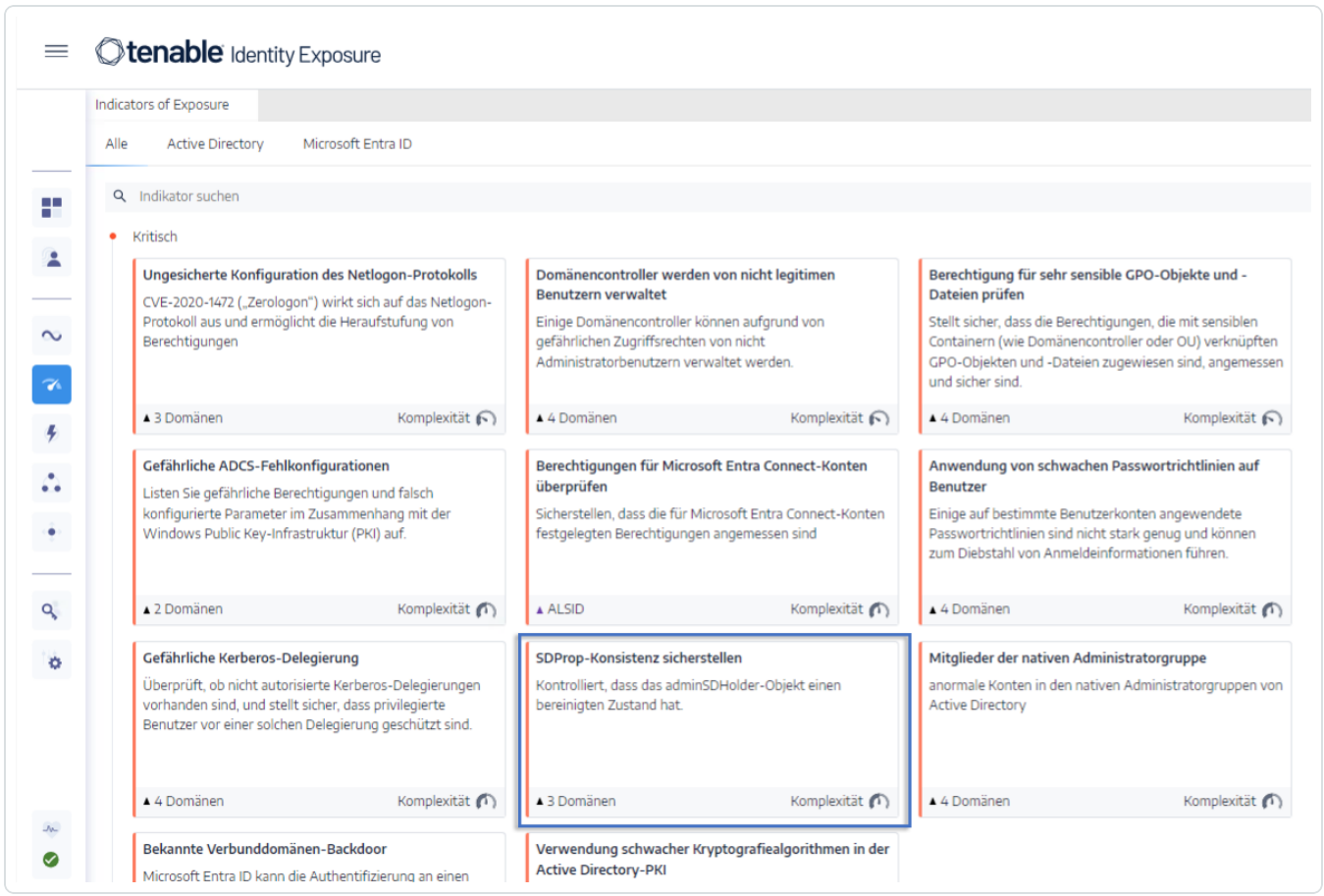
Dieser IoE mit Schweregrad „Kritisch“ prüft, ob die für das `adminSDHolder`-Objekt festgelegten Berechtigungen nur privilegierten Zugriff auf Administratorkonten erlauben.

So führen Sie Behebungsmaßnahmen für ein abweichendes Objekt aus dem IoE **SDProp-Konsistenz sicherstellen** durch:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Exposure**, um dieses Fenster zu öffnen.

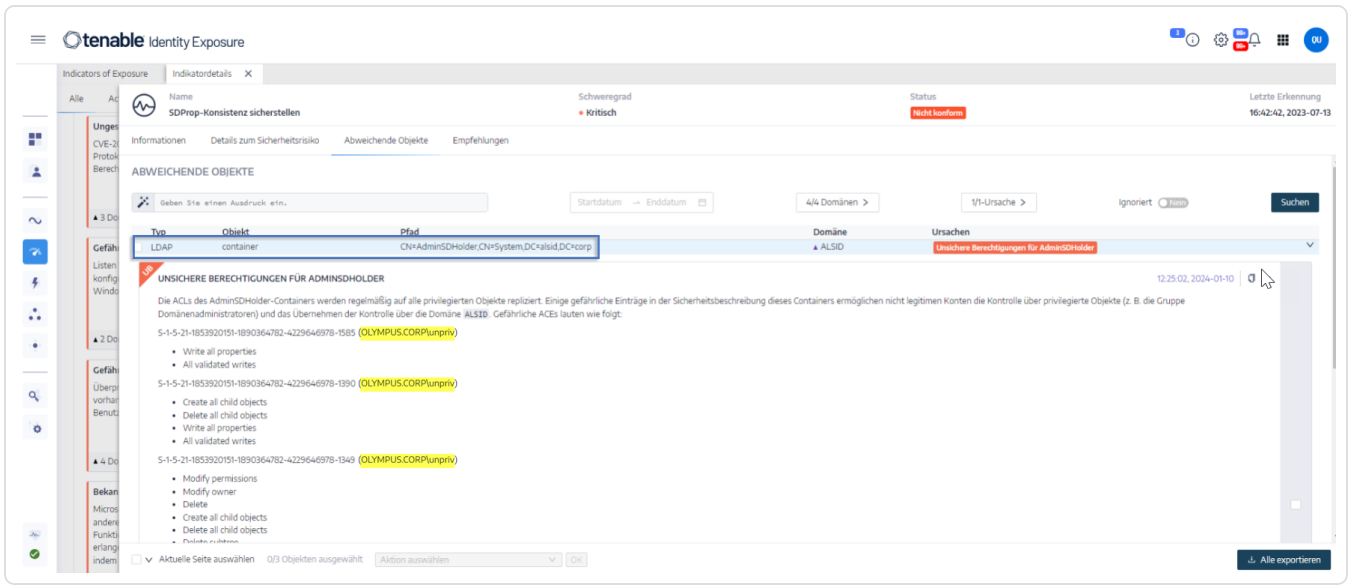
   Standardmäßig zeigt Tenable Identity Exposure nur die IoEs an, die abweichende Objekte enthalten.

2. Klicken Sie auf die Kachel für den IoE **SDProp-Konsistenz sicherstellen**.



Der Fensterbereich **Indikatordetails** wird geöffnet.

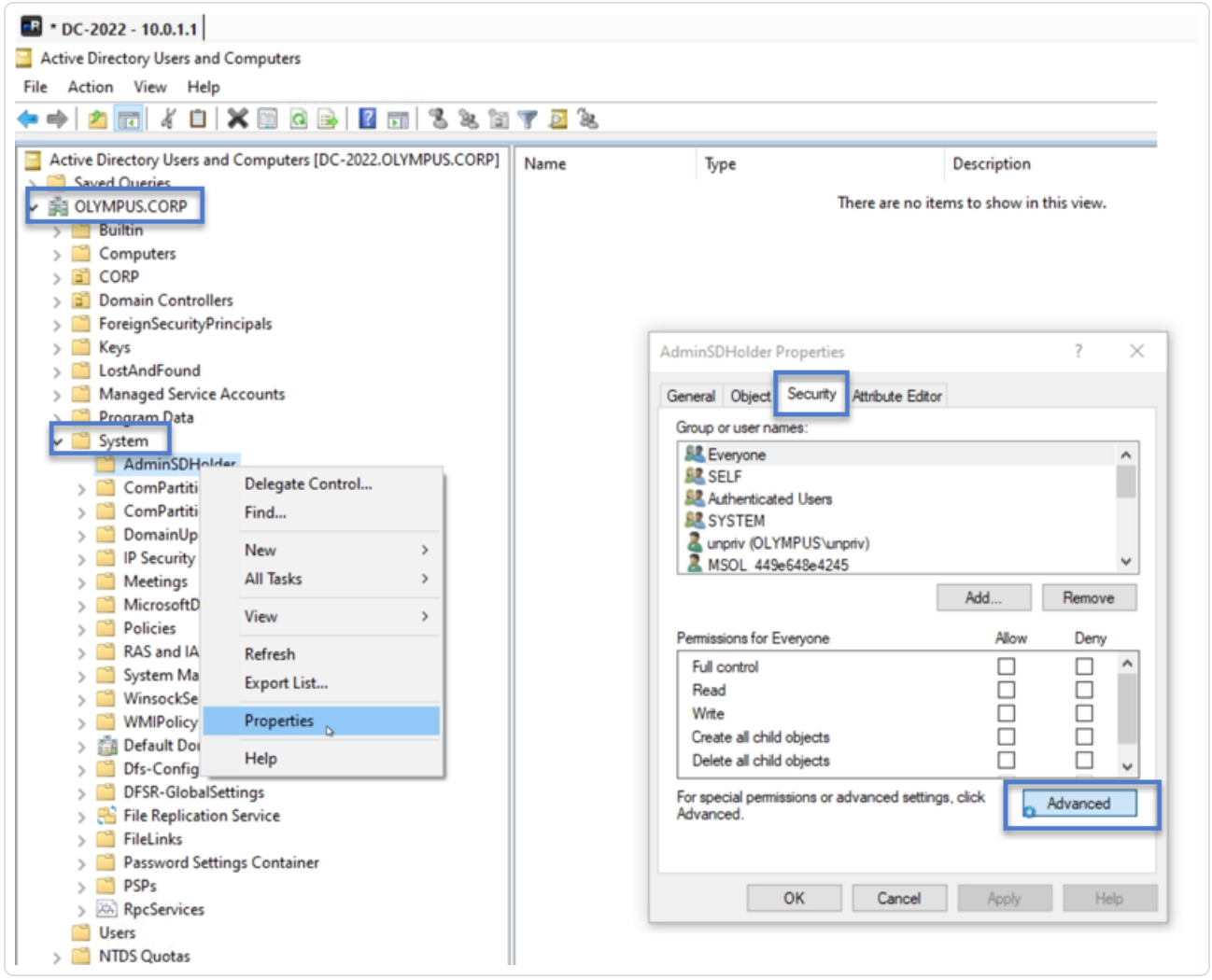
3. Bewegen Sie den Mauszeiger über das abweichende Objekt und klicken Sie darauf, um seine Details anzuzeigen. Notieren Sie sich den Domänennamen und die zugehörige Berechtigung, die von Tenable Identity Exposure gekennzeichnet wurde. (In diesem Beispiel: `OLYMPUS.CORP .\unpriv`)



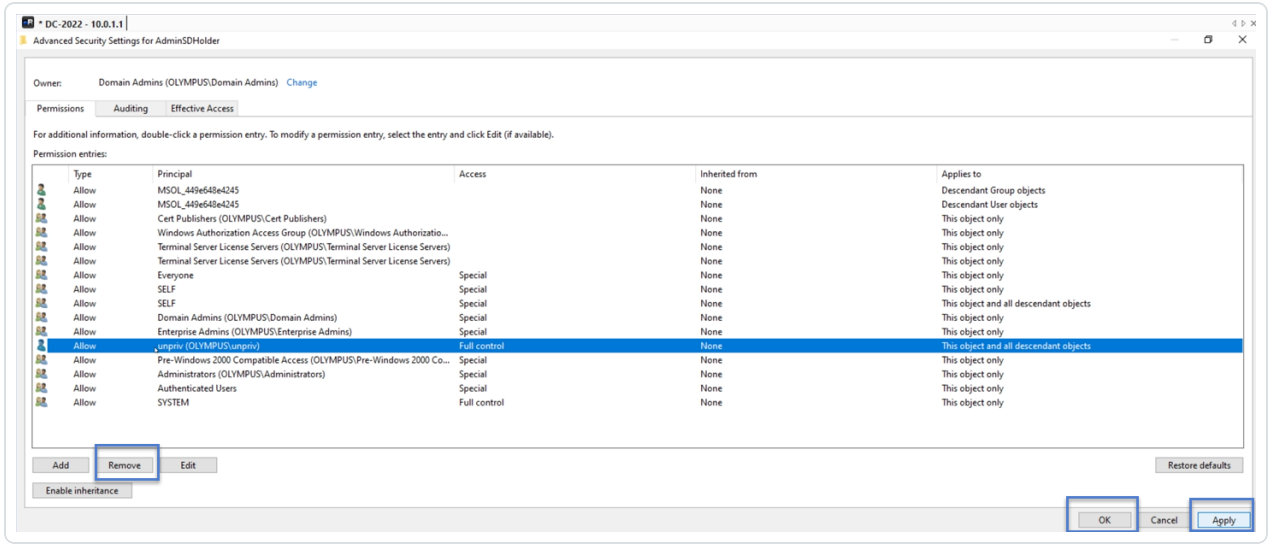
4. Suchen Sie im Remote Desktop Manager (oder einem ähnlichen Tool) nach dem Domänennamen und navigieren Sie zu **System** > **AdminSDHolder**.

> **Erforderliche Berechtigung**: Sie müssen über ein Administratorkonto in der Domäne verfügen, um das Verfahren durchzuführen.

5. Klicken Sie mit der rechten Maustaste auf **AdminSDHolder** und wählen Sie **Eigenschaften** im Kontextmenü aus.



6. Wählen Sie im Dialogfeld **Eigenschaften** die Registerkarte **Sicherheit** aus und klicken Sie auf **Erweitert**.
7. Wählen Sie im Fenster **Erweiterte Sicherheitseinstellungen** auf der Registerkarte **Berechtigungen** die Berechtigung, die die Warnung ausgelöst hat, in der Liste der Berechtigungseinträge aus.
8. Klicken Sie auf **Entfernen**.
9. Klicken Sie auf **Anwenden** und **OK**, um das Einstellungsfenster zu schließen.
10. Klicken Sie auf **OK**, um das Fenster **Eigenschaften** zu schließen.



11. Kehren Sie in Tenable Identity Exposure zum Fensterbereich „Indikatordetails“ zurück und aktualisieren Sie die Seite.

    Das abweichende Objekt wird nicht mehr in der Liste angezeigt.

Indicators of Attack

Erforderliche Lizenz: Indicators of Attack

Mit dem Modul **Indicators of Attack** (IoA) von Tenable Identity Exposure können Sie Angriffe auf Ihr Active Directory (AD) erkennen.

Eine konsolidierte Ansicht von Indicators of Attack zeigt eine Zeitleiste, eine Echtzeit-Ansicht der Top 3-Vorfälle, von denen Ihr AD betroffen war, sowie die Angriffsverteilung in einem einzigen Fensterbereich. Sie haben folgende Möglichkeiten:

- Jede Bedrohung anhand einer genauen Angriffszeitleiste visualisieren.
- Detaillierte Informationen zu einem AD-Angriff analysieren.
- MITRE ATT&CK-Beschreibungen direkt von erkannten Vorfällen aus untersuchen.

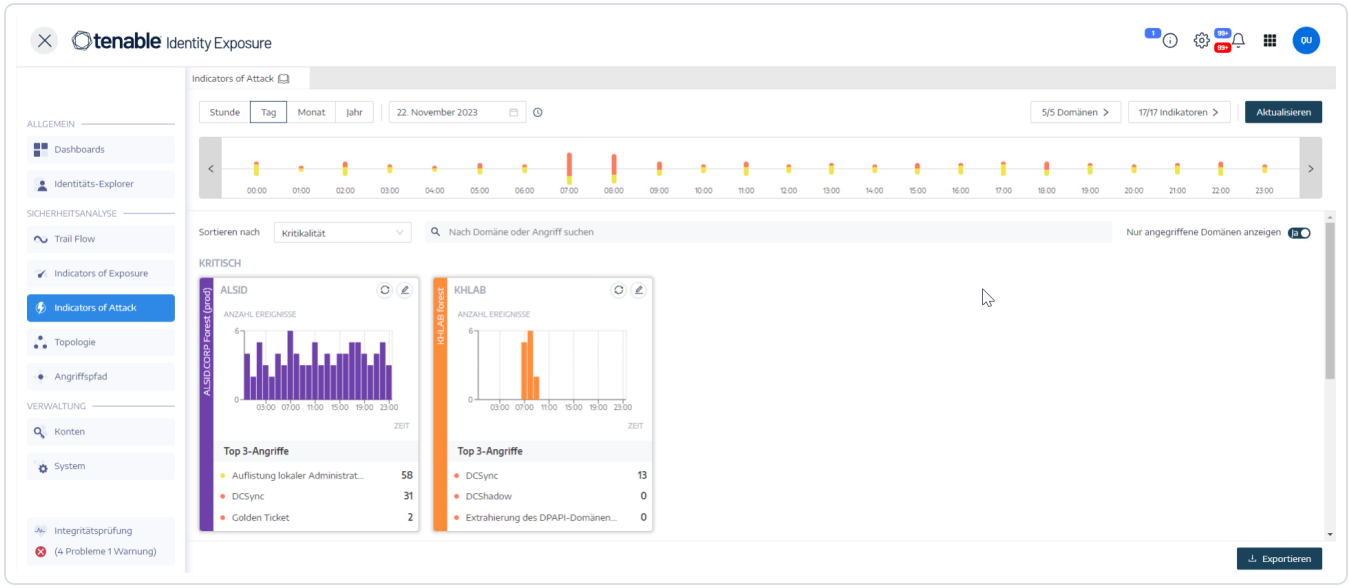
Weitere Informationen zu bestimmten IoAs finden Sie unter Indicators of Attack and the Active Directory.

Hinweis: Wenn Sie eine hohe Anzahl erkannter Angriffe beobachten, überprüfen Sie, ob Ihr Administrator die Indicators of Attack durch Anwendung der empfohlenen Werte für die verschiedenen IoA-Optionen korrekt kalibriert hat. Weitere Informationen finden Sie unter So kalibrieren Sie IoAs.

So zeigen Sie Indicators of Attack an:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Attack**.

   Der Fensterbereich **Indicators of Attack** wird geöffnet.



2. Standardmäßig zeigt Tenable Identity Exposure alle Ihre AD-Gesamtstrukturen und -Domänen an. Um diese Ansicht anzupassen, können Sie einen der folgenden Schritte ausführen:

   - Den anzuzeigenden Zeitraum auswählen – Klicken Sie auf **Stunde**, **Tag** (Standardeinstellung), **Monat** oder **Jahr**.
   - Sich entlang der Zeitleiste bewegen – Klicken Sie auf den Nach-links- oder Nach-rechts-Pfeil, um sich vorwärts oder rückwärts durch die Zeitleiste zu bewegen.
   - Einen bestimmten Zeitpunkt auswählen – Klicken Sie auf die Datumsauswahl, um eine Stunde, einen Tag, einen Monat oder ein Jahr zu wählen.
   - Zum aktuellen Datum und zur aktuellen Zeit zurückkehren – Klicken Sie neben der Datumsauswahl auf das Symbol .
   - Die Domänen auswählen – Klicken Sie auf **n/n Domänen**.

     a. Wählen Sie die Domänen im Fensterbereich **Gesamtstrukturen und Domänen** aus.

     b. Klicken Sie auf **Auswahlbasierter Filter**.

Tenable Identity Exposure aktualisiert die Ansicht.

- IoAs auswählen – Klicken Sie auf **n/n Indikatoren**.

  a. Wählen Sie die IoAs im Fensterbereich „Indicators of Attack“ aus.

  b. Klicken Sie auf **Auswahlbasierter Filter**.

  Tenable Identity Exposure aktualisiert die Ansicht.

- Die IoA-Kacheln sortieren – Klicken Sie auf den Pfeil im Feld **Sortieren nach**, um eine Dropdown-Liste mit Auswahloptionen anzuzeigen: **Domäne**, **Kritikalität** und **Gesamtstruktur**.
- Nach Domäne oder Angriff suchen – Geben Sie im Feld **Suche** den Domänennamen oder Angriff ein.
- Nur angegriffene Domänen anzeigen – Legen Sie den Umschalter **Nur angegriffene Domänen anzeigen** auf **Ja** fest.
- Angriffsbericht exportieren – Klicken Sie auf **Exportieren**.

  Der Fensterbereich **Karten exportieren** wird angezeigt.

  a. Klicken Sie im Feld **Exportformat** auf den Pfeil der Dropdown-Liste, um ein Format auszuwählen: **PDF**, **CSV** oder **PPTX**.

  b. Klicken Sie auf **Exportieren**.

  Tenable Identity Exposure lädt den Bericht auf den lokalen Computer herunter.

Schweregrad

Tenable Identity Exposure erkennt Angriffe und weist ihnen einen Schweregrad zu:

Schweregrad	Beschreibung
Kritisch – Rot	Es wurde ein nachweislicher Post-Exploitation-Angriff erkannt, für den Domänendominanz eine Voraussetzung ist.
Hoch – Orange	Es wurde ein größerer Angriff erkannt, über den ein Angreifer Domänendominanz erlangen kann.

Mittel – Gelb	Der IoA hängt mit einem Angriff zusammen, der zu einer gefährlichen Rechteausweitung führen oder den Zugriff auf sensible Ressourcen ermöglichen könnte.
Gering – Blau	Warnt vor verdächtigem Verhalten in Zusammenhang mit Auskundschaftung oder Vorfällen mit geringen Auswirkungen.

Siehe auch

- Indicator of Attack-Details
- Indicators of Attack-Vorfälle

Indicator of Attack-Details

Der Fensterbereich „Indicators of Attack“ von Tenable Identity Exposure enthält Informationen über Angriffe, die in Ihrem Active Directory stattgefunden haben.

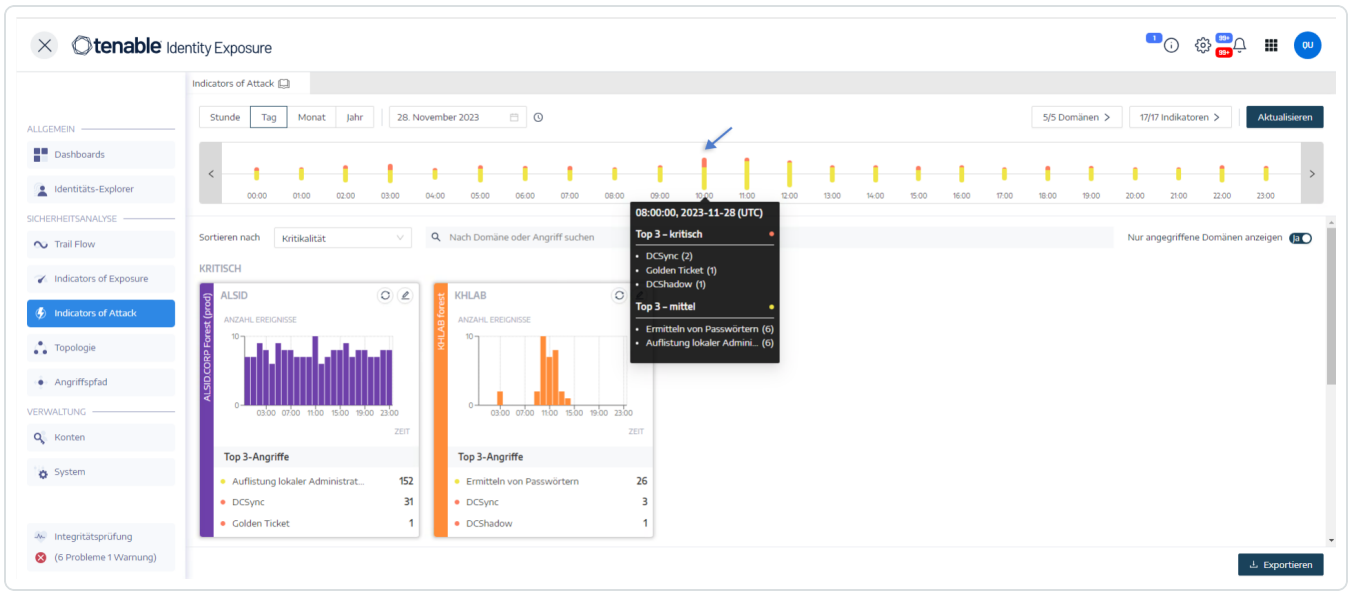
So zeigen Sie Indicators of Attack an:

- Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Attack**.

  Der Fensterbereich **Indicators of Attack** wird geöffnet.

So zeigen Sie Angriffsinformationen in der Zeitleiste an:

- Klicken Sie auf ein beliebiges Ereignis in der Zeitleiste, um Folgendes anzuzeigen:
  - Das Datum und die Uhrzeit der Entdeckung des Vorfalls.
  - Die Schweregradstufe der Top 3-Angriffe.
  - Die Gesamtzahl der zu diesem Datum und dieser Uhrzeit festgestellten Angriffe.



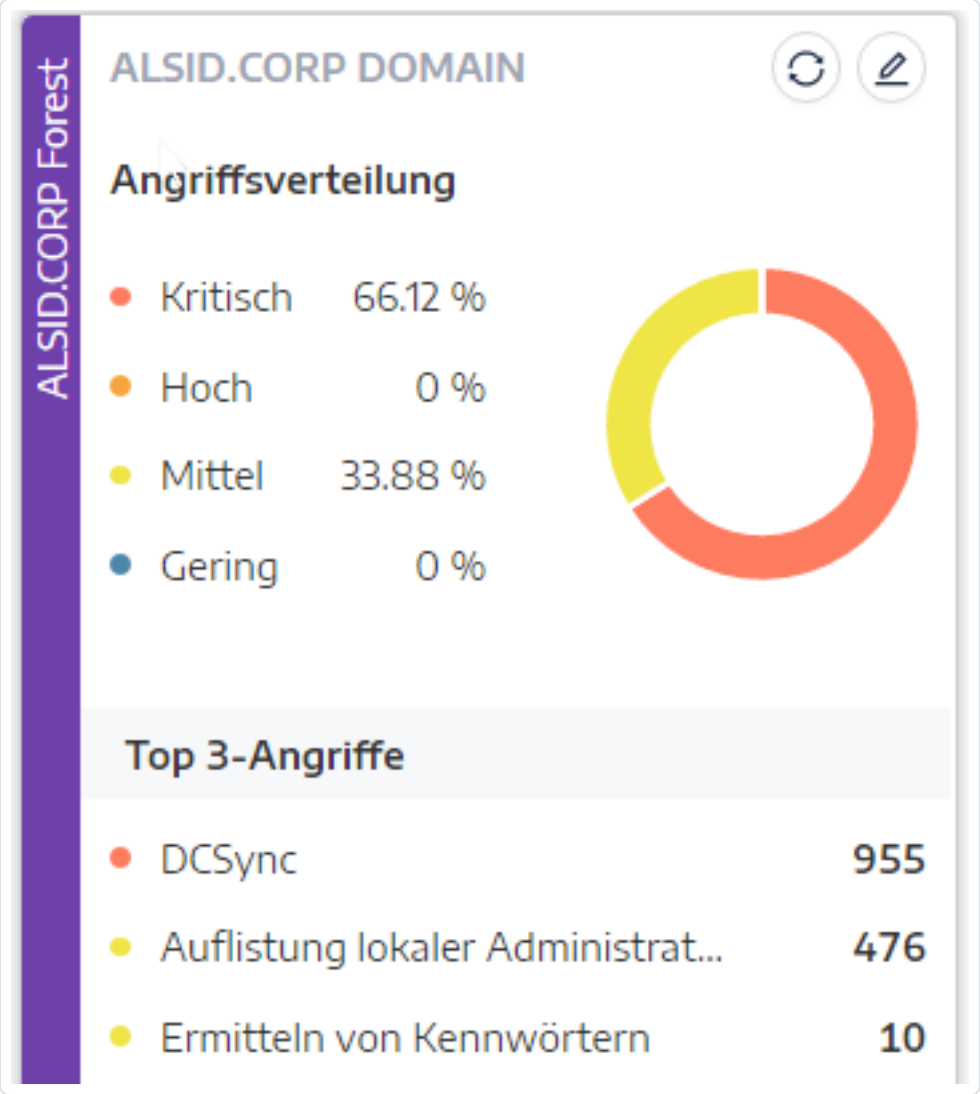
So ändern Sie den Diagrammtyp:

1. Klicken Sie auf das Symbol ✎, um die Domänenkachel zu bearbeiten.

   Der Fensterbereich **Karteninformationen bearbeiten** wird angezeigt.

2. Wählen Sie einen Diagrammtyp aus:

- **Angriffsverteilung**: Zeigt die Verteilung des Angriffsschweregrads.



- **Anzahl Ereignisse**: Zeigt die Top 3-Angriffe und die Anzahl der Vorkommnisse.

3. Klicken Sie auf **Speichern**.

   Tenable Identity Exposure aktualisiert das Diagramm.

Siehe auch

- Indicators of Attack
- Indicators of Attack-Vorfälle

Indicators of Attack-Vorfälle

Die Liste der Indicators of Attack (IoA)-Vorfälle enthält detaillierte Informationen zu bestimmten Angriffen auf Ihr Active Directory (AD). Anhand dieser Informationen können Sie je nach Schweregradstufe des IoA die erforderlichen Maßnahmen ergreifen.

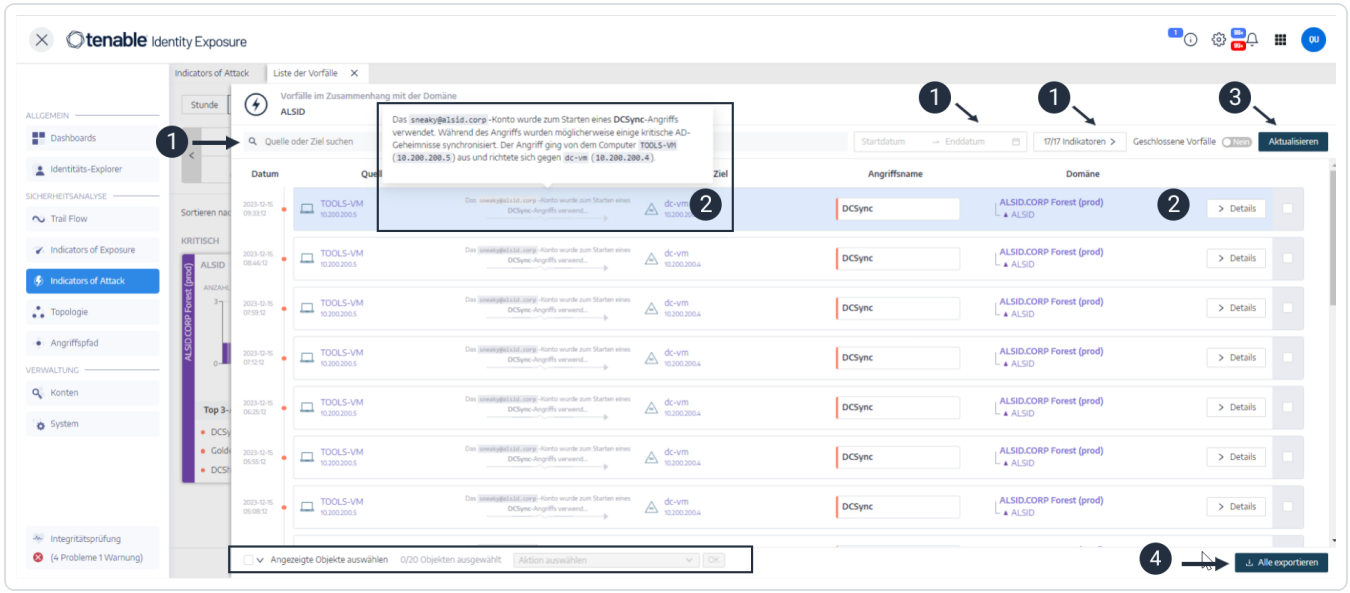
So zeigen Sie Angriffsvorfälle an:

1. Klicken Sie in Tenable Identity Exposure im Navigationsbereich auf **Indicators of Attack**.

   Der Fensterbereich **Indicators of Attack** wird geöffnet.

2. Klicken Sie auf eine beliebige Domänenkachel.

   Daraufhin wird der Fensterbereich **Liste der Vorfälle** mit einer Liste der Vorfälle angezeigt, die in der Domäne aufgetreten sind.



3. In dieser Liste können Sie die folgenden Aufgaben ausführen:
   - Suchkriterien zum Suchen nach bestimmten Vorfällen definieren ❶ .
   - Detaillierte Erläuterungen zu den Angriffen aufrufen, die das AD betreffen ❷ .
   - Einen Vorfall schließen oder erneut öffnen ❸ .
   - Einen Bericht mit allen Vorfällen herunterladen ❹ .

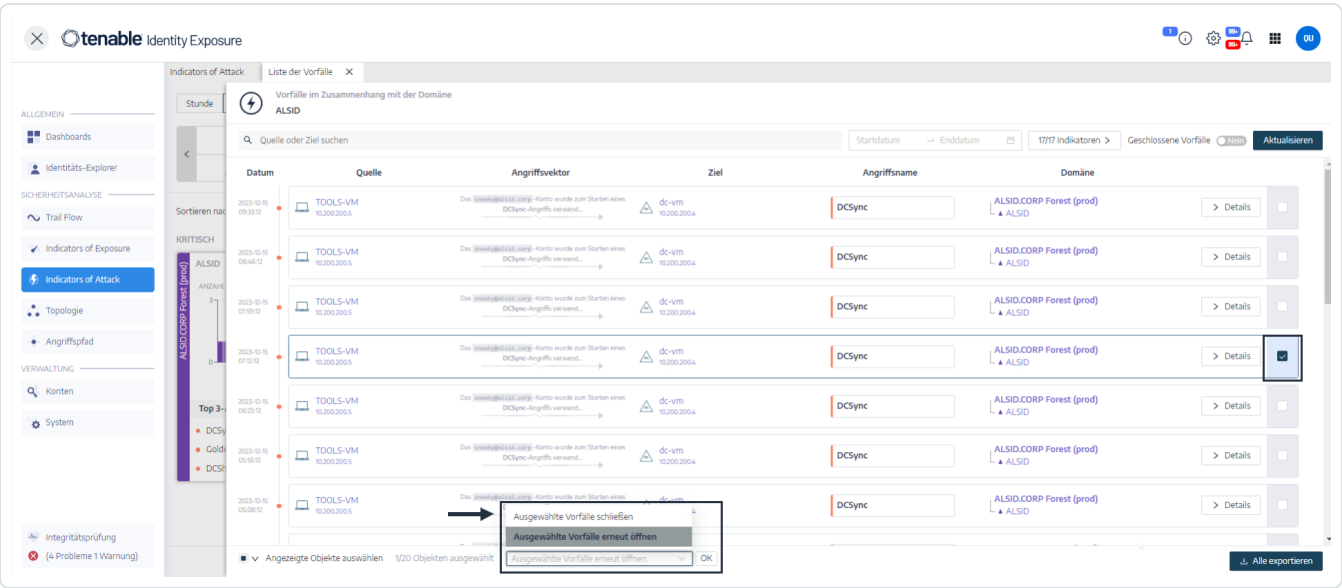
So suchen Sie nach einem Vorfall:

1. Geben Sie im Feld **Suchen** den Namen einer Quelle oder eines Ziels ein.
2. Klicken Sie auf die Datumsauswahl, um ein Startdatum und ein Enddatum für den Vorfall auszuwählen.
3. Klicken Sie auf **n/n Indikatoren**, um die zugehörigen Indikatoren auszuwählen.
4. Stellen Sie den Umschalter **Geschlossene Vorfälle** auf **Ja**, um die Suche auf geschlossene Vorfälle zu beschränken.
5. Klicken Sie auf **Aktualisieren**.

   Tenable Identity Exposure aktualisiert die Liste mit den übereinstimmenden Vorfällen.

So schließen Sie einen Vorfall:

1. Wählen Sie in der Liste der Vorfälle einen Vorfall aus, den Sie schließen oder erneut öffnen möchten.



2. Klicken Sie unten im Fensterbereich auf das Dropdown-Menü und wählen Sie **Ausgewählte Vorfälle schließen** aus.

3. Klicken Sie auf **OK**.

   In einer Meldung werden Sie aufgefordert, den Schließvorgang zu bestätigen.

4. Klicken Sie auf **Bestätigen**.

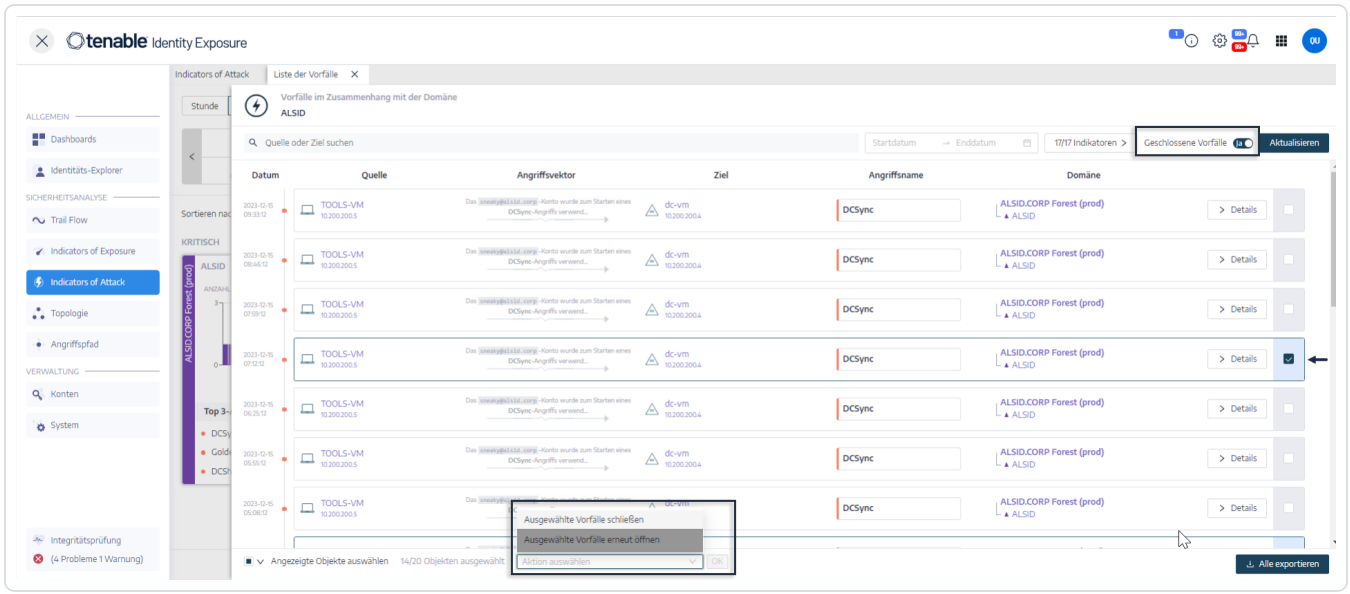
   In einer Meldung wird bestätigt, dass Tenable Identity Exposure den Vorfall geschlossen hat und ihn nicht länger anzeigt.

So öffnen Sie einen Vorfall erneut:

1. Klicken Sie im Fensterbereich **Liste der Vorfälle** auf den Umschalter **Geschlossene Vorfälle**, um ihn auf **Ja** zu setzen.

   Tenable Identity Exposure aktualisiert die Liste mit geschlossenen Vorfällen.

2. Wählen Sie den Vorfall aus, den Sie erneut öffnen möchten.



3. Klicken Sie unten im Fensterbereich auf das Dropdown-Menü und wählen Sie **Ausgewählte Vorfälle erneut öffnen** aus.

4. Klicken Sie auf **OK**.

   In einer Meldung wird bestätigt, dass Tenable Identity Exposure den Vorfall erneut geöffnet hat.

Tipp: Sie können Vorfälle auch in einem Massenvorgang schließen oder erneut öffnen. Klicken Sie unten im Fensterbereich auf **Angezeigte Objekte auswählen**.

Vorfallsdetails

Jeder Eintrag in der Liste der Vorfälle umfasst die folgenden Informationen:

- **Datum** – Das Datum, an dem der Vorfall, der den IoA ausgelöst hat, aufgetreten ist. Tenable Identity Exposure zeigt den jüngsten Vorfall am Anfang der Zeitleiste an.
- **Quelle** – Die Quelle, von der der Angriff ausgegangen ist, und ihre IP-Adresse.
- **Angriffsvektor** – Eine Erklärung, was während des Angriffs geschah.

  > **Tipp**: Bewegen Sie den Mauszeiger über den Angriffsvektor, um weitere Informationen zum IoA anzuzeigen.

- **Ziel** – Das Ziel des Angriffs und seine IP-Adresse.
- **Angriffsname** – Der technische Name des Angriffs.
- **Domäne** – Die vom Angriff betroffenen Domänen.

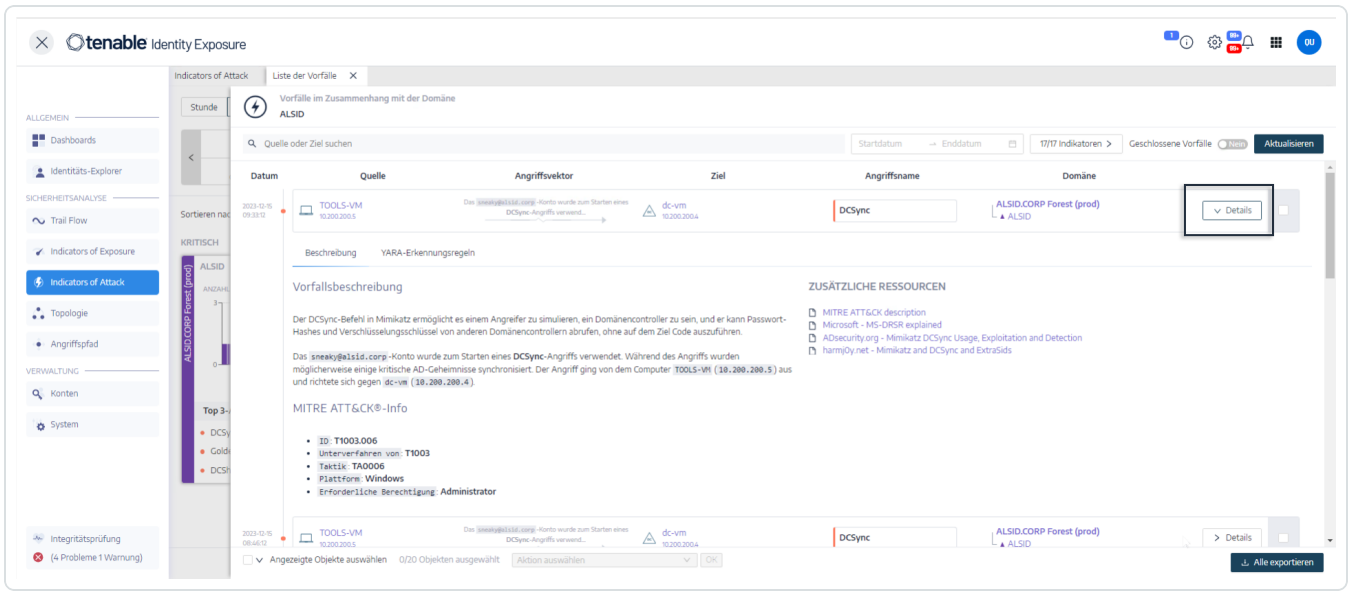
  > **Tipp**: Tenable Identity Exposure kann maximal fünf Fensterbereiche anzeigen, wenn Sie in der **Liste der Vorfälle** auf mehrere interaktive Elemente (Links, Aktionsschaltflächen usw.) klicken. Um alle Fensterbereiche gleichzeitig zu schließen, klicken Sie auf eine beliebige Stelle auf der Seite.

Angriffsdetails

In der Liste der Vorfälle können Sie einen bestimmten Angriff aufschlüsseln und erforderliche Maßnahmen ergreifen, um ihn zu beheben.

So zeigen Sie Angriffsdetails an:

1. Wählen Sie in der Liste der Vorfälle einen Vorfall aus, den Sie aufschlüsseln möchten, um Details anzuzeigen.
2. Klicken Sie auf **Details**.



Tenable Identity Exposure zeigt die Details zum Angriff an:

Beschreibung

Die Registerkarte **Beschreibung** enthält die folgenden Abschnitte:

- **Vorfallsbeschreibung** – Gibt eine kurze Beschreibung des Angriffs.
- **MITRE ATT&CK Info** – Enthält technische Informationen aus der Wissensdatenbank von Mitre Att&ck (Adversarial Tactics, Techniques, and Common Knowledge). Mitre Att&ck ist ein Framework, das Angriffe von Bedrohungsakteuren klassifiziert und die Aktionen beschreibt, die Angreifer durchführen, nachdem sie ein Netzwerk kompromittiert haben. Außerdem werden Standardkennungen für Sicherheitsschwachstellen bereitgestellt, um in der Cybersecurity-Community ein gemeinsames Verständnis zu gewährleisten.
- **Zusätzliche Ressourcen** – Enthält Links zu Websites, Artikeln und Whitepapers mit ausführlicheren Informationen über den Angriff.

YARA-Erkennungsregeln

Auf der Registerkarte **YARA-Erkennungsregeln** werden die YARA-Regeln beschrieben, die Tenable Identity Exposure verwendet, um AD-Angriffe auf Netzwerkebene zu erkennen und damit die Erkennungskette von Tenable Identity Exposure zu stärken.

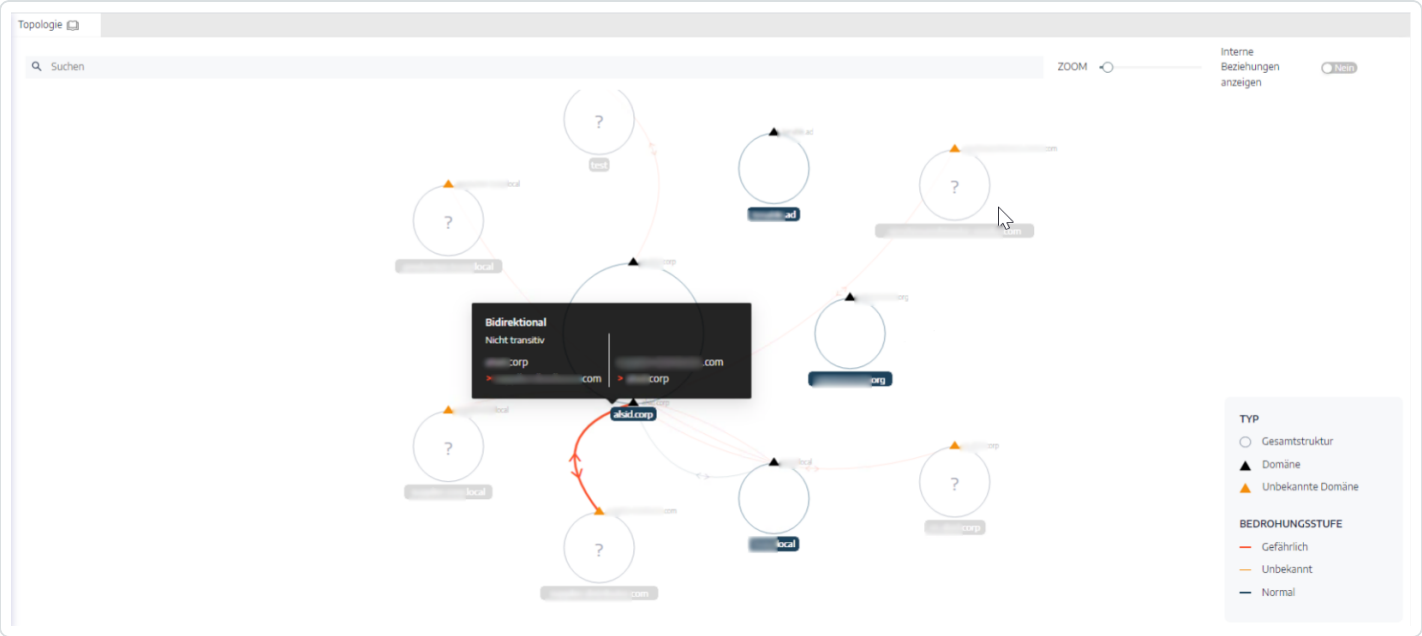
Hinweis: YARA ist der Name eines Tools, das hauptsächlich in der Malware-Forschung und -Erkennung eingesetzt wird. Es bietet einen regelbasierten Ansatz zur Erstellung von Beschreibungen von Malware-Familien auf der Grundlage von textuellen oder binären Mustern. Eine Beschreibung ist im Wesentlichen ein YARA-Regelname. Die Regeln bestehen dabei aus einer Reihe von Zeichenfolgen und einem booleschen Ausdruck (Quelle: wikipedia.org).

Siehe auch

- Indicators of Attack
- Indicator of Attack-Details

Topologie

Auf der Seite „Topologie“ wird eine interaktive grafische Visualisierung Ihres Active Directory angezeigt. Das **Topologiediagramm** zeigt die Gesamtstrukturen, Domänen und die zwischen ihnen bestehenden Vertrauensstellungen an.



So öffnen Sie die Seite „Topologie“:

- Klicken Sie in Tenable Identity Exposure im linken Navigationsmenü auf **Topologie**.

  Der Fensterbereich „Topologie“ wird mit einer grafischen Darstellung Ihres AD geöffnet.

So suchen Sie nach einer Domäne:

- Geben Sie im Fensterbereich **Topologie** den Namen einer Domäne in das Feld **Suche** ein.

  Die Domäne wird in Tenable Identity Exposure hervorgehoben dargestellt.

So vergrößern Sie das Diagramm:

- Klicken Sie im Fensterbereich **Topologie** auf den **Zoom**-Schieberegler, um die Größe des Diagramms anzupassen.

So wird die Verbindung zwischen zwei Domänen angezeigt:

- Stellen Sie im Fensterbereich **Topologie** den Schalter **Interne Beziehungen anzeigen** auf **Ja**.

So zeigen Sie Details zu einer Domäne an:

- Klicken Sie im Fensterbereich **Topologie** auf das Symbol ▲ für den Namen der Domäne.

  Der Fensterbereich **Domänendetails** wird geöffnet und zeigt die erkannten Indicators of Exposure (IoE) und die Compliance-Bewertung für die Domäne an. Sie können auf die Kachel für den IoE klicken, um weitere Informationen zu erhalten.

Siehe auch

- Vertrauensstellungen
- Gefährliche Vertrauensstellungen

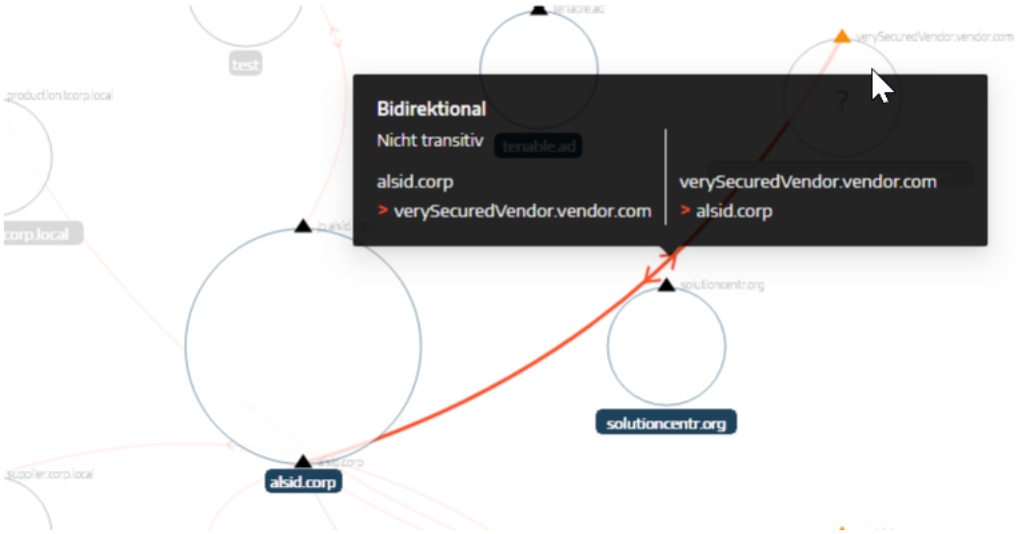
Vertrauensstellungen

Die gebogenen Pfeile zwischen den Domänen im Topologiediagramm stellen Vertrauensstellungen dar.

So zeigen Sie Vertrauensstellungen an:

- Bewegen Sie im Topologiediagramm den Mauszeiger über die gebogenen Pfeile.

  Tenable Identity Exposure zeigt die Vertrauensstellungen mit bestimmten Attributen zwischen zwei Entitäten an.



Die Farbe einer Vertrauensstellung hängt von ihrem Bedrohungsgrad ab:

- **Rot** für gefährliche Vertrauensstellungen
- **Orange** für reguläre Vertrauensstellungen
- **Blau** für unbekannte Vertrauensstellungen

Weitere Informationen finden Sie unter Gefährliche Vertrauensstellungen.

Das Attribut für die Vertrauensstellung gibt die Vertrauensrichtung als **unidirektional** oder **bidirektional** (eingehend/ausgehend) an und zeigt einen der folgenden Werte an:

Wert	Beschreibung
Nicht transitiv	Standardmäßig sind Vertrauensstellungen innerhalb der Gesamtstruktur transitive Vertrauensstellungen. Tenable

	Identity Exposure verwendet dieses Flag, um sie in nicht transitive Vertrauensstellungen umzuwandeln. Andererseits sind Vertrauensstellungen zwischen Gesamtstrukturen standardmäßig nicht transitiv. Daher ist das Flag „Gesamtstruktur transitiv" vorhanden. Tenable Identity Exposure zeigt diesen Wert an, wenn eine Vertrauensstellung zwischen Domänen innerhalb der Gesamtstruktur besteht. Die Vertrauensstellung gewährt keinen Zugriff und delegiert keine Befugnisse an verbundene Domänen außerhalb der Gesamtstruktur.
Gesamtstruktur transitiv	Gibt an, dass eine transitive Vertrauensstellung zwischen zwei Gesamtstrukturen besteht. Die einer anderen Domäne gewährte Vertrauensstellung kann an die vertrauenswürdige Gesamtstruktur weitergegeben werden.
Innerhalb der Gesamtstruktur	Gibt an, dass eine Vertrauensstellung zwischen Domänen innerhalb derselben Gesamtstruktur besteht. Wenn `WITHIN_FOREST` und `QUARANTINED_DOMAIN` beide vorhanden sind, wird die Vertrauensstellung als **QuarantinedWithinForest** bezeichnet.
Nur aufwärtskompatibel	Gibt an, dass die Vertrauensstellung nur von Clients mit Windows 2000 und neueren Betriebssystemen verwendet werden kann.
Als extern behandeln	(Nur, wenn `FOREST_TRANSITIVE` festgelegt ist) Kennzeichnet einen externen Typ von Vertrauensstellung. Tenable Identity Exposure ändert die Filterung der Sicherheitskennungen (SID) für die Vertrauensstellung und erlaubt den SIDs, deren relative Kennung (RID) größer oder gleich 1000 ist, die Gesamtstruktur zu passieren.
In Quarantäne	Gibt an, dass Tenable Identity Exposure die Filterung der SIDs, deren RID größer oder gleich 1000 ist, für die Vertrauensstellung aktiviert hat. Standardmäßig aktiviert Tenable Identity Exposure sie nur für eine externe

	Vertrauensstellung, sie kann aber auch für eine übergeordnete/untergeordnete Vertrauensstellung oder die einer Gesamtstruktur gelten.
Organisationsübergreifende Authentifizierung	Gibt an, dass Tenable Identity Exposure die selektive Authentifizierung aktiviert hat und sie über Domänen- oder Gesamtstruktur-Vertrauensstellungen hinweg verwenden kann.
Selektive Authentifizierung	Weitere Informationen hierzu finden Sie unter „Organisationsübergreifende Authentifizierung“.
Organisationsübergreifend ohne TGT-Delegierung	Wird angezeigt, wenn die Delegierung in einer vertrauenswürdigen Domäne vollständig deaktiviert ist (die Option „ok-as-delegate“ wird in den ausgestellten Diensttickets nie festgelegt).
RC4-Verschlüsselung:	Gibt an, dass die Vertrauensstellung RC4-Verschlüsselungsschlüssel für den Kerberos-Austausch unterstützt. Dieses Flag ist nur vorhanden, wenn sich der `TrustType` auf `TRUST_TYPE_MIT` bezieht.
AES-Schlüssel	Gibt an, dass die Vertrauensstellung AES-Verschlüsselungsschlüssel für den Kerberos-Austausch unterstützt.
PIM-Vertrauensstellung	Wenn die Flags `FOREST_TRANSITIVE` und `TREAT_AS_EXTERNAL` gesetzt sind und das Flag `QUARANTINED_DOMAIN` nicht aktiviert wurde, zeigt das Flag für die PIM-Vertrauensstellung an, dass die vertrauenswürdige Gesamtstruktur privilegierte Identitäten (Privileged Identity Management) in Bezug auf die SID-Filterung verwaltet (lokale SIDs können diese Vertrauensstellung überschreiten). PIM-Vertrauensstellungen werden zur Implementierung von Bastion-Gesamtstrukturen verwendet.
Kein Attribut	Gibt an, dass die externe Vertrauensstellung kein

	bestimmtes Attribut hat.

Gefährliche Vertrauensstellungen

Die Farbe einer Vertrauensstellung hängt von ihrem Bedrohungsgrad ab:

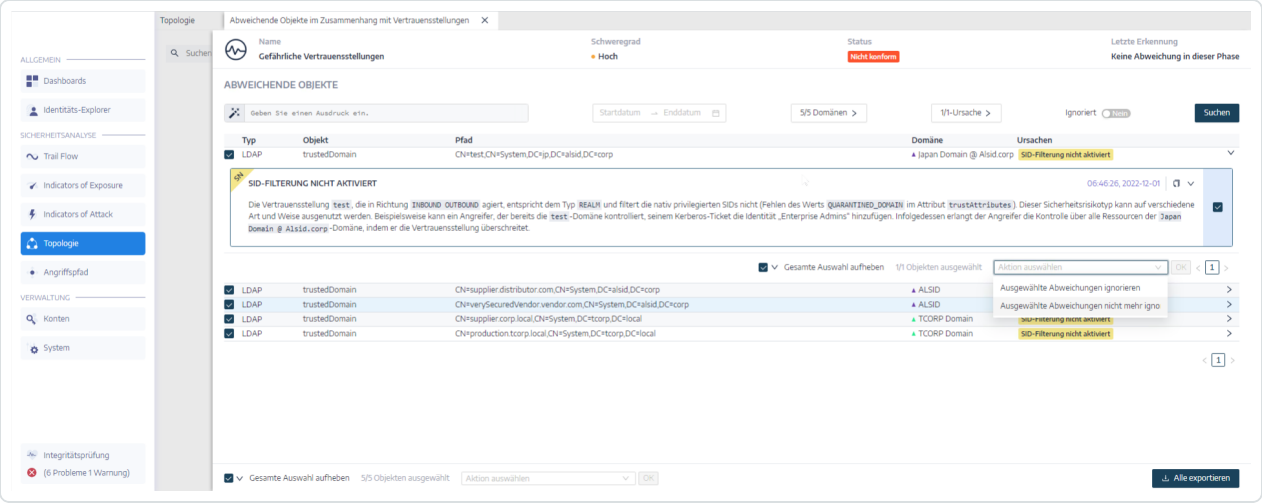
- **Rot** für gefährliche Vertrauensstellungen
- **Orange** für reguläre Vertrauensstellungen
- **Blau** für unbekannte Vertrauensstellungen

So untersuchen Sie eine gefährliche Vertrauensstellung:

1. Klicken Sie im Topologiediagramm auf die gebogenen Pfeile.

   Der Fensterbereich **Abweichende Objekte im Zusammenhang mit Vertrauensstellungen** wird geöffnet.

   > **Tipp**: Die Details der Ereignisse, die in diesem Fensterbereich für gefährliche Vertrauensstellungen angezeigt werden, sind alle mit dem Indicator of Exposure **Gefährliche Vertrauensstellungen** verknüpft, auf den Sie auch über das Navigationsmenü **Indicators of Exposure** zugreifen können.



2. Klicken Sie mit dem Mauszeiger auf ein abweichendes Objekt in der Liste, um die Details anzuzeigen.

So exportieren Sie abweichende Objekte:

1. Klicken Sie im Topologiediagramm auf die gebogenen Pfeile.

   Der Fensterbereich **Abweichende Objekte im Zusammenhang mit Vertrauensstellungen** wird geöffnet.

2. Klicken Sie auf **Alle exportieren**.

   Der Fensterbereich **Abweichende Objekte exportieren** wird geöffnet.

3. Klicken Sie im Feld **Exportformat** auf den Dropdown-Pfeil, um ein Format auszuwählen.

4. Klicken Sie auf **Alle exportieren**.

   Tenable Identity Exposure lädt eine Datei im ausgewählten Format auf Ihren Computer herunter.

5. Klicken Sie auf **X**, um den Fensterbereich zu schließen.

Angriffspfad

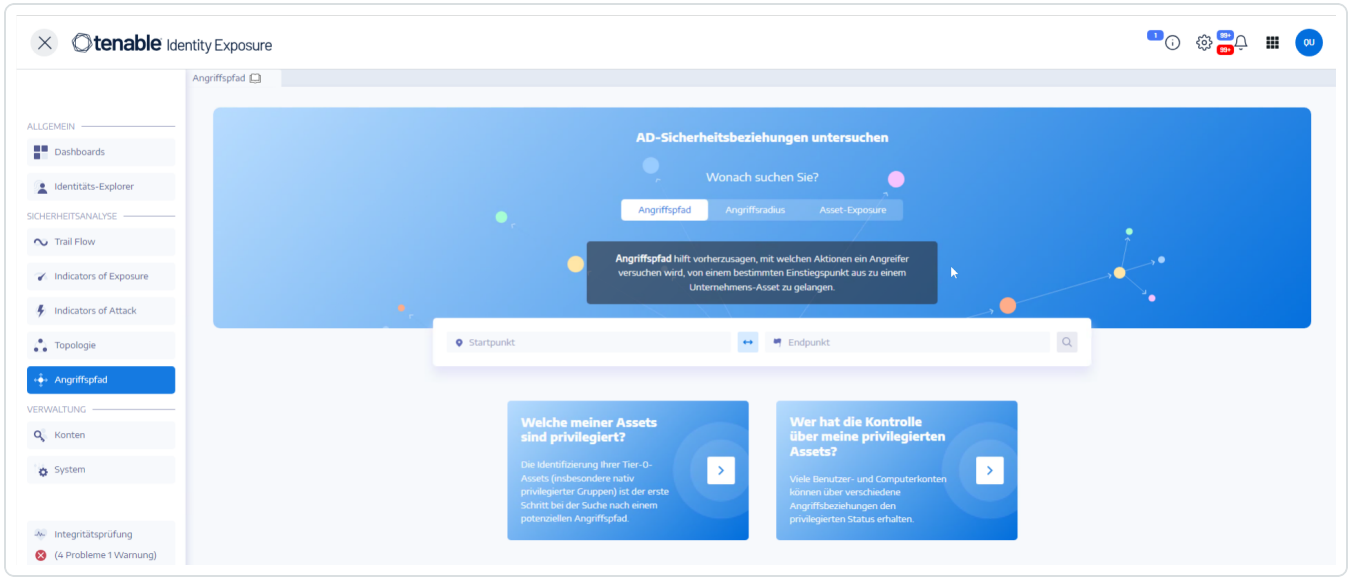
Tenable Identity Exposure bietet mehrere Möglichkeiten, die potenzielle Schwachstelle eines Assets durch grafische Darstellungen zu visualisieren.

- **Angriffspfad**: Zeigt die möglichen Angriffspfade, die ein Angreifer nehmen kann, um ein Asset von einem Einstiegspunkt aus zu kompromittieren.
- **Angriffsradius**: Zeigt die möglichen lateralen Bewegungen (Lateral Movements) in das Active Directory von jedem Asset aus an.
- **Asset-Exposure**: Zeigt alle Pfade, die potenziell die Kontrolle über ein Asset übernehmen können.

So zeigen Sie den Angriffspfad an:

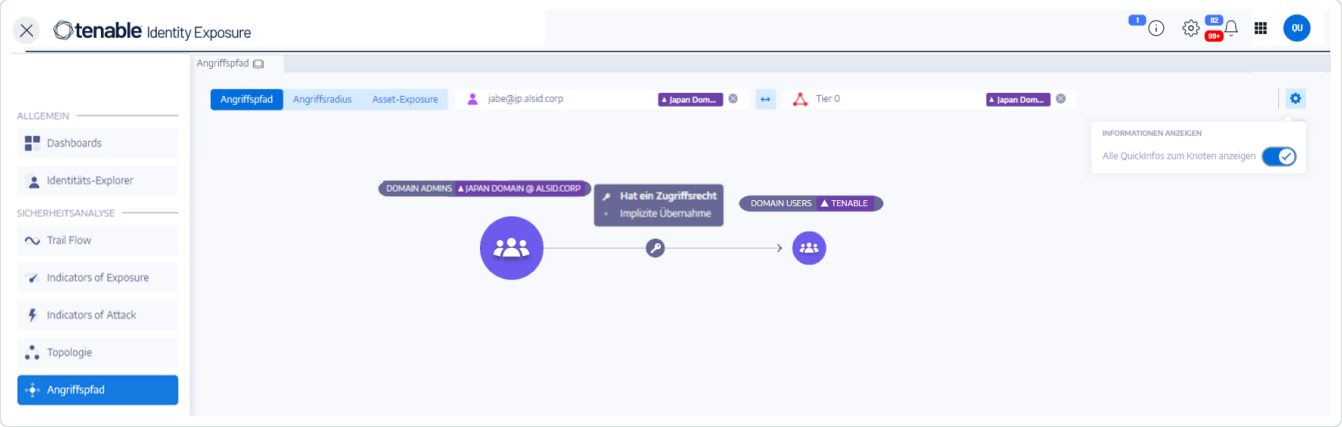
1. Klicken Sie in Tenable Identity Exposure im Menü der Seitenleiste auf **Angriffspfad**.

   Der Fensterbereich **Angriffspfad** wird angezeigt.



2. Klicken Sie im Banner auf **Angriffspfad**.
3. Geben Sie im Feld **Startpunkt** das Asset am Einstiegspunkt ein.
4. Geben Sie im Feld **Endpunkt** das Asset am Ende des Pfades ein.
5. Klicken Sie auf das Symbol .

Tenable Identity Exposure zeigt den Angriffspfad zwischen den beiden Assets an.



6. Optional können Sie auf das Symbol klicken, um Folgendes zu tun:

    - Klicken Sie auf den **Zoom**-Schieberegler, um die Vergrößerung der grafischen Darstellung einzustellen.
    - Klicken Sie auf die Schaltfläche **Alle QuickInfos zum Knoten anzeigen**, um Informationen über die Assets anzuzeigen.

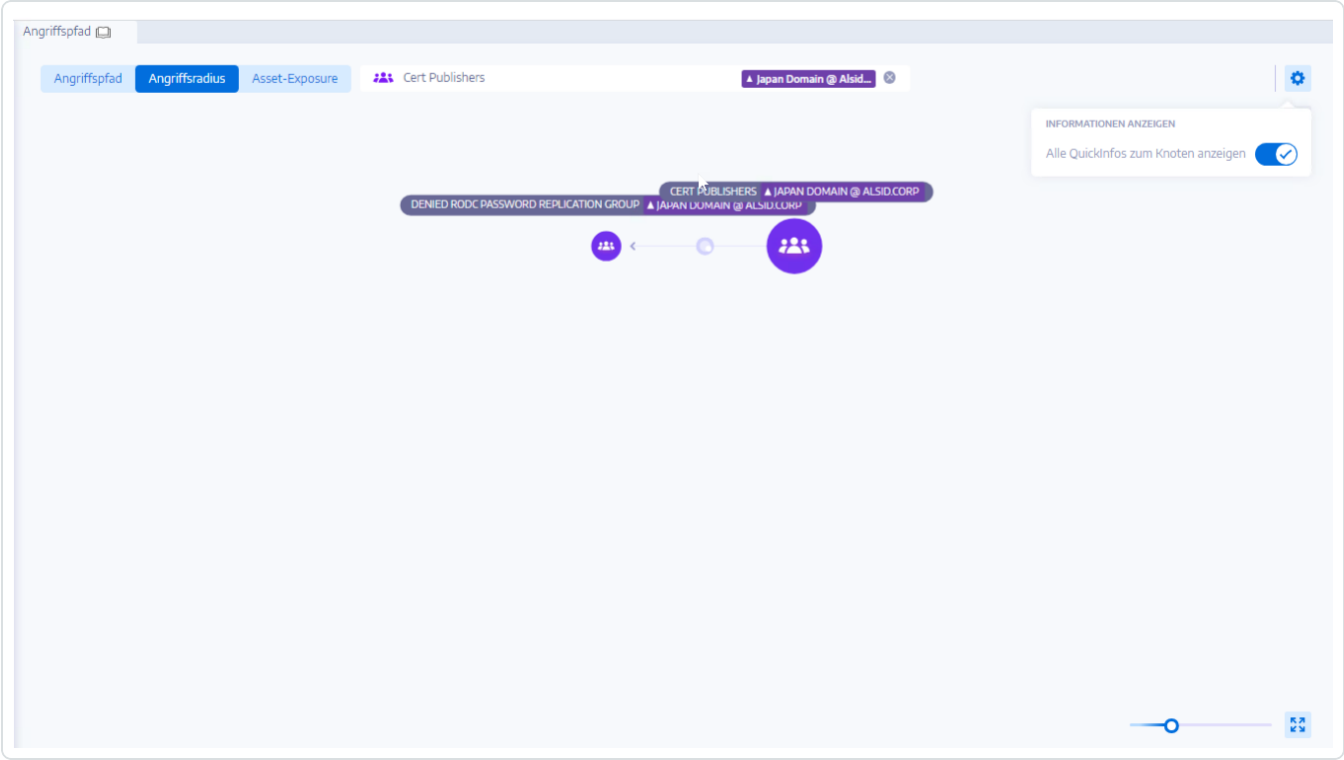
So zeigen Sie den Angriffsradius an:

1. Klicken Sie in Tenable Identity Exposure im Menü der Seitenleiste auf **Angriffspfad**.

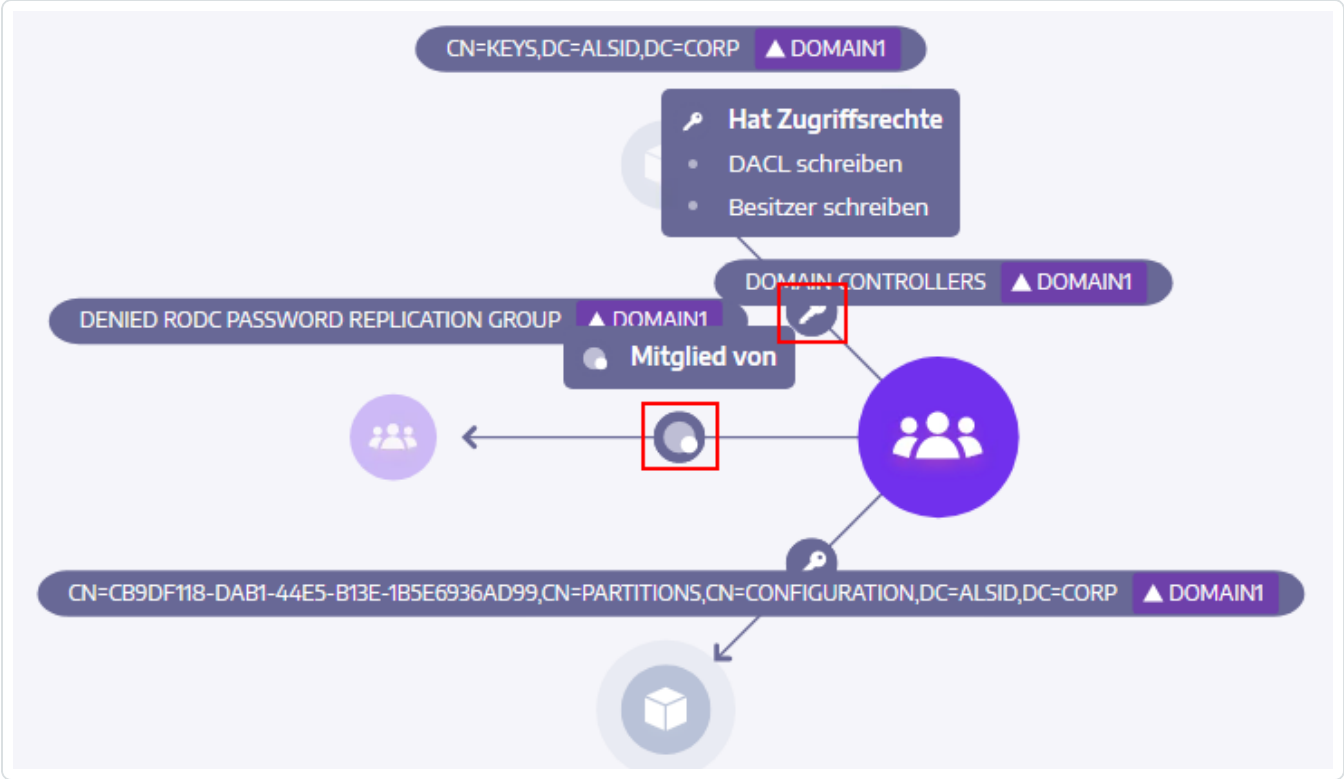
    Der Fensterbereich **Angriffspfad** wird angezeigt.

2. Klicken Sie im Banner auf **Angriffsradius**.
3. Geben Sie im Feld **Objekt suchen** den Namen eines Assets ein.
4. Klicken Sie auf das Symbol .

    Tenable Identity Exposure zeigt die lateralen Verbindungen an, die von diesem Asset ausgehen:



5. Klicken Sie auf die Symbole auf den Pfeilen zwischen den Assets, um die Beziehungen zwischen ihnen anzuzeigen.



So zeigen Sie die Asset-Exposure an:

1. So zeigen Sie den Angriffsradius an:
2. Klicken Sie in Tenable Identity Exposure im Menü der Seitenleiste auf **Angriffspfad**.

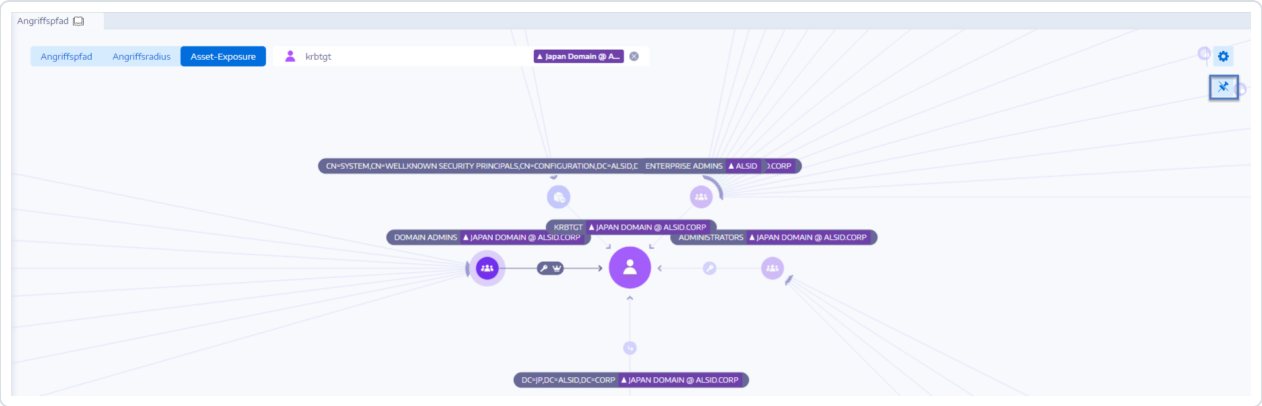
   Der Fensterbereich **Angriffspfad** wird angezeigt.
3. Klicken Sie im Banner auf **Asset-Exposure**.
4. Geben Sie im Feld **Objekt suchen** den Namen eines Assets ein.
5. Klicken Sie auf das Symbol .

   Tenable Identity Exposure zeigt die Pfade, die zu dem Asset führen, und die Beziehungen zwischen den Assets an.
6. Klicken Sie auf die Symbole auf den Pfeilen zwischen den Assets, um die Beziehungen zwischen ihnen anzuzeigen.

So stecken Sie einen Angriffspfad ab:

1. Klicken Sie auf einen Knoten im Angriffspfad, den Sie hervorheben möchten.

   Tenable Identity Exposure steckt diesen Angriffspfad auf den Bildschirm ab.
2. Um den Angriffspfad zu entfernen, klicken Sie auf das Symbol oder auf einen anderen Knoten in einem anderen Angriffspfad.

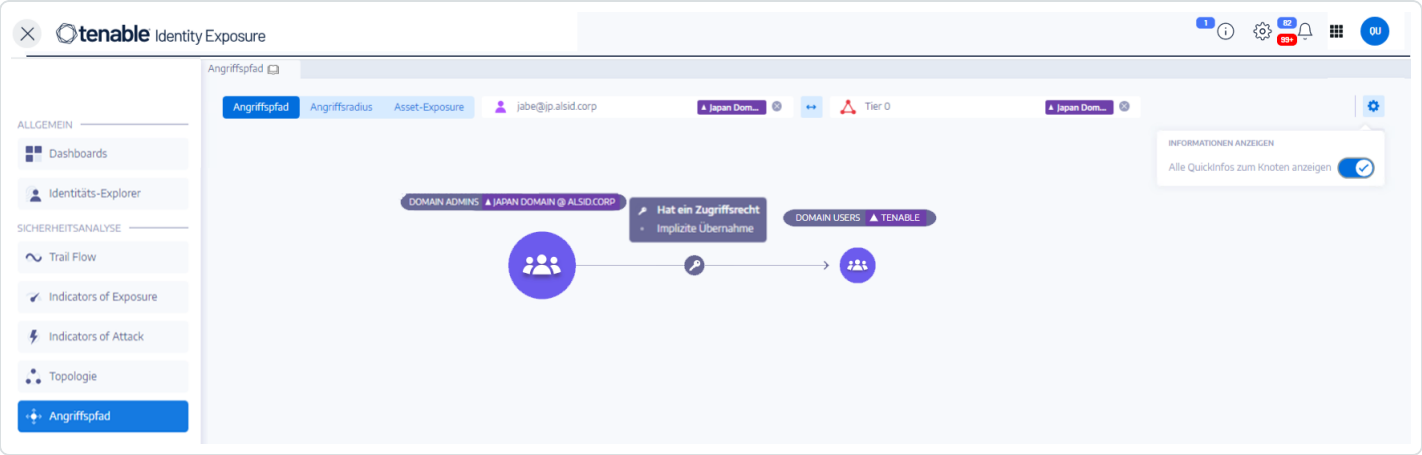


Siehe auch

- Angriffsbeziehungen

Angriffsbeziehungen

Angriffsbeziehungen sind unidirektional von einem Quellknoten zu einem Zielknoten. Da Beziehungen transitiv sind, können Angreifer sie miteinander verketten, um einen „Angriffspfad" zu erstellen:



Tenable Identity Exposure hat die folgenden Angriffsbeziehungen:

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von

- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Schlüssel-Anmeldeinformation hinzufügen

Beschreibung

Der Sicherheitsprinzipal der Quelle kann sich als das Ziel ausgeben, indem er Zuordnungen von Vertrauensstellungen ausnutzt, die auch als Schlüssel-Anmeldeinformationen oder „Schatten-Anmeldeinformationen" bezeichnet werden.

Dies ist möglich, weil die Quelle die Berechtigung hat, das Attribut `msDS-KeyCredentialLink` des Ziels zu bearbeiten.

Windows Hello for Business (WHfB) verwendet diese Funktion normalerweise, aber Angreifer können sie auch dann ausnutzen, wenn sie nicht in Gebrauch ist.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, müssen das Attribut `msDS-KeyCredentialLink` des Zielcomputers mithilfe spezieller Hacker-Tools wie Whisker oder DSInternals bearbeiten.

Das Ziel der Angreifer ist es, dem Attribut dieses Ziels ein neues Zertifikat hinzuzufügen, für das sie den privaten Schlüssel besitzen. Sie können sich dann mit dem bekannten privaten Schlüssel über das Kerberos PKINIT-Protokoll als Ziel authentifizieren, um ein TGT zu erhalten. Dieses Protokoll ermöglicht es Angreifern auch, den NTLM-Hash des Ziels abzurufen.

Behebung

Mehrere Sicherheitsprinzipale mit nativen Rechten verfügen standardmäßig über diese Berechtigung, nämlich Kontooperatoren, Administratoren, Domänenadministratoren, Unternehmensadministratoren, Unternehmensschlüssel-Administratoren und SYSTEM. Für diese legitimen Sicherheitsprinzipale sind keine Behebungsmaßnahmen erforderlich.

Für Sicherheitsprinzipale der Quelle, die dieses Attribut nicht ändern müssen, müssen Sie diese Berechtigung entfernen. Suchen Sie nach Berechtigungen wie „Alle Eigenschaften schreiben", „msDS-AllowedToActOnBehalfOfOtherIdentity schreiben", „Vollständige Kontrolle" usw.

Siehe auch

- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig“ gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Mitglied hinzufügen

Beschreibung

Der Sicherheitsprinzipal der Quelle kann sich selbst (Recht für validierte Schreibvorgänge) oder eine beliebige Person (Recht zum Schreiben von Eigenschaften) zu den Mitgliedern der Ziel-Gruppe hinzufügen und die der Gruppe erteilten Zugriffsrechte nutzen.

Ein böswilliger Sicherheitsprinzipal, der diese Operation durchführt, würde eine „Mitglied von"-Angriffsbeziehung erstellen.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, müssen nur das Attribut „members" der Ziel-Gruppe über native Windows-Befehle wie „net group/domain", PowerShell wie „Add-ADGroupMember", Verwaltungstools wie „Active Directory-Benutzer und -Computer" oder spezielle Hacker-Tools wie PowerSploit bearbeiten.

Behebung

Wenn der Sicherheitsprinzipal der Quelle das Recht, ein Mitglied zur Ziel-Gruppe hinzuzufügen, nicht benötigt, müssen Sie dieses Recht entfernen.

So ändern Sie die Sicherheitsbeschreibung der Ziel-Gruppe:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf **Eigenschaften** > **Sicherheit**.
2. Entfernen Sie Berechtigungen wie „Mitglieder schreiben", „Alle Eigenschaften schreiben", „Vollständige Kontrolle", „Alle validierten Schreibvorgänge", „Sich selbst als Mitglied hinzufügen/entfernen" usw.

> **Hinweis**: Eine Gruppe kann die Berechtigung von einem höheren Objekt in der Active Directory-Struktur erben.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Agieren zulässig

Beschreibung

Der Sicherheitsprinzipal der Quelle darf die ressourcenbasierte eingeschränkte Delegierung in Kerberos (Kerberos Resource-Based Constrained Delegation, KRBCD) auf dem Zielcomputer durchführen. Das bedeutet, dass er sich bei der Kerberos-Authentifizierung gegenüber jedem auf dem Zielcomputer laufenden Dienst als ein beliebiger Benutzer ausgeben kann.

Daher führt er oft zu einer vollständigen Kompromittierung des Zielcomputers.

Dieser Angriff ist auch bekannt als ressourcenbasierte eingeschränkte Delegierung (Resource-Based Constrained Delegation, RBCD), ressourcenbasierte eingeschränkte Delegierung in Kerberos (Kerberos Resource-Based Constrained Delegation, KRBCD), ressourcenbasierte von Kerberos eingeschränkte Delegierung (Resource-Based Kerberos Constrained Delegation, RBKCD) und „Handlung im Namen einer anderen Identität zugelassen".

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können spezielle Hacker-Tools wie Rubeus verwenden, um legitime Kerberos-Protokollerweiterungen (S4U2self und S4U2proxy) auszunutzen, um Kerberos-Service-Tickets zu fälschen und sich als der gewünschte Benutzer auszugeben. Angreifer werden sich wahrscheinlich als privilegierte Benutzer ausgeben, um privilegierten Zugriff zu erhalten.

Sobald Angreifer das Service-Ticket gefälscht haben, können sie ein beliebiges natives Verwaltungstool oder ein spezialisiertes Hacker-Tool verwenden, das mit Kerberos kompatibel ist, um remote beliebige Befehle auszuführen.

Ein erfolgreicher Ausnutzungsversuch muss die folgenden Bedingungen erfüllen:

- Die Sicherheitsprinzipale von Quelle und Ziel müssen einen ServicePrincipalName haben. Tenable Identity Exposure erstellt diese Angriffsbeziehung nicht ohne diese Bedingung.
- Das für das Spoofing anvisierte Konto darf weder als „sensibel und nicht delegierbar" (`ADS_UF_NOT_DELEGATED` in UserAccountControl) markiert sein noch zur Gruppe „Geschützte Benutzer" gehören, da Active Directory solche Konten vor Delegierungsangriffen schützt.

Behebung

Wenn der Sicherheitsprinzipal der Quelle keine Berechtigung zur Durchführung der ressourcenbasierten eingeschränkten Delegierung durch Kerberos (RBCD) auf dem Zielcomputer benötigt, müssen Sie ihn entfernen. Sie müssen die Änderung auf der Zielseite vornehmen, im Gegensatz zur Angriffsbeziehung der Delegierung „Delegieren zugelassen".

Sie können RBCD nicht mit vorhandenen grafischen Verwaltungswerkzeugen wie „Active Directory-Benutzer und -Computer" verwalten. Sie müssen stattdessen PowerShell verwenden, um den Inhalt des Attributs `msDS-AllowedToActOnBehalfOfOtherIdentity` zu ändern.

Listen Sie Sicherheitsprinzipale der Quelle, die in Bezug auf das Ziel handeln dürfen, anhand der folgenden Befehle auf (im Abschnitt „Zugriff:"):

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

Wenn Sie keinen der aufgeführten Sicherheitsprinzipale wünschen, können Sie mit diesem Befehl alle löschen:

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

Wenn Sie nur einen Sicherheitsprinzipal aus der Liste entfernen müssen, stellt Microsoft leider keinen direkten Befehl zur Verfügung. Sie müssen das Attribut mit der gleichen Liste abzüglich des zu entfernenden Attributs überschreiben. Wenn zum Beispiel „sourceA", „sourceB" und „sourceC" alle zugelassen waren und Sie nur „sourceB" entfernen wollen, führen Sie folgenden Befehl aus:

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

Um die Anfälligkeit sensibler privilegierter Konten für derartige Delegierungsangriffe zu begrenzen, empfiehlt Tenable Identity Exposure, sie als „sensibel und nicht delegierbar" (`ADS_UF_NOT_DELEGATED`) zu kennzeichnen oder sie nach sorgfältiger Prüfung der damit verbundenen betrieblichen Auswirkungen zur Gruppe „Geschützte Benutzer" hinzuzufügen.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen

- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Delegieren zulässig

Beschreibung

Der Sicherheitsprinzipal der Quelle darf die eingeschränkte Kerberos-Delegierung (Kerberos Constrained Delegation, KCD) auf dem Zielcomputer durchführen. Das bedeutet, dass er sich bei der Kerberos-Authentifizierung gegenüber jedem auf dem Zielcomputer laufenden Dienst als ein beliebiger Benutzer ausgeben kann.

Daher führt er oft zu einer vollständigen Kompromittierung des Zielcomputers.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können spezielle Hacker-Tools wie Rubeus verwenden, um legitime Kerberos-Protokollerweiterungen (S4U2self und S4U2proxy) auszunutzen, um Kerberos-Service-Tickets zu fälschen und sich als der gewünschte Benutzer auszugeben. Angreifer geben sich wahrscheinlich als privilegierte Benutzer aus, um privilegierten Zugriff zu erhalten.

Sobald Angreifer das Service-Ticket gefälscht haben, können sie ein beliebiges natives Verwaltungstool oder ein spezialisiertes Hacker-Tool verwenden, das mit Kerberos kompatibel ist, um remote beliebige Befehle auszuführen.

Ein erfolgreicher Ausnutzungsversuch muss die folgenden Bedingungen erfüllen:

- Der Sicherheitsprinzipal der Quelle muss für den Protokollübergang aktiviert sein (`ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION` in UserAccountControl / „Beliebiges Authentifizierungsprotokoll verwenden" in der GUI für die Delegierung). Genauer gesagt könnte der Angriff ohne Protokollübergang funktionieren („Nur Kerberos verwenden" in der GUI für die Delegierung), aber die Angreifer müssen zunächst eine Kerberos-Authentifizierung des Zielbenutzers gegenüber dem Sicherheitsprinzipal der Quelle erzwingen, was den Angriff erschwert. Daher stellt Tenable Identity Exposure in diesem Fall keine Angriffsbeziehung her.
- Die Sicherheitsprinzipale von Quelle und Ziel müssen einen ServicePrincipalName haben. Tenable Identity Exposure erstellt diese Angriffsbeziehung nicht ohne diese Bedingung.
- Das für das Spoofing anvisierte Konto darf weder als „sensibel und nicht delegierbar" (`ADS_UF_`

NOT_DELEGATED in UserAccountControl) markiert sein noch zur Gruppe „Geschützte Benutzer" gehören, da Active Directory solche Konten vor Delegierungsangriffen schützt.

Im Gegensatz dazu wird der Zielcomputer, auf dem die Delegierung zulässig ist, durch einen Serviceprinzipalnamen (SPN) bezeichnet und enthält somit einen bestimmten Dienst, z. B. SMB mit „cifs/host.example.net", HTTP mit „http/host.example.net" usw. Angreifer können jedoch mit einem „Sname-Ersetzungsangriff" auf jeden anderen SPN und Dienst abzielen, der unter demselben Zielkonto läuft. Es handelt sich also nicht um eine Einschränkung.

Behebung

Wenn der Sicherheitsprinzipal der Quelle keine Berechtigung zur Durchführung der eingeschränkten Kerberos-Delegierung (Kerberos Constrained Delegation, KCD) auf dem Zielcomputer benötigt, müssen Sie ihn entfernen. Sie müssen die Änderung auf der Quellseite vornehmen, im Gegensatz zur Angriffsbeziehung der Delegierung „Handlung zugelassen".

So entfernen Sie den Sicherheitsprinzipal der Quelle:

1. Wechseln Sie in der Verwaltungs-GUI von „Active Directory-Benutzer und -Computer" zu den **Eigenschaften** des Quellobjekts > Registerkarte **Delegierung**.
2. Entfernen Sie den dem Ziel entsprechenden Serviceprinzipalnamen.
3. Wenn Sie keine Delegierung von dieser Quelle wünschen, entfernen Sie alle SPNs und wählen Sie „Diesem Computer für die Delegierung nicht vertrauen".

Alternativ können Sie PowerShell verwenden, um den Inhalt des Attributs „msDS-AllowedToDelegateTo" der Quelle zu ändern.

- Führen Sie zum Beispiel in Powershell diesen Befehl aus, um alle Werte zu ersetzen:

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

- Wenn Sie keine Delegierung von dieser Quelle wünschen, führen Sie den folgenden Befehl aus, um das Attribut zu löschen:

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

Es ist auch möglich, das Risiko zu verringern, ohne diesen Angriffspfad vollständig zu schließen, indem der Protokollübergang deaktiviert wird. Dazu müssen alle Sicherheitsprinzipale eine Verbindung zur Quelle nur über Kerberos anstelle von NTLM herstellen.

So deaktivieren Sie den Protokollübergang:

1. Wechseln Sie in der Verwaltungs-GUI von „Active Directory-Benutzer und -Computer" zu den **Eigenschaften** des Quellobjekts > Registerkarte **Delegierung**.
2. Wählen Sie „Nur Kerberos verwenden" anstelle von „Beliebiges Authentifizierungsprotokoll verwenden".

Alternativ können Sie auch den folgenden Befehl in PowerShell ausführen, um den Protokollübergang zu deaktivieren:

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

Um die Anfälligkeit sensibler privilegierter Konten für derartige Delegierungsangriffe zu begrenzen, empfiehlt Tenable Identity Exposure, sie als „sensibel und nicht delegierbar" (`ADS_UF_NOT_DELEGATED`) zu kennzeichnen oder sie nach sorgfältiger Prüfung der damit verbundenen betrieblichen Auswirkungen zur Gruppe „Geschützte Benutzer" hinzuzufügen.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben

- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Gehört zu GPO

Beschreibung

Die Quell-GPO-Datei bzw. der Quell-GPO-Ordner in der SYSVOL-Freigabe gehört zum Ziel-GPC (GPO), d. h., sie definiert die Einstellungen oder Programme/Skripts, die das GPO anwendet.

Ausnutzung

Es handelt sich nicht um eine Angriffsbeziehung, die ein Angreifer isoliert verwenden würde. Er kann jedoch beispielsweise komplette Angriffspfade aufzeigen, bei denen Angreifer, die die Kontrolle über eine GPO-Datei/einen GPO-Ordner haben, beliebige Einstellungen erzwingen oder Skripts auf den Benutzern/Computern am Ende des Angriffspfades starten können.

Behebung

Diese Beziehung zeigt, wie die in SYSVOL gefundenen GPO-Dateien und -Ordner mit dem entsprechenden GPC (GPO)-Objekt zusammenhängen. Das ist normal und so gewollt.

Eine Behebung ist daher nicht erforderlich.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben

- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

DCSync

Beschreibung

DCSync ist eine legitime Active Directory-Funktion, die von Domänencontrollern nur für die Replikation von Änderungen verwendet wird, die aber auch von illegitimen Sicherheitsprinzipalen genutzt werden kann.

Der Sicherheitsprinzipal der Quelle kann mithilfe der DCSync-Funktion sensible Geheimnisse (Passwort-Hashes, Kerberos-Schlüssel usw.) von der Zieldomäne anfordern, was letztlich zu einer vollständigen Kompromittierung der Domäne führt.

Um Geheimnisse abzurufen, sind zwei Sicherheitsberechtigungen erforderlich: „Verzeichnisänderungen replizieren" (DS-`Replication-Get-Changes`) und „Alle Verzeichnisänderungen replizieren" (DS-`Replication-Get-Changes-All`). Die Beziehung kommt nur zustande, wenn Sie der Quelle beide Berechtigungen entweder direkt oder durch verschachtelte Gruppenmitgliedschaft erteilen.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können mit speziellen Hacker-Tools wie *mimikatz* oder *impacket* Geheimnisse abrufen.

- **Golden Ticket**: Ergibt sich aus der Beschaffung des Passwort-Hashs des „krbtgt"-Kontos, der es ermöglicht, eine Kerberos-TGT zu fälschen und sich als eine beliebige Person auf einem beliebigen Computer/Dienst auszugeben. Insbesondere werden dadurch Administratorrechte auf jedem Computer in der Domäne gewährt.
- **Silver Ticket**: Ergibt sich aus der Beschaffung des Passwort-Hashs eines Computer/Dienst-Kontos, der es ermöglicht, ein Kerberos-Dienstticket zu fälschen und sich als eine beliebige Person auf dem angegebenen Computer/Dienst auszugeben.

Behebung

Legitime Sicherheitsprinzipale, die standardmäßig zur Nutzung von DCSync zugelassen sind:

- Administratoren
- Domänenadministratoren

- Unternehmensadministratoren
- SYSTEM

Darüber hinaus lässt die Microsoft Entra ID Connect-Konfiguration zu, dass das Dienstkonto DCSync für die Passwort-Hash-Synchronisierung (MSOL_...) nutzen kann.

Zudem ist es möglich, Dienstkonten für bestimmte Sicherheitstools zu ermitteln, vor allem für Lösungen zur Passwortprüfung. Vergewissern Sie sich bei den Verantwortlichen, dass sie legitim sind.

Für Sicherheitsprinzipale der Quelle, die DCSync nicht ausführen müssen, müssen Sie diese Berechtigung entfernen.

So ändern Sie die Sicherheitsbeschreibung der Zieldomäne:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf den Domänennamen und wählen Sie „Eigenschaften" > „Sicherheit".
2. Entfernen Sie die Berechtigungen „Verzeichnisänderungen replizieren" und „Alle Verzeichnisänderungen replizieren" für unzulässige Sicherheitsprinzipale.

> **Hinweis**: DCSync-Beziehungen können durch Berechtigungen aus verschachtelten Gruppenmitgliedschaften entstehen. Je nach Situation müssen Sie also die Gruppen selbst oder nur einige ihrer Mitglieder entfernen.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme

- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

„Agieren zulässig" gewähren

Beschreibung

Der Sicherheitsprinzipal der Quelle darf sich selbst oder einer anderen Person eine Agieren zulässig-Beziehung zum Zielcomputer einräumen. Dies führt häufig zu einer vollständigen Kompromittierung des Zielcomputers über einen Angriff mit Kerberos RBCD-Delegierung.

Dies ist möglich, weil die Quelle die Berechtigung hat, das Attribut „msDS-AllowedToActOnBehalfOfOtherIdentity" des Ziels zu bearbeiten.

Ein böswilliger Sicherheitsprinzipal, der diese Operation durchführt, kann eine „Agieren zulässig"-Angriffsbeziehung erstellen.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, müssen das Attribut `msDS-AllowedToActOnBehalfOfOtherIdentity` des Zielcomputers mit PowerShell bearbeiten (zum Beispiel „Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount ...").

Behebung

Mehrere Sicherheitsprinzipale mit nativen Rechten verfügen standardmäßig über diese Berechtigung, nämlich Kontooperatoren, Administratoren, Domänenadministratoren, Unternehmensadministratoren und SYSTEM. Diese Sicherheitsprinzipale sind legitim und es sind für sie keine Behebungsmaßnahmen erforderlich.

Kerberos RBCD ist so konzipiert, dass die Administratoren eines Computers die Rechte zur Delegierung auf dem Computer an jeden vergeben können, der sie benötigt. Dies unterscheidet sich von anderen Modi der Kerberos-Delegierung, die eine Berechtigung auf Domänenadministrator-Ebene erfordern. Dadurch können Administratoren der unteren Ebenen diese Sicherheitseinstellungen selbst verwalten, ein Prinzip, das auch als Delegierung bezeichnet wird. In diesem Fall ist die Beziehung legitim.

Wenn der Sicherheitsprinzipal der Quelle jedoch kein legitimer Administrator des Zielcomputers ist, ist die Beziehung nicht legitim und Sie müssen diese Berechtigung entfernen.

So ändern Sie die Sicherheitsbeschreibung des Ziel-Computers:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf **Eigenschaften** > **Sicherheit**.
2. Entfernen Sie die Berechtigung für den Sicherheitsprinzipal der Quelle. Suchen Sie nach Berechtigungen wie „msDS-AllowedToActOnBehalfOfOtherIdentity schreiben", „Alle Eigenschaften schreiben", „Kontobeschränkungen schreiben", „Vollzugriff" usw.

Hinweis: Der Sicherheitsprinzipal der Quelle kann die Berechtigung von einem Objekt erben, das in der Active Directory-Baumstruktur höher angesiedelt ist.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Hat SID-Verlauf

Beschreibung

Der Sicherheitsprinzipal der Quelle hat die SID des Sicherheitsprinzipals des Ziels in seinem SIDHistory-Attribut, was bedeutet, dass die Quelle die gleichen Rechte wie das Ziel hat.

Der Verlauf der SID ist ein legitimer Mechanismus, der bei der Migration von Sicherheitsprinzipalen zwischen Domänen verwendet wird, um alle Berechtigungen, die sich auf ihre vorherige SID beziehen, funktionsfähig zu halten.

Dies ist jedoch auch ein Persistenzmechanismus, den Angreifer nutzen, da er es einem diskreten Backdoor-Konto ermöglicht, die gleichen Rechte wie das gewünschte Ziel zu haben, wie zum Beispiel ein Administratorkonto.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können sich direkt als Sicherheitsprinzipal des Ziels authentifizieren, da die SID des Ziels transparent in das Token eingefügt wird, das die Authentifizierungsmechanismen von Active Directory (NTLM und Kerberos) erzeugen.

Behebung

Wenn die Sicherheitsprinzipale von Quelle und Ziel mit einer genehmigten Domänenmigration verbunden sind, können Sie die Beziehung als legitim betrachten und müssen keine Maßnahmen ergreifen. Diese Beziehung bleibt als Erinnerung an einen möglichen Angriffspfad sichtbar.

Wenn die Ursprungsdomäne nach der Migration gelöscht wurde oder nicht in Tenable Identity Exposure konfiguriert ist, wird der Sicherheitsprinzipal des Ziels als nicht aufgelöst markiert. Da das Risiko beim Ziel liegt und dieses Ziel nicht existiert, gibt es kein Risiko und somit ist auch keine Behebung erforderlich.

Im Gegenteil, SID-Verläufe, die sich auf Benutzer oder Gruppen mit nativen Rechten beziehen, sind sehr wahrscheinlich bösartig, da Active Directory ihre Erstellung verhindert. Dies bedeutet, dass sie wahrscheinlich mit Hilfe von Hackertechniken wie einem „DCShadow"-Angriff erstellt wurden. Sie finden diese Fälle auch im IoE unter „SID-Verlauf".

Ist dies der Fall, empfiehlt Tenable Identity Exposure eine forensische Untersuchung der Active Directory-Gesamtstruktur. Der Grund dafür ist, dass Angreifer hohe Rechte (Domänenadministrator oder gleichwertig) erlangt haben müssen, um den SID-Verlauf der Quelle böswillig zu bearbeiten. Die forensische Untersuchung hilft Ihnen bei der Analyse des Angriffs mit entsprechenden Anleitungen zur Behebung und identifiziert potenzielle Hintertüren, die entfernt werden müssen.

Schließlich empfiehlt Microsoft, alle Zugriffsrechte in allen Diensten (SMB-Freigaben, Exchange usw.) zu ändern, um die neuen SIDs zu verwenden, und unnötige SIDHistory-Werte zu entfernen, nachdem die Migration abgeschlossen ist. Dies ist eine bewährte Praxis, auch wenn es sehr schwierig ist, alle ACLs vollständig zu identifizieren und zu korrigieren.

Ein Benutzer, der das Recht hat, das SIDHistory-Attribut auf dem Quellobjekt selbst zu bearbeiten, kann SIDHistory-Werte entfernen. Anders als bei der Erstellung sind für diesen Vorgang keine Domänenadministratorrechte erforderlich.

Hierfür können Sie nur PowerShell verwenden, da grafische Tools wie „Active Directory-Benutzer und -Computer" nicht funktionieren. Beispiel:

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

Achtung: Ein SIDHistory-Wert lässt sich zwar leicht entfernen, doch es ist sehr kompliziert, diesen Vorgang rückgängig zu machen. Dies liegt daran, dass Sie den SIDHistory-Wert neu erstellen müssen, wofür das Vorhandensein der anderen Domäne erforderlich ist, die möglicherweise außer Betrieb genommen wurde. Aus diesem Grund empfiehlt Microsoft auch, dass Sie Snapshots oder Sicherungskopien erstellen.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync

- „Agieren zulässig" gewähren
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Implizite Übernahme

Beschreibung

Die Quelle ist ein Tier0-Sicherheitsprinzipal. Tier0 ist die Gruppe der Active Directory-Objekte, die die höchsten Berechtigungen in der Domäne haben, wie z. B. die Mitglieder der Gruppe der Domänenadministratoren oder Domänencontroller. Alle Tier0-Assets können implizit jedes andere Objekt in der Domäne kompromittieren, auch wenn es keine explizite andere Beziehung gibt.

Diese Beziehung ermöglicht die Modellierung impliziter, in Active Directory integrierter Rechte. Diese Rechte sind von vornherein festgelegt und dokumentiert und somit Angreifern bekannt. Tenable Identity Exposure kann diese Rechte jedoch nicht mit den üblichen Mitteln einfordern. Außerdem vereinfacht diese Beziehung die Angriffspfad-Diagramme, denn sobald Angreifer einen Tier0-Knoten kompromittieren, können sie jedes andere Objekt direkt angreifen, ohne andere explizite Beziehungen zu durchlaufen.

Zusammenfassend wird davon ausgegangen, dass alle Tier0-Assets der Quelle „Implizite Übernahme"-Beziehungen zu jedem Zielknoten im Diagramm haben.

Ausnutzung

Die genaue Ausnutzungsmethode hängt von der Art des anvisierten Tier0-Assets der Quelle ab, aber es handelt sich um gut dokumentierte Techniken, die Angreifer effizient beherrschen.

Behebung

Diese Beziehung ist gewollt und kann nicht behoben werden. Es ist fast unmöglich, einen Angreifer, der ein Tier0-Asset erreicht hat, an weiteren Angriffen zu hindern.

Die Behebung der Probleme muss sich auf die vorgelagerten Beziehungen in den Angriffspfaden konzentrieren.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen

- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig“ gewähren
- Hat SID-Verlauf
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

GPO erben

Beschreibung

Ein mit der Quelle verknüpfbarer Container wie eine Organisationseinheit (OU) oder eine Domäne (nicht aber Sites) enthält die OE, den Benutzer, das Gerät, den DC oder den schreibgeschützten Domänencontroller (Read-Only Domain Controller, RODC) des Ziels in der LDAP-Struktur. Dies liegt daran, dass die untergeordneten Objekte des verknüpfbaren Containers das GPO erben, mit dem er verknüpft ist (siehe „Verknüpfte GPO"-Beziehungen).

Tenable Identity Exposure berücksichtigt es, wenn eine OE die Vererbung blockiert.

Ausnutzung

Angreifer müssen nichts tun, um diese Beziehung auszunutzen, solange es ihnen gelingt, das GPO auf dem Angriffspfad zu kompromittieren. Die Beziehung gilt für verknüpfbare Container und darunter liegende Objekte, wie die „GPO erben"-Beziehungen zeigen.

Behebung

In den meisten Fällen ist es normal und legitim, dass GPOs auf verknüpfbare untergeordnete Container von ihren übergeordneten Containern angewendet werden. Diese Verknüpfung macht jedoch den Weg für zusätzliche Angriffspfade frei.

Um die Risiken zu verringern, sollten Sie daher GPOs nach Möglichkeit mit der untersten Ebene in der Hierarchie der Organisationseinheiten verknüpfen.

Außerdem müssen GPOs vor unbefugten Änderungen durch Angreifer geschützt werden, um sie nicht anderen Angriffsbeziehungen auszusetzen.

Schließlich können OEs die Vererbung von GPOs von höheren Ebenen durch ihre Option „Vererbung blockieren" deaktivieren. Verwenden Sie diese Option jedoch nur als letzten Ausweg, da sie alle GPOs blockiert, einschließlich der potenziellen Absicherungs-GPOs, die auf der höchsten Domänenebene definiert sind. Dies erschwert auch die Überlegungen zu den angewendeten GPOs.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Verknüpftes GPO

Beschreibung

Das Quell-GPO wird mit dem verknüpfbaren Ziel-Container verknüpft, z. B. einer Domäne oder einer Organisationseinheit (OU). Dies bedeutet, dass das Quell-GPO Einstellungen zuweisen und Programme auf den im Ziel enthaltenen Geräten und Benutzern ausführen kann. Das Quell-GPO gilt auch für Objekte in den darunter liegenden Containern durch „GPO erben"-Beziehungen.

Letztendlich kann das GPO die Geräte und Benutzer gefährden, auf die es angewendet wird.

Ausnutzung

Angreifer müssen zunächst das Quell-GPO durch eine andere Angriffsbeziehung kompromittieren.

Dann setzen sie verschiedene Techniken ein, um böswillige Aktionen auf Geräten und Benutzern innerhalb und unterhalb des Ziels durchzuführen. Beispiele:

- Missbrauch der legitimen „unmittelbar geplanten Aufgaben" zur Ausführung beliebiger Skripts auf Geräten
- Hinzufügen eines neuen lokalen Benutzers mit Verwaltungsrechten auf allen Geräten
- Installieren eines MSI-Programms
- Deaktivieren der Firewall oder des Virenschutzes
- Erteilung weiterer Rechte
- usw.

Angreifer können ein GPO ändern, indem sie dessen Inhalt manuell mit Verwaltungstools wie „Gruppenrichtlinienverwaltung" oder speziellen Hacker-Tools wie PowerSploit bearbeiten.

Behebung

In den meisten Fällen ist es normal und legitim, ein GPO mit einem verknüpfbaren Container zu verknüpfen. Diese Verknüpfung vergrößert jedoch die Angriffsfläche dort, wo sie auftritt, sowie in den darunter liegenden Containern.

Um die Risiken zu verringern, sollten Sie daher GPOs nach Möglichkeit mit der untersten Ebene in der Hierarchie der Organisationseinheiten verknüpfen.

Außerdem müssen GPOs vor unbefugten Änderungen durch Angreifer geschützt werden, um sie nicht anderen Angriffsbeziehungen auszusetzen.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Mitglied von

Beschreibung

Der Sicherheitsprinzipal der Quelle ist ein Mitglied der Ziel-Gruppe. Daher profitiert er von allen Zugriffsrechten, die die Gruppe besitzt, wie z. B. Zugriff auf Dateifreigaben, Übernahme von Rollen in Geschäftsanwendungen usw.

Ausnutzung

Angreifer müssen nichts tun, um diese Angriffsbeziehung auszunutzen. Sie müssen sich nur als Sicherheitsprinzipal der Quelle authentifizieren, um die Ziel-Gruppe in ihrem lokalen oder Remote-Sicherheitstoken bzw. Kerberos-Ticket zu erhalten.

Behebung

Wenn der Sicherheitsprinzipal der Quelle ein nicht legitimes Mitglied der Ziel-Gruppe ist, müssen Sie ihn entfernen.

Sie können jedes standardmäßige Active Directory-Verwaltungstool wie „Active Directory-Benutzer und -Computer" oder PowerShell wie Remove-ADGroupMember verwenden.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme

- GPO erben
- Verknüpftes GPO
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Besitzt

Beschreibung

Der Sicherheitsprinzipal der Quelle ist der erklärte Besitzer des Ziel-Objekts, da er wahrscheinlich das Ziel-Objekt erstellt hat. Die Besitzer haben implizite Rechte („Lesekontrolle" und „DACL schreiben"), die es ihnen ermöglichen, zusätzliche Rechte für sich selbst oder eine andere Person zu erhalten und letztendlich das Ziel-Objekt zu kompromittieren.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, müssen nur die Sicherheitsbeschreibung des Ziel-Objekts über native Windows-Befehle wie „dsacls", PowerShell wie „Set-ACL", Verwaltungstools wie „Active Directory-Benutzer und -Computer" oder spezielle Hacker-Tools wie PowerSploit bearbeiten.

Wenn ein Objekt erstellt wird, besteht das Risiko einer Rechteausweitung, wenn ein Benutzer mit geringen Privilegien es erstellt und somit besitzt (z. B. ein Standard-Helpdesk-Techniker) und dieses Objekt später mit höheren Rechten ausgestattet wird (z. B. Administrator). Der ursprüngliche Besitzer bleibt bestehen und kann das nun privilegierte Objekt kompromittieren, um dessen Rechte zu nutzen.

Behebung

Wenn der Sicherheitsprinzipal der Quelle kein legitimer Besitzer des Ziel-Objekts ist, müssen Sie ihn ändern.

So ändern Sie den Besitzer des Ziel-Objekts:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf **Eigenschaften** > **Sicherheit** > **Erweitert**.
2. Klicken Sie oben in der Zeile **Besitzer** auf **Ändern**.

Sichere Besitzer der Ziel-Objekte, die standardmäßig für die meisten sensiblen Active Directory-Objekte verwendet werden, sind:

- Objekte in der Domänenpartition: „Administratoren" oder „Domänenadministratoren"
- Objekte in der Konfigurationspartition: „Unternehmensadministratoren"
- Objekte in der Schema-Partition: „Schemaadministratoren"

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

Passwort zurücksetzen

Beschreibung

Der Sicherheitsprinzipal der Quelle kann das Passwort des Ziels zurücksetzen, wodurch er sich mit dem neuen zugewiesenen Passwort als Ziel authentifizieren und von den Rechten des Ziels profitieren kann.

Ein Passwort zurückzusetzen ist nicht dasselbe wie das Ändern eines Passworts, was jeder tun kann, der das aktuelle Passwort kennt. Eine Passwortänderung erfolgt in der Regel, wenn ein Passwort abläuft.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können das Passwort des Ziels mit nativen Windows-Befehlen wie „net user /domain", PowerShell wie „Set-ADAccountPassword -Reset", Verwaltungstools wie „Active Directory-Benutzer und -Computer" oder speziellen Hacker-Tools wie PowerSploit zurücksetzen.

Angreifer müssen sich dann nur noch beim Active Directory oder der Zielressource mit legitimen Authentifizierungsmethoden und dem neu gewählten Passwort authentifizieren, um sich vollständig als das Ziel auszugeben.

Allerdings kennen Angreifer in der Regel nicht das vorherige Passwort, um dieses nach dem Angriff wieder anwenden zu können. Daher ist der Angriff oft für die legitime Person hinter dem Ziel sichtbar und kann sogar ein Denial of Service verursachen, insbesondere für Dienstkonten.

Behebung

IT-Administratoren und Helpdesk-Mitarbeiter sind legitimerweise berechtigt, Passwörter zurückzusetzen. Sie müssen jedoch die entsprechenden Delegierungen einrichten, damit sie diese Aktion nur innerhalb ihres zulässigen Perimeters durchführen können.

Außerdem müssen Sie gemäß dem Tiering-Modell sicherstellen, dass Mitarbeiter einer niedrigeren Stufe, z. B. ein Helpdesk für normale Benutzer, das Passwort eines Kontos einer höheren Stufe, z. B. eines Domänenadministrators, nicht zurücksetzen können, da dies eine Möglichkeit zur Rechteausweitung darstellt.

So ändern Sie die Sicherheitsbeschreibung des Ziels und entfernen unzulässige Berechtigungen:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf Eigenschaften > Sicherheit.
2. Entfernen Sie die „Passwort zurücksetzen"-Berechtigung für den Sicherheitsprinzipal der Quelle.

   > **Hinweis**: Verwechseln Sie diese Berechtigung nicht mit „Passwort ändern".

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- RODC-Verwaltung
- DACL schreiben
- Besitzer schreiben

RODC-Verwaltung

Beschreibung

Der Sicherheitsprinzipal der Quelle ist im Attribut „ManagedBy“ des RODC (Read-Only Domain Controller) des Ziels zu finden. Dies bedeutet, dass die Quelle über Administratorrechte für den Ziel-RODC verfügt.

> **Hinweis**: Andere Active Directory-Objekttypen verwenden das gleiche Attribut „ManagedBy” nur zu Informationszwecken und erteilen dem angegebenen Manager keine Verwaltungsrechte. Daher besteht diese Beziehung nur für Ziel-Knoten vom Typ RODC.

RODCs sind weniger sensibel als die häufigeren beschreibbaren Domänencontroller, aber sie sind immer noch ein hochwertiges Ziel für Angreifer, da sie Anmeldeinformationen von RODCs stehlen können, um dann auf andere Systeme zuzugreifen. Dies hängt vom Grad der Absicherung in der RODC-Konfiguration ab, wie zum Beispiel von der Anzahl der Objekte mit Geheimnissen, die synchronisiert werden können.

Ausnutzung

Die Methode der Ausnutzung ist die gleiche wie bei der „AdminTo”-Beziehung.

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können dessen Identität nutzen, um eine Remote-Verbindung herzustellen und Befehle auf dem Ziel-RODC mit Administratorrechten auszuführen. Sie können verfügbare native Protokolle wie Server Message Block (SMB) mit administrativen Freigaben, Remote Desktop Protocol (RDP), Windows Management Instrumentation (WMI), Remote Procedure Call (RPC), Windows Remote Management (WinRM) usw. ausnutzen.

Angreifer können native Remoteverwaltungstools wie PsExec, Dienste, geplante Aufgaben, Invoke-Command usw. oder spezialisierte Hacker-Tools wie wmiexec, smbexec, Invoke-DCOM, SharpRDP usw. verwenden.

Das endgültige Ziel des Angriffs kann entweder die Kompromittierung des Ziel-RODCs sein oder die Verwendung von Tools zum Auslesen von Zugangsdaten wie Mimikatz, um weitere Anmeldeinformationen und Geheimnisse zu erhalten, die auf andere Rechner übertragen werden können.

Behebung

Wenn der Sicherheitsprinzipal der Quelle kein legitimer Administrator des RODC (Read-Only Domain Controller) des Ziels ist, müssen Sie ihn durch einen richtigen Administrator ersetzen.

Beachten Sie, dass Domänenadministratoren in der Regel keine RODCs verwalten, daher die spezielle Einstellung „verwaltet von". Dies liegt daran, dass RODCs eine geringere Vertrauensstellung haben und Domänenadministratoren mit hohen Rechten ihre Anmeldeinformationen durch Authentifizierung auf ihnen preisgeben sollten.

Daher müssen Sie gemäß Ihren Active Directory-RODC-Regeln einen geeigneten Administrator der mittleren Ebene für RODCs auswählen, wie zum Beispiel den IT-Administrator der lokalen Niederlassung eines Unternehmens, in der sie sich befinden.

So ändern Sie das Attribut „ManagedBy":

1. Wählen Sie in „Active Directory-Benutzer und -Computer" die Registerkarte RODC > **Eigenschaften** > **ManagedBy**.
2. Klicken Sie auf **Ändern**.

Sie können auch den folgenden Befehl in PowerShell ausführen:

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

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme

- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- DACL schreiben
- Besitzer schreiben

DACL schreiben

Beschreibung

Der Sicherheitsprinzipal der Quelle hat die Genehmigung, die Berechtigungen des Ziel-Objekts in der DACL (Discretionary Access Control List) zu ändern. Dies ermöglicht es der Quelle, für sich selbst zusätzliche Rechte zu erlangen oder an jemand anderen zu übertragen und letztlich das Ziel-Objekt zu kompromittieren.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, müssen nur die Sicherheitsbeschreibung des Ziel-Objekts über native Windows-Befehle wie „dsacls", PowerShell wie „Set-ACL", Verwaltungstools wie „Active Directory-Benutzer und -Computer" oder spezielle Hacker-Tools wie PowerSploit bearbeiten.

Behebung

Wenn der Sicherheitsprinzipal der Quelle nicht die legitime Berechtigung hat, die Berechtigungen des Ziel-Objekts zu ändern, müssen Sie diese Berechtigung entfernen.

So ändern Sie die Sicherheitsbeschreibung des Ziel-Objekts:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf **Eigenschaften** > **Sicherheit** > **Erweitert**.
2. Entfernen Sie die „Berechtigungen ändern"-Berechtigung für den Sicherheitsprinzipal der Quelle.

> **Hinweis**: Ein Objekt kann die Berechtigung von einem höheren Objekt in der Active Directory-Struktur erben.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen

- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig“ gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- Besitzer schreiben

Besitzer schreiben

Beschreibung

Der Sicherheitsprinzipal der Quelle hat die Berechtigung, den Besitzer des Ziel-Objekts zu ändern, einschließlich sich selbst als Besitzer zuzuweisen. Besitzer haben implizite Rechte („Lesekontrolle" und „DACL schreiben"), die es ihnen ermöglichen, zusätzliche Rechte für sich selbst oder eine andere Person zu erhalten und letztendlich das Ziel-Objekt zu kompromittieren.

Weitere Informationen finden Sie unter der Besitzt-Beziehung.

Ausnutzung

Angreifer, die den Sicherheitsprinzipal der Quelle kompromittieren, können sich mit nativen Windows-Befehlen wie „dsacls /takeownership", PowerShell wie „Set-ACL", Verwaltungstools wie „Active Directory-Benutzer und -Computer" oder speziellen Hacker-Tools wie PowerSploit als Besitzer des Ziels zuweisen.

Sie können dann die Sicherheitsbeschreibung des Ziel-Objekts mit ähnlichen Methoden bearbeiten.

Behebung

Wenn der Sicherheitsprinzipal der Quelle keine legitime Berechtigung hat, den Besitzer des Ziel-Objekts zu ändern, müssen Sie diese Berechtigung entfernen.

So ändern Sie die Sicherheitsbeschreibung des Ziel-Objekts:

1. Klicken Sie in „Active Directory-Benutzer und -Computer" mit der rechten Maustaste auf das Objekt und wählen Sie **Eigenschaften** > **Sicherheit** > **Erweitert** aus.
2. Entfernen Sie die „Besitzer ändern"-Berechtigung für den Sicherheitsprinzipal der Quelle.

> **Hinweis**: Ein Objekt kann die Berechtigung von einem höheren Objekt in der Active Directory-Struktur erben.

Siehe auch

- Schlüssel-Anmeldeinformation hinzufügen
- Mitglied hinzufügen
- Agieren zulässig
- Delegieren zulässig
- Gehört zu GPO
- DCSync
- „Agieren zulässig" gewähren
- Hat SID-Verlauf
- Implizite Übernahme
- GPO erben
- Verknüpftes GPO
- Mitglied von
- Besitzt
- Passwort zurücksetzen
- RODC-Verwaltung
- DACL schreiben

Identifizieren von Tier-0-Assets

Tier-0-Assets umfassen Konten, Gruppen und andere Assets, die direkte oder indirekte administrative Kontrolle über die Active Directory-Gesamtstrukturen und -Domänen haben.

Tenable Identity Exposure listet Ihre Tier-0-Assets und -Konten mit potenziellen Angriffspfaden auf, die zu dem jeweiligen Asset führen.

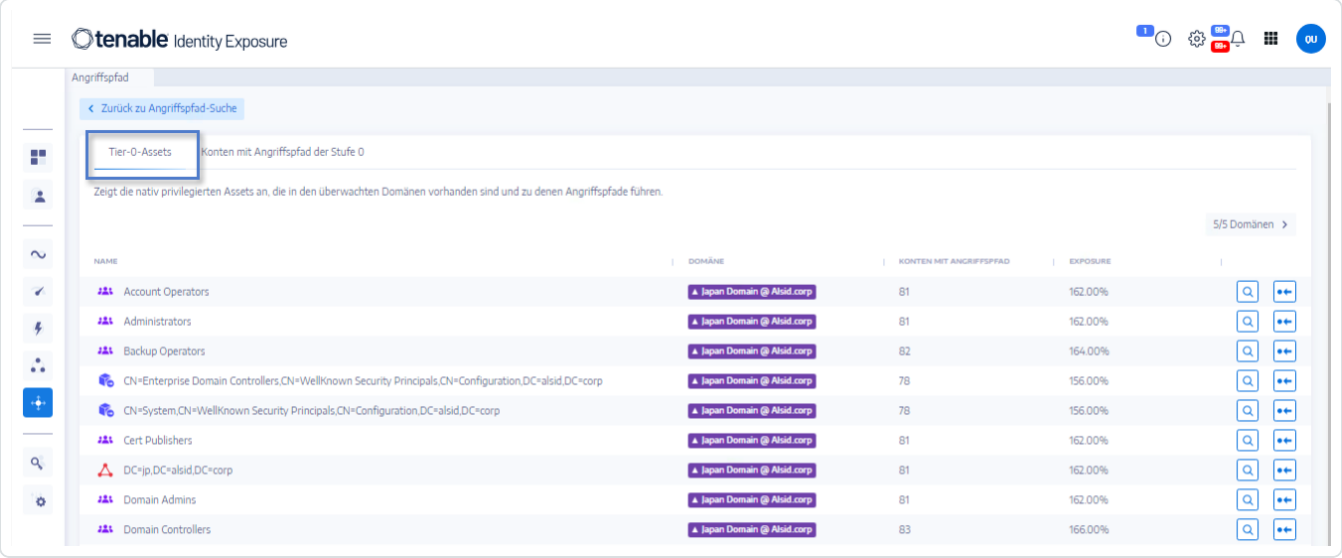
So listen Sie Tier-0-Assets auf:

1. Klicken Sie in Tenable Identity Exposure auf das Angriffspfad-Symbol in der linken Navigationsleiste.

   Der Fensterbereich **Angriffspfad** wird geöffnet.

2. Klicken Sie auf die Kachel **Welche meiner Assets sind privilegiert?**

   Tenable Identity Exposure zeigt eine Liste der Tier-0-Assets in Ihrem AD.



Jede Zeile enthält den **Asset-Namen**, die **Domäne** und die folgenden Informationen:

- **Konten mit Angriffspfad**: Die Anzahl der Assets, die einen Angriffspfad haben, der zum Tier-0-Asset führt.
- **Exposure**: Die Konten mit einem Angriffspfad, der zum Tier-0-Asset führt, ausgedrückt als Prozentsatz der Gesamtzahl der Konten in der Domäne.

So filtern Sie die Assets für eine bestimmte Domäne:

1. Klicken Sie auf die Schaltfläche **n/n**.

   Der Fensterbereich **Gesamtstrukturen und Domänen** wird geöffnet. Sie können einen der folgenden Schritte ausführen:

   - Geben Sie im Feld **Suche** den Namen einer Gesamtstruktur oder Domäne ein.
   - Aktivieren Sie das Kontrollkästchen **Alle erweitern** und wählen Sie die gewünschte Gesamtstruktur oder Domäne aus.

2. Klicken Sie auf **Auswahlbasierter Filter**.

   Tenable Identity Exposure aktualisiert die Liste der Assets.

So listen Sie die Konten mit Angriffspfaden auf, die zum Tier-0-Asset führen:

- Klicken Sie am Ende der Zeile mit dem Namen des Tier-0-Assets auf das Symbol  .

  Tenable Identity Exposure zeigt eine Liste von Konten mit Angriffspfaden, die zum betreffenden Tier-0-Asset führen.

So zeigen Sie die Asset-Exposure des Tier-0-Assets an:

- Klicken Sie am Ende der Zeile mit dem Namen des Tier-0-Assets auf das Symbol  .

  Tenable Identity Exposure öffnet die Seite „Asset-Exposure“ für dieses Tier-0-Asset. Weitere Informationen finden Sie unter Angriffsbeziehungen.

Konten mit Angriffspfaden

Tenable Identity Exposure zeigt Konten mit Angriffspfaden, die zu Tier-0-Assets führen, um Ihnen einen umfassenden Überblick über eine potenzielle Sicherheitsbedrohung zu geben, da Benutzer- und Computerkonten durch verschiedene Angriffsbeziehungen privilegiert werden können.

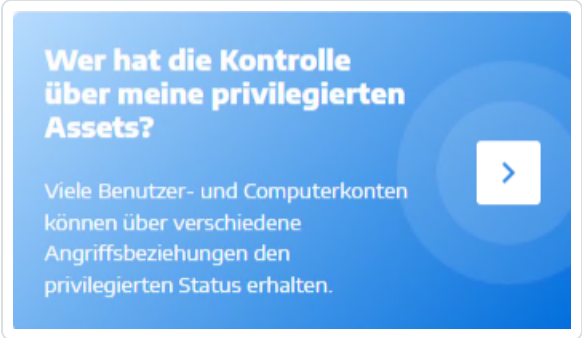
Weitere Informationen finden Sie unter Identifizieren von Tier-0-Assets.

So zeigen Sie Assets mit Angriffspfaden an:

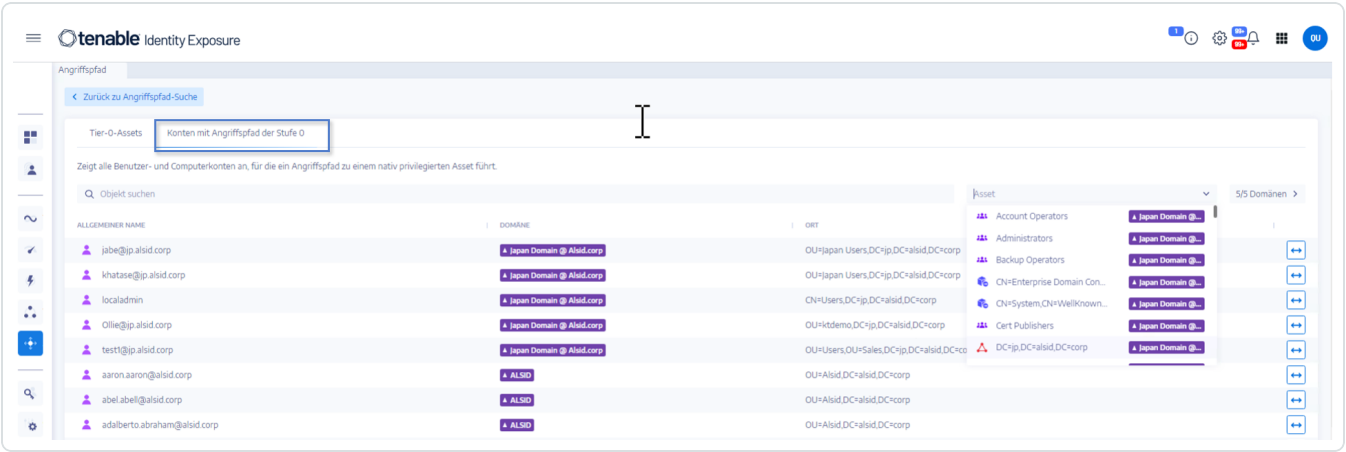
1. Klicken Sie in Tenable Identity Exposure auf das Angriffspfad-Symbol in der linken Navigationsleiste.

   Der Fensterbereich **Angriffspfad** wird geöffnet.

2. Klicken Sie auf die Kachel **Wer hat die Kontrolle über meine privilegierten Assets?**

   Tenable Identity Exposure zeigt alle Benutzer- und Computerkonten mit einem Angriffspfad, der zu einem Tier-0-Asset führt.

So suchen Sie nach einem bestimmten Asset:

1. Geben Sie im Feld **Suche** den Namen des Assets ein.
2. Klicken Sie im Feld **Asset** auf den Pfeil **>**, um eine Dropdown-Liste mit Tier-0-Assets anzuzeigen, und wählen Sie ein Asset aus.

   Tenable Identity Exposure aktualisiert die Liste mit den passenden Ergebnissen.

So filtern Sie die Assets für eine bestimmte Domäne:

1. Klicken Sie auf die Schaltfläche **n/n**.

   Der Fensterbereich **Gesamtstrukturen und Domänen** wird geöffnet. Sie können einen der folgenden Schritte ausführen:

   - Geben Sie im Feld **Suche** den Namen einer Gesamtstruktur oder Domäne ein.
   - Aktivieren Sie das Kontrollkästchen **Alle erweitern** und wählen Sie die gewünschte Gesamtstruktur oder Domäne aus.
2. Klicken Sie auf **Auswahlbasierter Filter**.

   Tenable Identity Exposure aktualisiert die Liste der Assets.

So untersuchen Sie den Angriffspfad:

- Klicken Sie am Ende der Zeile mit dem Asset-Namen auf das Symbol  .

  Tenable Identity Exposure öffnet die Seite „Angriffspfad“ von diesem Asset zu allen Tier-0-Assets. Weitere Informationen finden Sie unter Angriffspfad und Angriffsbeziehungen.

Typen von Angriffspfad-Knoten

Die Angriffspfad-Funktion in Tenable Identity Exposure zeigt Ihnen ein Diagramm, das die Angriffspfade visualisiert, die Angreifern in Ihrer Active Directory-Umgebung offen stehen. Das Diagramm umfasst **Edges**, die Angriffsbeziehungen darstellen, und **Knoten**, die Active Directory-Objekte (LDAP/SYSVOL) darstellen.

In der folgenden Liste werden alle möglichen Knotentypen beschrieben, die in Angriffspfad-Diagrammen enthalten sein können.

Knotentyp	Position	Symbol	Beschreibung
Benutzer	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `user` enthält, aber nicht die Klasse `computer`.
Gruppe	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `group` enthält.
Gerät	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `computer` enthält, aber nicht die Klasse `msDS-GroupManagedServiceAccount`. Das Attribut `primaryGroupID` ist nicht gleich 516 (DC) oder 521 (RODC). **Hinweis**: Zur Unterscheidung von Tenable-Produkten wird diese Kategorie nicht als „Computer", sondern allgemeiner als „Gerät" bezeichnet.
Organisationseinheit (OU)	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `organizationalUnit` enthält. Vermeiden Sie die Verwirrung zwischen Objekten der Klasse `container` und der Tatsache, dass jedes Active Directory (AD)-Objekt als Container dienen und dann andere Objekte enthalten kann.
Domäne	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `domainDNS` und bestimmte Attribute enthält.

Domänencontroller (DC)	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `computer` enthält und dessen `primaryGroupID`-Attribut gleich 516 ist (und daher kein RODC).
Schreibgeschützter Domänencontroller (Read-Only Domain Controller, RODC)	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `computer` enthält und dessen `primaryGroupID`-Attribut gleich 521 ist (und daher kein Standard-DC).
Gruppenrichtlinie (GPC)	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `groupPolicyContainer` enthält.
GPO-Datei	SYSVOL		Datei in der SYSVOL-Freigabe eines bestimmten GPO (z. B. „`\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml`“)
GPO-Ordner	SYSVOL		Ordner in der SYSVOL-Freigabe eines bestimmten GPO. Es gibt einen Ordner für jedes GPO (z. B. „`\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup`“)
Gruppenverwaltetes Dienstkonto (gMSA)	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `msDS-GroupManagedServiceAccount` enthält.
Enterprise NTAuth-Speicher	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `certificationAuthority` enthält.

PKI-Zertifikatvorlage	LDAP		LDAP-Objekt, dessen `objectClass`-Attribut die Klasse `pKICertificateTemplate` enthält.
Nicht aufgelöster Sicherheitsprinzipal	LDAP		LDAP-Objekt, dessen `objectSid`- oder `DistinguishedName`-Attribut irgendwann beim Aufbau von Beziehungen verwendet wird, für das jedoch ein unbekanntes entsprechendes LDAP-Sicherheitsprinzipal-Objekt vorhanden ist (klassischer Fall von „nicht aufgelöste SID“). Außerdem fehlen Informationen zum spezifischen Sicherheitsprinzipaltyp (Benutzer, Computer, Gruppe usw.), der mit den Objekten verbunden ist. Nur SID/DN ist bekannt.
Spezielle Identität	LDAP		Windows und Active Directory verwenden intern bekannte Identitäten. Diese Identitäten funktionieren ähnlich wie Gruppen, aber AD deklariert sie nicht als solche. Weitere Informationen finden Sie unter Spezielle Identitätsgruppen.
Sonstige			Derzeit alle AD/SYSVOL-Objekte, die nicht unter die genannten Kategorien fallen.

Aktivitätsprotokolle

Die Aktivitätsprotokolle in Tenable Identity Exposure enthalten die Spuren aller Aktivitäten, die auf der Tenable Identity Exposure-Plattform im Zusammenhang mit bestimmten IP-Adressen, Benutzern oder Aktionen stattgefunden haben.

Hinweis: Aufgrund technischer Einschränkungen sind Aktivitätsprotokolle, die bestimmte Ansichten betreffen, wie etwa „Mandantenverwaltung" (einschließlich Hinzufügen, Bearbeiten oder Entfernen), derzeit nicht sichtbar.

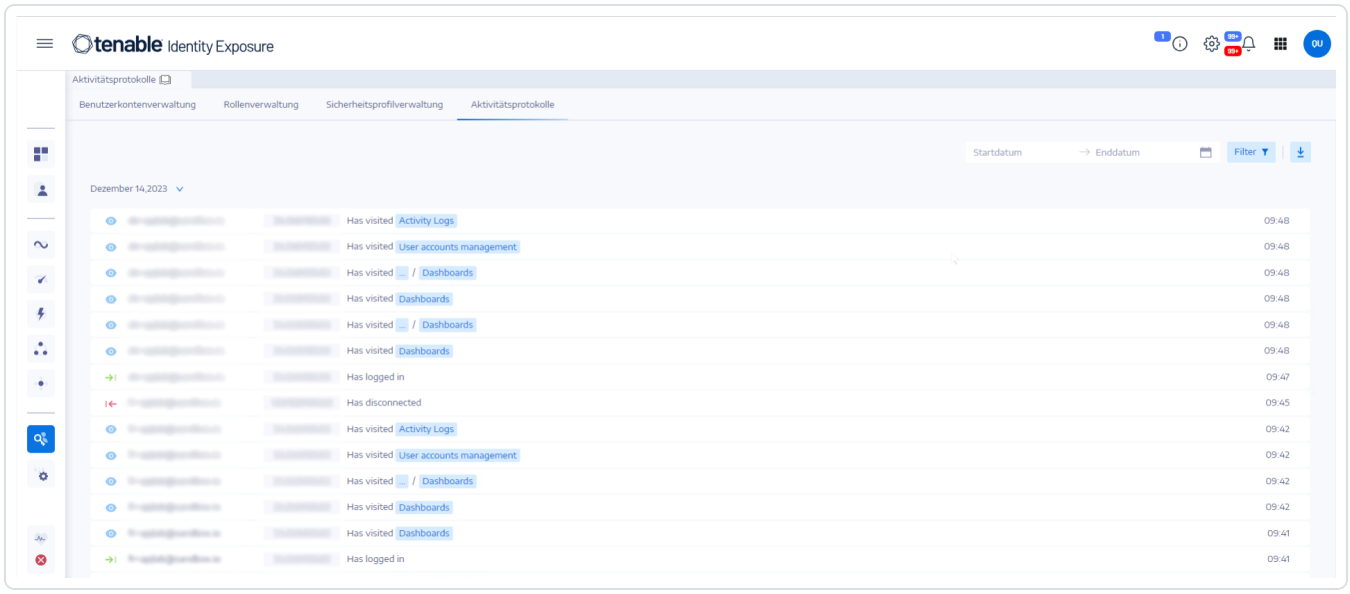
So zeigen Sie die Aktivitätsprotokolle an:

1. Klicken Sie in Tenable Identity Exposure auf das Symbol **Konten** in der linken Navigationsleiste.

   Der Fensterbereich zur **Benutzerkontenverwaltung** wird angezeigt.

2. Wählen Sie die Registerkarte **Aktivitätsprotokolle** aus.

   Der Fensterbereich „Aktivitätsprotokolle" wird geöffnet.



So zeigen Sie Aktivitätsprotokolle für einen bestimmten Zeitraum an:

1. Klicken Sie oben im Fensterbereich „Aktivitätsprotokolle" auf die Datumsauswahl.
2. Wählen Sie ein Startdatum und ein Enddatum für den gewünschten Zeitraum aus.

3. (Optional) Wählen Sie die Zeit mithilfe der Scrollleiste aus (Standardeinstellung: aktuelle Zeit).
4. Klicken Sie auf **OK**.

   Tenable Identity Exposure zeigt das Aktivitätsprotokoll für den betreffenden Zeitraum an.

So filtern Sie Aktivitätsprotokolle:

1. Klicken Sie oben im Fensterbereich „Aktivitätsprotokolle“ auf die Schaltfläche Filters.

   Der Fensterbereich **Filter** wird angezeigt.
2. Klicken Sie in den folgenden Feldern auf >:
   - IP-Adresse
   - Benutzer
   - Aktion
3. Klicken Sie auf **Validieren**.

   Tenable Identity Exposure zeigt das Aktivitätsprotokoll für den definierten Filter an.

So löschen Sie Filter:

- Klicken Sie unten im Fensterbereich **Filter** auf **Filter löschen**.

  Tenable Identity Exposure zeigt das ungefilterte Aktivitätsprotokoll an.

So exportieren Sie die Aktivitätsprotokolle:

- Klicken Sie oben im Fensterbereich „Aktivitätsprotokolle“ auf das Symbol .

  Tenable Identity Exposure lädt das Aktivitätsprotokoll im CSV-Format auf Ihren Computer herunter.

Tenable Identity Exposure-Administratorhandbuch

Zuletzt aktualisiert: 30 April 2024

Das Administratorhandbuch bietet Informationen über administrative Aufgaben für Tenable Identity Exposure (ehemals Tenable.ad).

Tenable empfiehlt die folgenden Schritte, um als Administrator in Tenable Identity Exposure zu beginnen:

- Vorbereiten und installieren
- Profil und Benutzer konfigurieren
- Erkennen und Überwachen

> **Tipp:** Weitere Informationen zu Tenable Identity Exposure finden Sie in den folgenden Materialien für Kundenschulungen:
>
> - Tenable Identity Exposure Self Help Guide
> - Einführung in Tenable Identity Exposure (Tenable University)

Vorbereiten und installieren

So bereiten Sie die Installation von Tenable Identity Exposure vor und führen sie durch:

- Installieren Sie Tenable Identity Exposure wie im *Tenable Identity Exposure Installation Guide* beschrieben.
- Verbinden Sie sich mit Tenable Identity Exposure und loggen Sie sich ein.

Profil und Benutzer konfigurieren

Als Nächstes empfehlen wir die folgenden Schritte, um die Benutzeroberfläche von Tenable Identity Exposure zu konfigurieren und darin zu navigieren:

- Profileinstellungen festlegen: Konfigurieren Sie Ihre Standardsprache, ändern Sie Ihr Passwort und legen Sie andere Einstellungen für Ihr Profil fest
- Erstellen Sie Benutzer und fügen Sie sie Ihrer Tenable Identity Exposure-Instanz hinzu.

- Konfigurieren Sie die rollenbasierte Zugriffssteuerung (RBAC), um den Zugriff auf Daten und Funktionen in Ihrer Organisation abzusichern.

Erkennen und Überwachen

Nachdem Sie Tenable Identity Exposure konfiguriert und an Ihre geschäftlichen Anforderungen angepasst haben, können Sie die Arbeit mit Ihren Daten beginnen.

- Stellen Sie das Modul Indicators of Attack bereit.
- Verwenden Sie das Tenable Identity Exposure-Portal, um die überwachte Infrastruktur zu verwalten und relevante Informationen über ihren Sicherheitsstatus zu erhalten.
- Definieren Sie Angriffsszenarien, indem Sie die Arten von Angriffen auswählen, die Tenable Identity Exposure in bestimmten Domänen überwachen soll.

Hinweis: Tenable Identity Exposure kann einzeln oder als Teil des Tenable One-Pakets erworben werden. Weitere Informationen finden Sie unter Tenable One.

Exposure-Management-Plattform Tenable One

Tenable One ist eine Exposure-Management-Plattform, mit deren Hilfe Unternehmen Sichtbarkeit auf ihrer gesamten modernen Angriffsoberfläche erzielen, Maßnahmen zur Verhinderung von wahrscheinlichen Angriffen fokussieren und Cyberrisiken präzise kommunizieren können, um eine optimale Unternehmensperformance zu unterstützen.

Die Plattform kombiniert eine umfassende Schwachstellen-Abdeckung über IT-Assets, Cloud-Ressourcen, Container, Web-Apps und Identitätssysteme hinweg, baut auf der Schnelligkeit und Breite der Schwachstellen-Abdeckung von Tenable Research auf und bietet zudem umfangreiche Analytik, um Maßnahmen zu priorisieren und Cyberrisiken zu kommunizieren Mit Tenable One können Unternehmen:

- Umfassenden Einblick in die gesamte moderne Angriffsoberfläche erzielen
- Bedrohungen vorhersehen und Maßnahmen zur Verhinderung von Angriffen priorisieren
- Cyberrisiken kommunizieren, um bessere Entscheidungen zu treffen

Tenable Identity Exposure ist als eigenständiges Produkt erhältlich oder kann als Teil der Exposure Management-Plattform Tenable One erworben werden.

Tipp: Weitere Informationen zu den ersten Schritten mit Tenable One-Produkten finden Sie im Tenable One Deployment Guide.

Weitere Informationen finden Sie in folgenden Ressourcen:

Active Directory-Konfiguration

Einige Aspekte des überwachten Active Directory müssen konfiguriert werden, damit bestimmte Tenable Identity Exposure-Funktionen ordnungsgemäß funktionieren:

- Zugriff auf AD-Objekte oder -Container
- Zugriff auf „Privilegierte Analyse“
- Bereitstellung von Indicators of Attack

Zugriff auf AD-Objekte oder -Container

Hinweis: Dieser Abschnitt gilt nur für eine Tenable Identity Exposure-Lizenz für das Modul „Indicators of Exposure“.

Tenable Identity Exposure erfordert für diese Sicherheitsüberwachung keine Administratorrechte.

Voraussetzung für diesen Ansatz ist, dass das von Tenable Identity Exposure verwendete Benutzerkonto alle in einer Domäne gespeicherten Active Directory-Objekte (einschließlich Benutzerkonten, Organisationseinheiten, Gruppen usw.) lesen kann.

Standardmäßig haben die meisten Objekte Lesezugriff für die vom Tenable Identity Exposure-Dienstkonto verwendeten Gruppendomänenbenutzer. Sie müssen einige Container jedoch manuell konfigurieren, um Lesezugriff für das Tenable Identity Exposure-Benutzerkonto zu gewähren.

Die folgende Tabelle enthält die Active Directory-Objekte und -Container, deren Lesezugriff auf die einzelnen von Tenable Identity Exposure überwachten Domänen manuell konfiguriert werden muss.

Speicherort des Containers	Beschreibung
`CN=Deleted Objects,DC=<DOMAIN>,DC=<TLD>`	Ein Container, der gelöschte Objekte hostet.
`CN=Password Settings Container,CN=System, DC=<DOMAIN>,DC=<TLD>`	(Optional) Ein Container, der Passworteinstellungsobjekte hostet.

So erteilen Sie Zugriff auf AD-Objekte oder -Container:

- Führen Sie in der Befehlszeilenschnittstelle des Domänencontrollers den folgenden Befehl aus, um Zugriff auf Active Directory-Objekte oder -Container zu erteilen:

  Hinweis: Sie müssen diesen Befehl für jede von Tenable Identity Exposure überwachte Domäne ausführen.

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

  Bedeutung:

- `<__CONTAINER__>` bezieht sich auf den Container, der Zugriff benötigt.
- `<__SERVICE_ACCOUNT__>` bezieht sich auf das von Tenable Identity Exposure verwendete Dienstkonto.

Zugriff auf „Privilegierte Analyse“

Die optionale Funktion „Privilegierte Analyse“ erfordert Administratorrechte. Sie müssen Berechtigungen für das von Tenable Identity Exposure verwendete Dienstkonto zuweisen.

Weitere Informationen finden Sie unter Privilegierte Analyse.

Hinweis: Sie müssen Berechtigungen in jeder Domäne zuweisen, in der Sie die Funktion „Privilegierte Analyse“ aktivieren.

So weisen Sie Berechtigungen über die Befehlszeile zu:

Anforderung: Zum Zuweisen von Berechtigungen benötigen Sie ein Konto mit Domänenadministrator- oder gleichwertigen Berechtigungen.

- Führen Sie in der Befehlszeilenschnittstelle des Domänencontrollers den folgenden Befehl aus, um beide Berechtigungen hinzuzufügen:

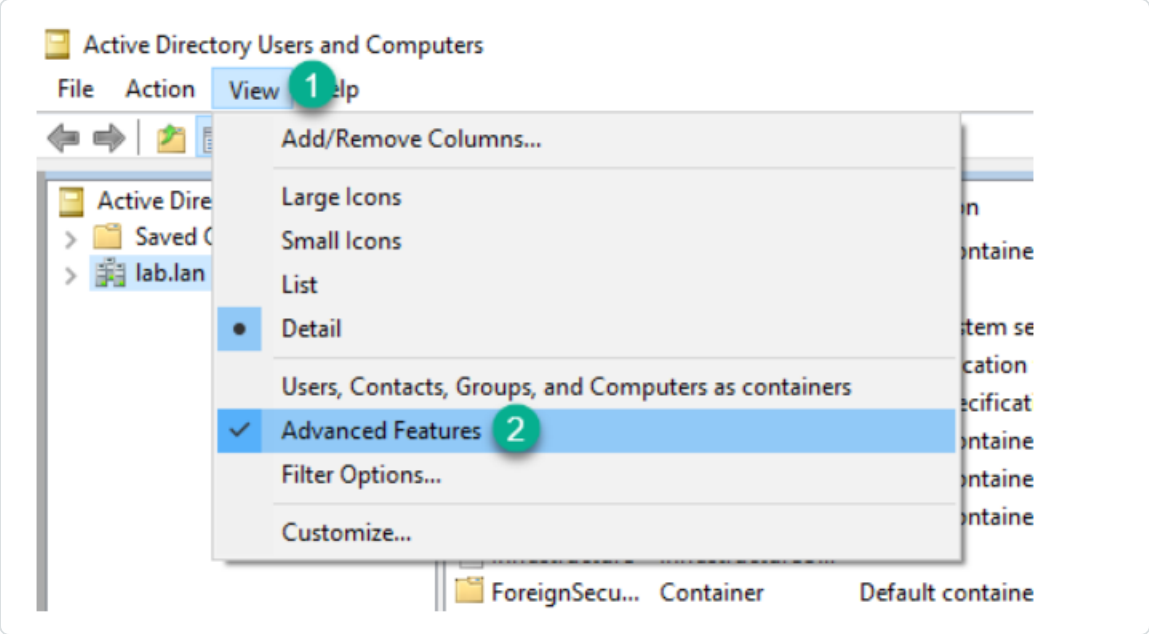
  ```
  dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
  SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
  ```

  Bedeutung:

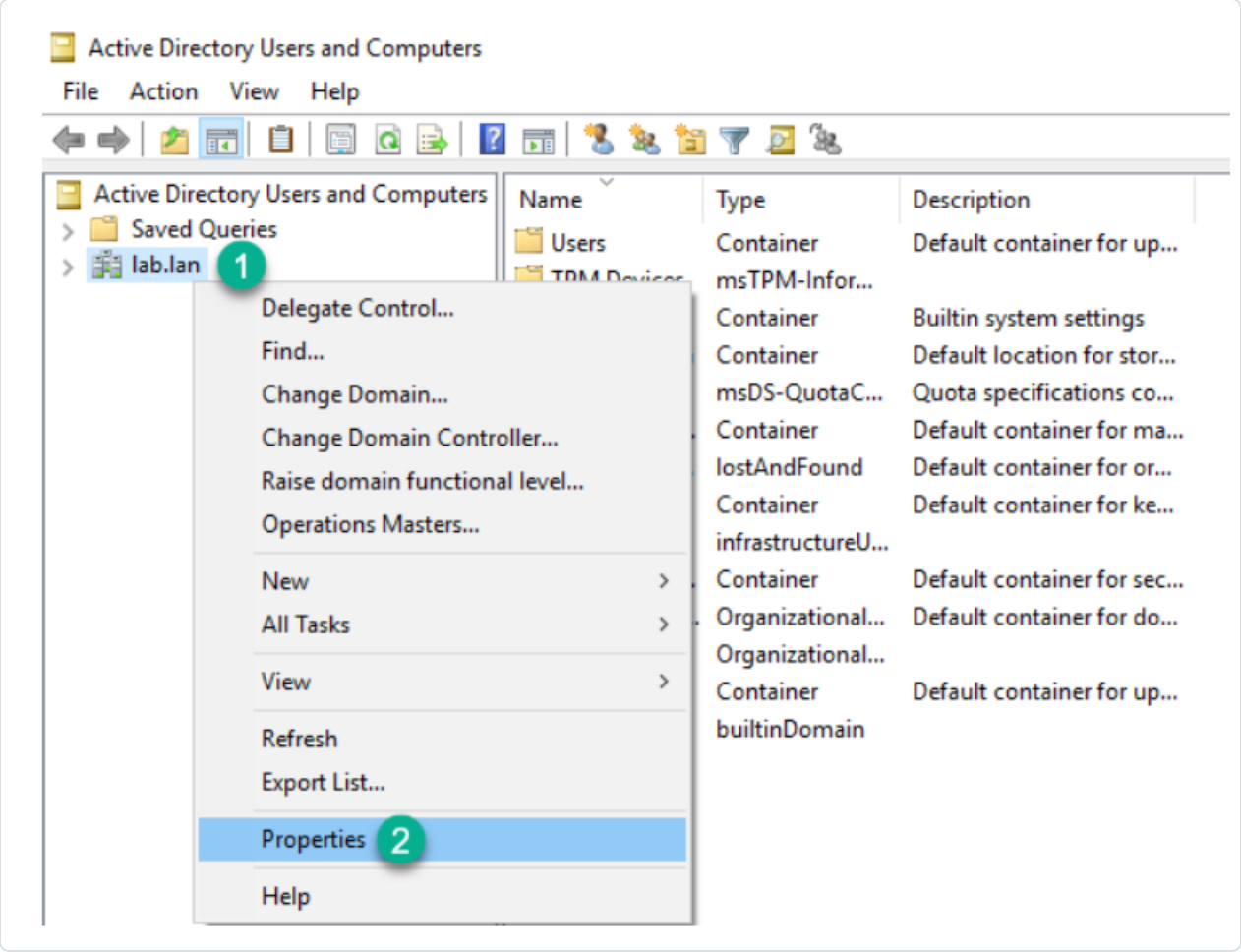
  - `<__DOMAIN_ROOT__>` bezieht sich auf den Distinguished Name des Domänenstamms. Beispiel: „`DC=<DOMAIN>,DC=<TLD>`“
  - `<__SERVICE_ACCOUNT__>` bezieht sich auf das von Tenable Identity Exposure verwendete Dienstkonto. Beispiel: „`DOMAIN\tenablead`“.

So weisen Sie Berechtigungen über die grafische Benutzeroberfläche zu:

1. Rufen Sie über das Menü **Start** in Windows das Tool **Active Directory-Benutzer und -Computer** auf.
2. Wählen Sie im Menü **Ansicht** die Option **Erweiterte Funktionen** aus.

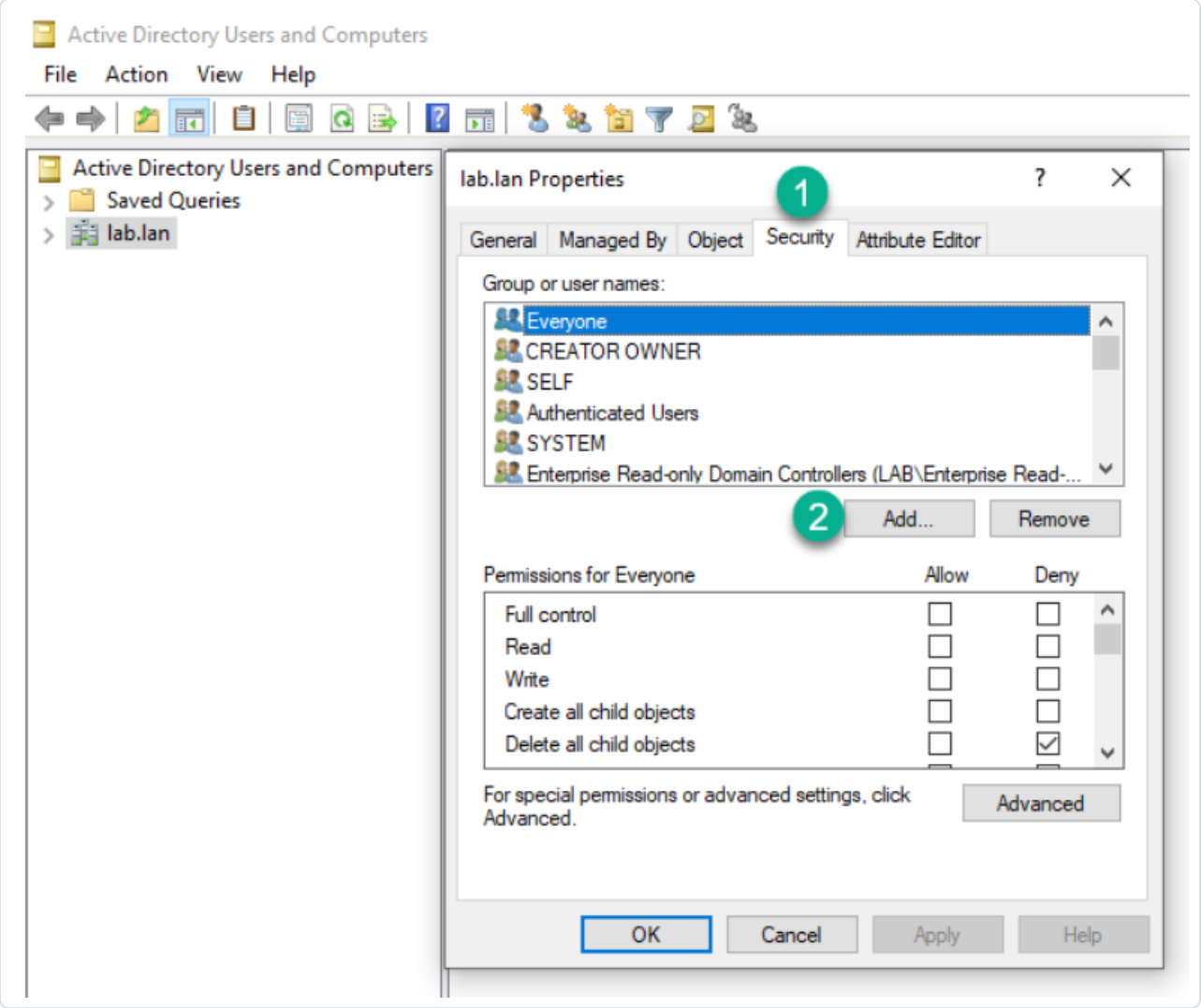


3. Klicken Sie mit der rechten Maustaste auf den Domänenstamm und wählen Sie **Eigenschaften** aus.



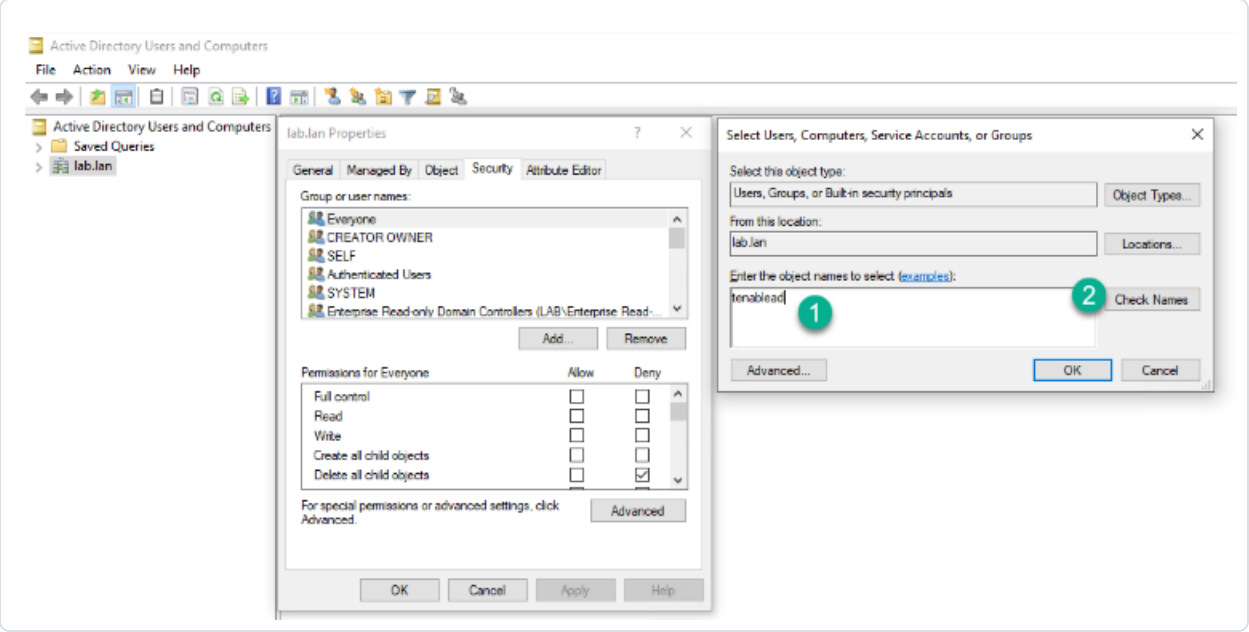
Das Eigenschaftenfenster des Domänenstamms wird geöffnet.

4. Klicken Sie auf die Registerkarte **Sicherheit** und dann auf **Hinzufügen**.

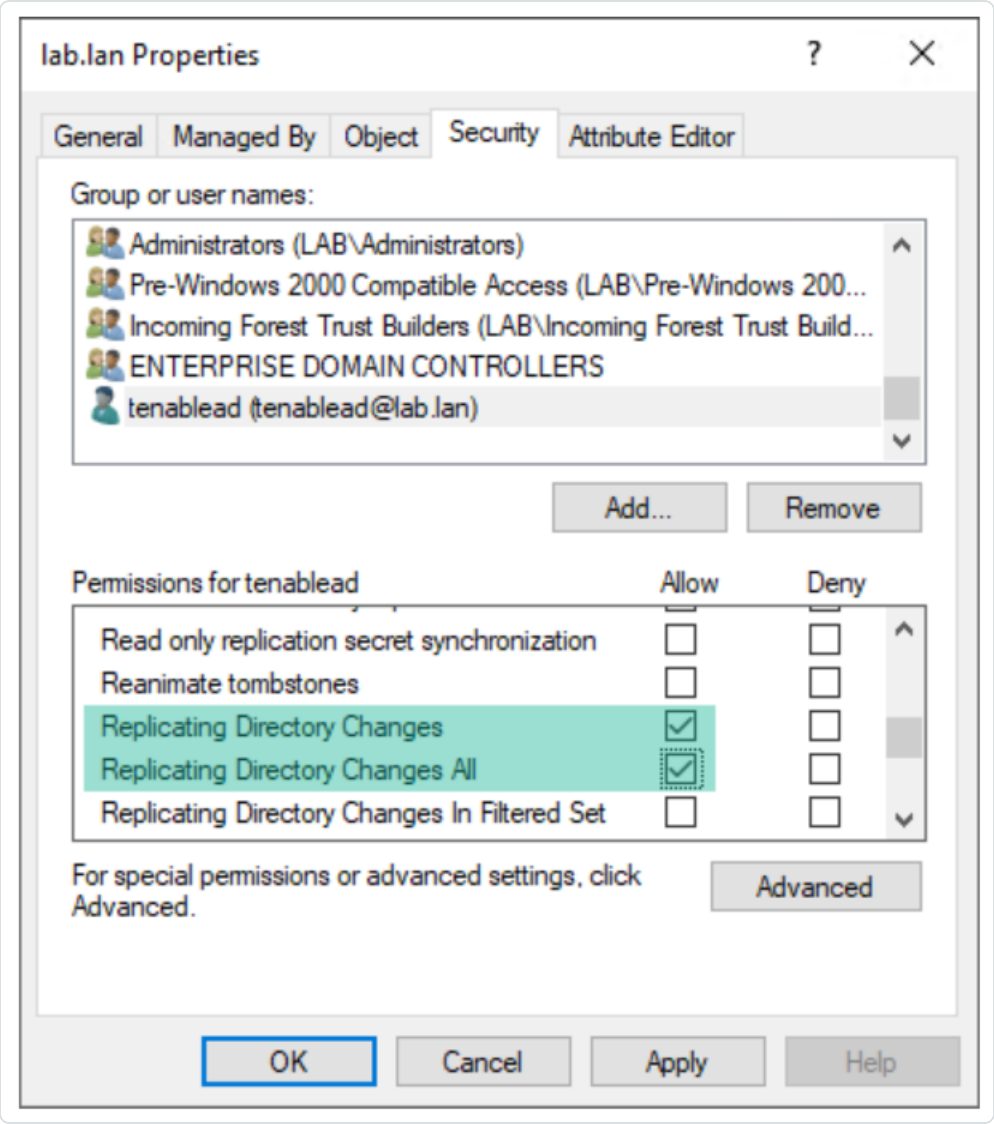


5. Suchen Sie das Tenable Identity Exposure-Dienstkonto:

> **Hinweis**: In einer Gesamtstruktur mit mehreren Domänen befindet sich das Dienstkonto möglicherweise in einer anderen Active Directory-Domäne.



6. Scrollen Sie in der Liste nach unten und heben Sie die Auswahl aller standardmäßig aktivierten Berechtigungen auf.
7. Wählen Sie in der Spalte **Zulassen** die Berechtigungen *Verzeichnisänderungen replizieren* und *Alle Verzeichnisänderungen replizieren* aus.



8. Klicken Sie auf **OK**.

Wichtige Hinweise

Tenable Identity Exposure erfordert nur ein Dienstkonto pro Gesamtstruktur. Daher müssen Sie beim Zuweisen von Berechtigungen in einer Domäne möglicherweise **nach dem Dienstkonto einer anderen Domäne suchen**.

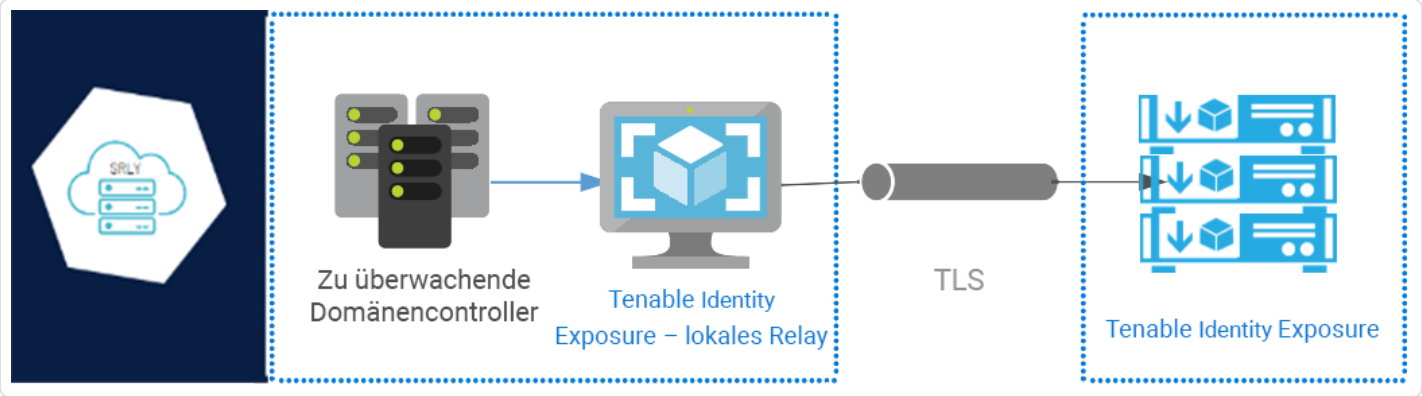
Sie müssen zusätzliche Berechtigungen **auf Ebene des Domänenstamms** zuweisen. Active Directory unterstützt keine Berechtigungen, die einer Organisationseinheit oder einem bestimmten Benutzer zugewiesen sind – z. B. um die Funktion „Privilegierte Analyse" auf die OU oder den Benutzer zu beschränken. Diese haben daher keine Wirkung.

Diese Berechtigungen geben dem Tenable Identity Exposure-Dienstkonto sehr viel mehr Kontrolle über die Active Directory-Domäne. Sie müssen es daher als **privilegiertes Konto (Tier 0)** betrachten und ähnlich schützen wie ein Domänenadministratorkonto. Das vollständige Verfahren finden Sie unter Schutz von Dienstkonten.

Secure Relay

Secure Relay ist ein Modus zur Übertragung Ihrer Active Directory-Daten aus Ihrem Netzwerk an Tenable Identity Exposure, bei dem TLS (Transport Layer Security) anstelle eines VPN verwendet wird, wie in dieser Abbildung dargestellt. Die Relay-Funktion unterstützt auch HTTP-Proxy mit oder ohne Authentifizierung, wenn das Netzwerk einen Proxy-Server benötigt, um das Internet zu erreichen.

Tenable Identity Exposure kann mehrere Secure Relays unterstützen, die Sie Ihren Anforderungen entsprechend Domänen zuordnen können.

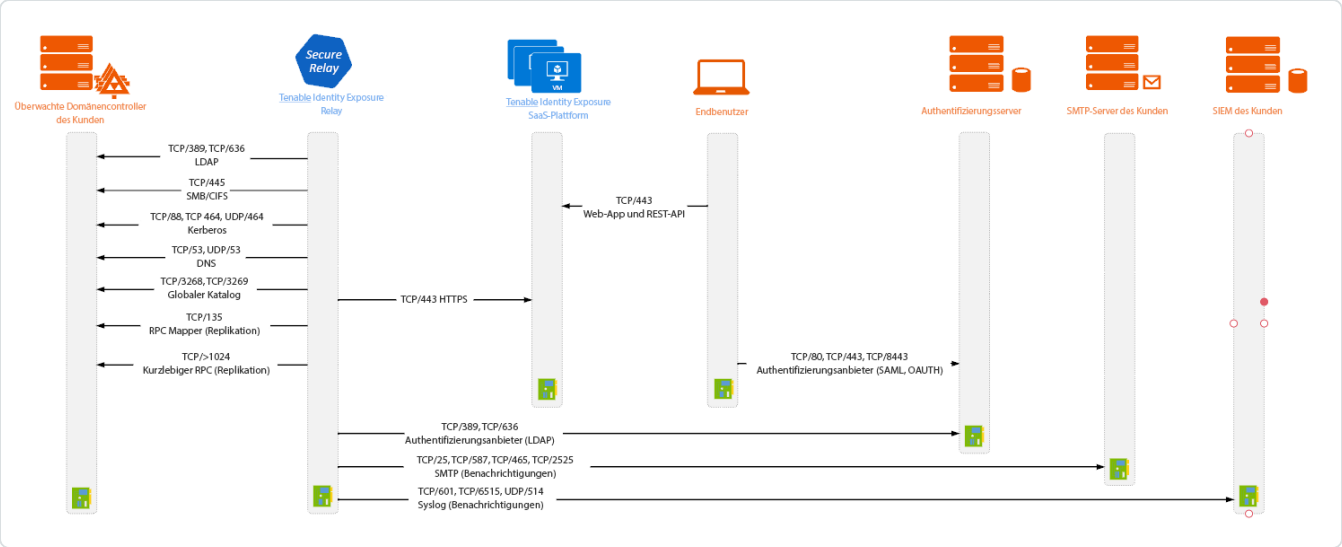


Hinweis: Die Secure Relay-Funktion ist derzeit nur verfügbar, wenn Tenable Identity Exposure Ihre Plattform für die Verwendung von Secure Relay einrichtet. Eine manuelle Umstellung der Bereitstellung von VPN auf Secure Relay ist nicht möglich. Wenden Sie sich an Ihren Tenable Identity Exposure-Kundendienstmitarbeiter, wenn Sie Unterstützung bei der Migration Ihrer Plattform von VPN zu Secure Relay benötigen.

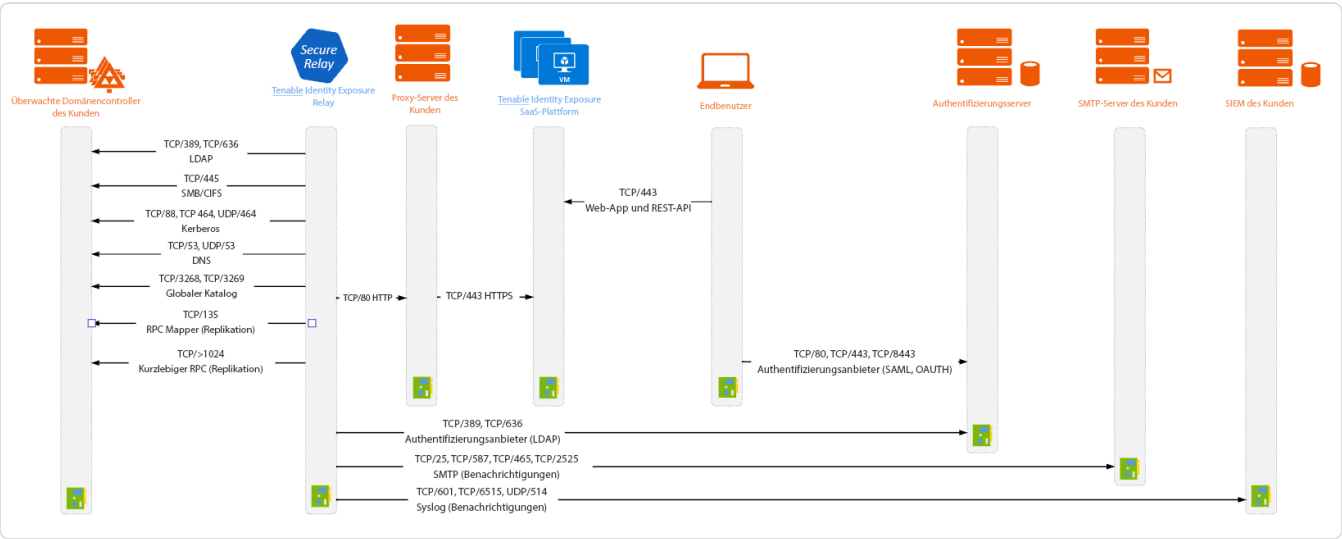
Netzwerkflüsse

Erforderliche Ports für Secure Relay

- Für ein klassisches Setup **ohne Proxy-Server** benötigt das Relay folgende Ports:



- Für ein Setup **mit Proxy-Server** benötigt das Relay folgende Ports:



TLS-Anforderungen

Um TLS 1.2 verwenden zu können, muss Ihr Relay-Server ab dem 24. Januar 2024 mindestens eine der folgenden Verschlüsselungssammlungen unterstützen:

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

Stellen Sie außerdem sicher, dass Ihre Windows-Konfiguration auf die angegebenen Verschlüsselungssammlungen abgestimmt ist, damit die Kompatibilität mit der Relay-Funktion gegeben ist.

So suchen Sie nach Verschlüsselungssammlungen:

1. Führen Sie in PowerShell den folgenden Befehl aus:

```
@("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. Prüfen Sie die Ausgabe: `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. Wenn kein Ergebnis zurückgegeben wird (leere Ausgabe), bedeutet dies, dass keine der erforderlichen Verschlüsselungssammlungen aktiviert ist, damit die TLS-Verbindung des Relay funktioniert. Aktivieren Sie mindestens eine Verschlüsselungssammlung.
4. Überprüfen Sie die ECC-Kurve (Elliptic Curve Cryptography) vom Relay-Server. Diese Überprüfung ist für die Verwendung von ECDHE-Verschlüsselungssammlungen (Elliptic Curve Diffie-Hellman Ephemeral) obligatorisch. Führen Sie in PowerShell den folgenden Befehl aus:

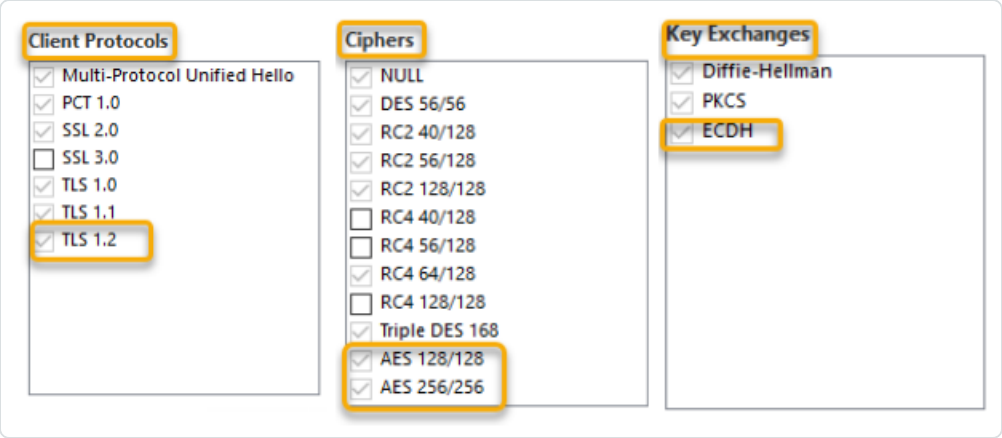
```
Get-TlsEccCurve
```

5. Prüfen Sie, ob die Kurve **25519** vorhanden ist. Wenn dies nicht der Fall ist, aktivieren Sie sie.

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

So überprüfen Sie die Windows-Kryptografieeinstellungen:

1. Prüfen Sie mithilfe eines IIS-Kryptotools, ob die folgenden Optionen aktiviert sind:
    - Client-Protokolle: **TLS 1.2**
    - Verschlüsselungen: **AES 128/128** und **AES 256/256**
    - Schlüsselaustausch: **ECDH**



2. Nachdem Sie die Kryptografieeinstellungen geändert haben, starten Sie den Computer neu.

> **Hinweis**: Eine Änderung der Windows-Kryptografieeinstellungen betrifft alle Anwendungen, die auf dem Computer ausgeführt werden und die die Windows TLS-Bibliothek, auch „Schannel" genannt, verwenden. Stellen Sie daher sicher, dass die von Ihnen vorgenommenen Anpassungen keine unbeabsichtigten Nebenwirkungen haben. Überprüfen Sie, ob die ausgewählten Konfigurationen auf die allgemeinen Härtungsziele oder Compliance-Vorgaben des Unternehmens abgestimmt sind.

Bevor Sie beginnen

Voraussetzungen

Virtuelle Maschine

Für die virtuelle Maschine (VM), auf der das Secure Relay gehostet wird, gelten folgende Anforderungen:

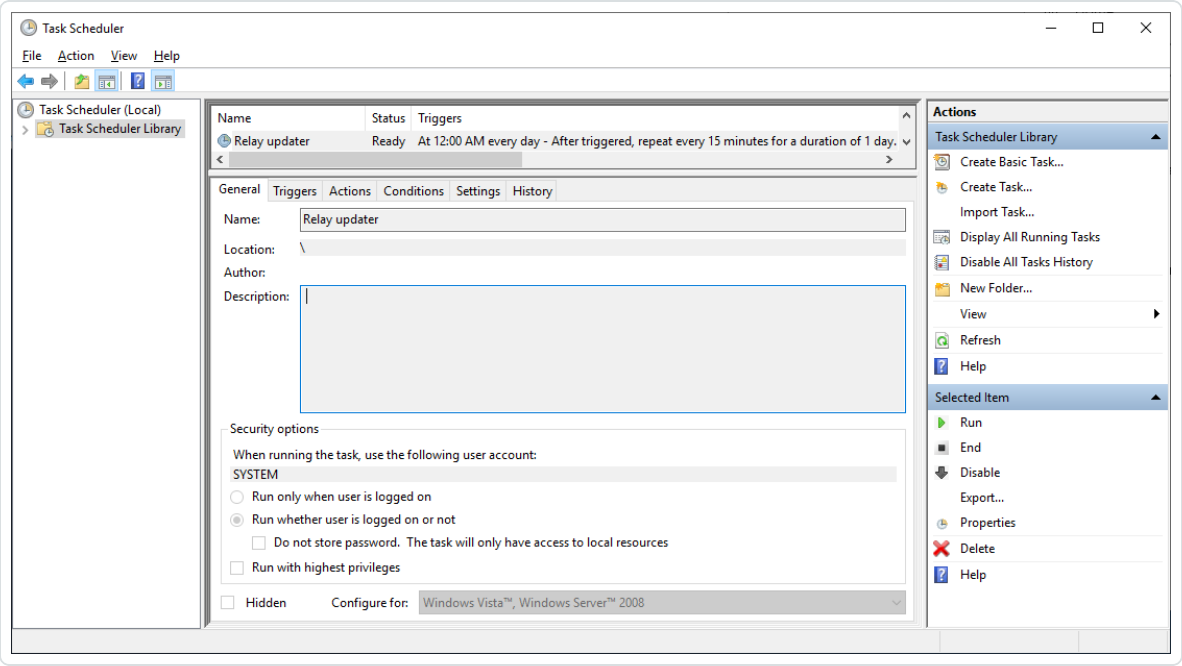
Kundengröße	Tenable Identity Exposure-Dienste	Erforderliche Instanz	Arbeitsspeicher (pro Instanz)	vCPU (pro Instanz)	Festplattentopologie	Verfügbarer Festplattenspeicher (pro Instanz)
Beliebige Größe	• `tenable_Relay` • `tenable_envoy`	1	8 GB RAM	2 vCPU	Partition für Protokolle getrennt von der Systempartition	30 GB

Die VM muss außerdem über Folgendes verfügen:

- Betriebssystem Windows Server 2016 oder höher (kein Linux)
- Gelöste Internet-DNS-Abfragen und Internetzugang für mindestens `cloud.tenable.com` und `*.tenable.ad` (TLS 1.2).
- Lokale Administratorrechte
- EDR-, Antivirus- und GPO-Konfiguration:
    - Ausreichend verbleibende CPU-Leistung auf der VM – zum Beispiel verbraucht die Echtzeitfunktion von Windows Defender eine beträchtliche Menge an CPU-Leistung und

kann den Rechner auslasten.

- Automatische Updates:
  - Erlauben Sie Aufrufe an `*.tenable.ad`, damit die automatische Aktualisierungsfunktion eine ausführbare Relay-Datei herunterladen kann.
  - Stellen Sie sicher, dass kein Gruppenrichtlinienobjekt (GPO) die automatische Aktualisierungsfunktion blockiert.
  - Löschen oder ändern Sie die geplante Aufgabe „Relay Updater“ nicht:



Rollenberechtigungen

Sie müssen ein Benutzer mit rollenbasierten Berechtigungen sein, um das Relay zu konfigurieren. Die folgenden Berechtigungen sind erforderlich:

- **Datenentitäten**: Entitäts-Relay
- **Schnittstellenentitäten**:
  - Verwaltung > System > Konfiguration > Anwendungsdienste > Relay
  - Verwaltung > System > Relay-Verwaltung

Weitere Informationen finden Sie unter Berechtigungen für eine Rolle festlegen.

Zulässige Dateien und Prozesse

Damit das Relay reibungslos funktioniert, müssen bestimmte Dateien und Prozesse für Sicherheitstools von Drittanbietern wie Antiviren- und/oder EDR (Endpoint Detection and Response)- und XDR (Extended Detection and Response)-Anwendungen zugelassen werden.

Lassen Sie die folgenden Dateien und Prozesse zu:

Hinweis: Passen Sie den Pfad auf C:\ an Ihr Relay-Installationslaufwerk an.

Windows
Dateien
C:\Tenable*
C:\tools*
C:\ProgramData\Tenable*
Prozesse
nssm.exe –> Pfad: C:\tools\nssm.exe
Tenable.Relay.exe –> Pfad: C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe –> Pfad: C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe –> Pfad: C:\Tenable\Tenable.ad\updater.exe
powershell.exe –> Pfad: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (kann je nach Betriebssystemversion unterschiedlich sein)
Geplante Aufgaben
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

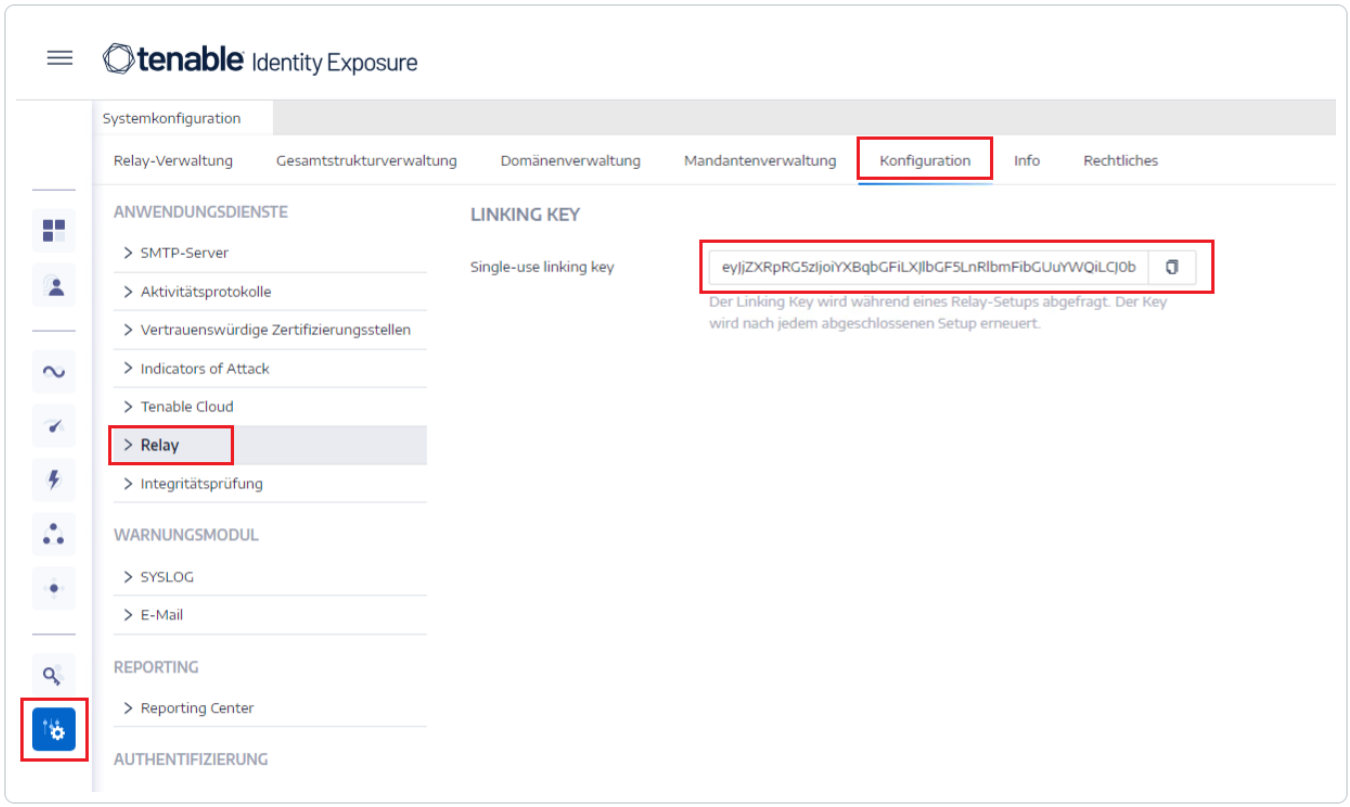
Registrierungsschlüssel
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

Linking Key

Für die Installation von Secure Relay ist ein einmal verwendbarer Linking Key erforderlich, der die Adresse Ihres Netzwerks und ein Authentifizierungstoken enthält. Tenable Identity Exposure generiert nach jeder erfolgreichen Installation von Secure Relay einen neuen Key.

So rufen Sie den Linking Key ab:

1. Klicken Sie in Tenable Identity Exposure in der linken Menüleiste auf **System** und wählen Sie die Registerkarte **Konfiguration** > **Relay** aus.



2. Klicken Sie auf ❐, um den Linking Key zu kopieren.

Installation

So installieren Sie das Secure Relay:

- Wählen Sie eine Installationsmethode:
  - Secure Relay installieren (GUI)
  - Secure Relay installieren (Tenable Nessus Agent)

Deinstallation

So deinstallieren Sie ein Secure Relay:

1. Gehen Sie in Windows zu **Einstellungen** > **Apps & Features** > **Tenable Identity Exposure Secure Relay**.
2. Klicken Sie auf **Deinstallieren**.

   Wenn die Deinstallation abgeschlossen ist, werden Dienste und Umgebungsvariablen von Tenable Identity Exposure Secure Relay nicht mehr in Ihrem System angezeigt.
3. Klicken Sie in Tenable Identity Exposure in der linken Menüleiste auf **Systeme** und wählen Sie die Registerkarte **Relay-Verwaltung** aus.
4. Wählen Sie das Relay aus, das Sie gerade deinstalliert haben, und klicken Sie auf  , um es aus der Liste der verfügbaren Relay zu entfernen.

Automatische Updates

Nachdem Sie Secure Relay installiert haben, sucht Tenable Identity Exposure regelmäßig nach neuen Versionen. Dieser Vorgang läuft vollständig automatisiert ab und erfordert HTTPS-Zugriff auf Ihre Domäne (TCP/443). Ein Symbol in der Netzwerkleiste zeigt an, wenn Secure Relay von Tenable Identity Exposure aktualisiert wird. Sobald der Vorgang abgeschlossen ist, werden die Tenable Identity Exposure-Dienste neu gestartet und die Datenerfassung wird fortgesetzt.

Siehe auch

Vollständige Informationen zu Secure Relay finden Sie unter „Secure Relay“ im Administratorhandbuch zu Tenable Identity Exposure.

Secure Relay installieren (GUI)

Mit dem folgenden Verfahren wird das Secure Relay über ein Windows-Installationsprogramm installiert. Bevor Sie beginnen, überprüfen Sie, ob die nötigen Voraussetzungen erfüllt sind und Sie über den **erforderlichen Linking Key** verfügen, wie unter Secure Relay beschrieben.

So installieren Sie das Secure Relay:

1. Laden Sie das Installationsprogramm aus dem Tenable Identity Exposure-Downloads-Portal auf Ihre virtuelle Maschine herunter.
2. Doppelklicken Sie auf die Datei `tenable.ad_SecureRelay_v3.xx.x`, um den Installationsassistenten zu starten.

   Der **Begrüßungsbildschirm** wird angezeigt.

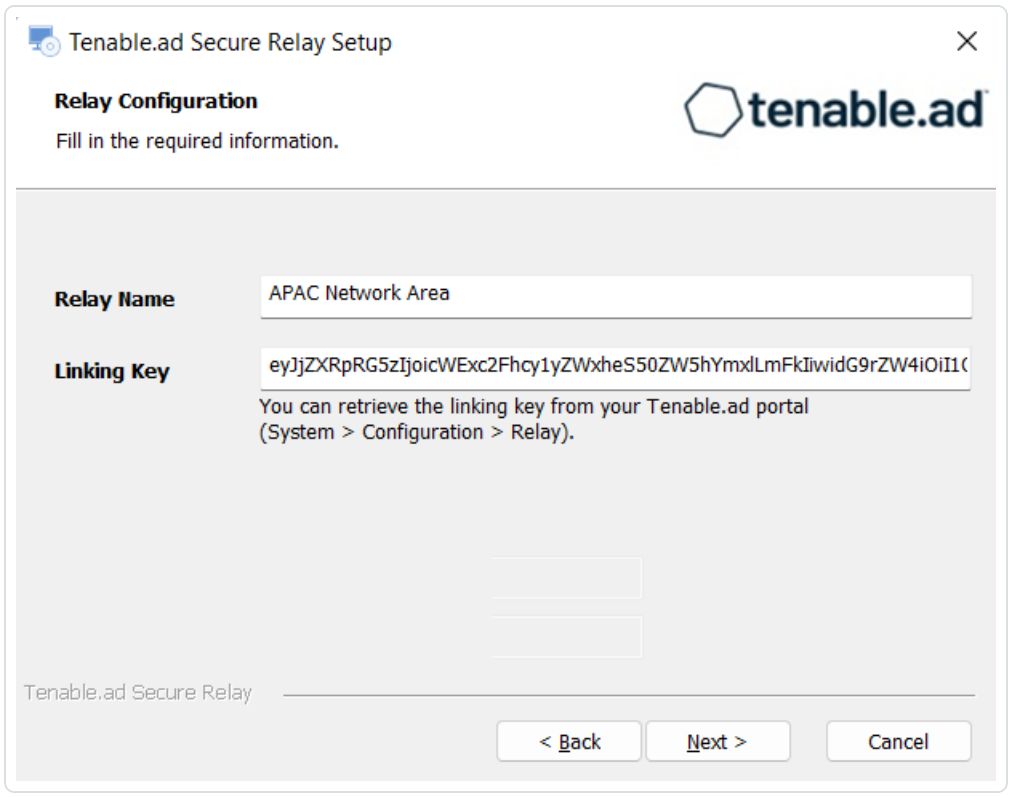
   

3. Klicken Sie auf **Next**.

   Das Fenster **Custom Setup** wird angezeigt.

4. Klicken Sie auf **Browse**, um die Festplattenpartition auszuwählen, die Sie für Secure Relay reserviert haben (getrennt von der Systempartition).
5. Klicken Sie auf **Next**.

   Das Fenster **Relay Configuration** wird angezeigt.



6. Geben Sie folgende Informationen an:

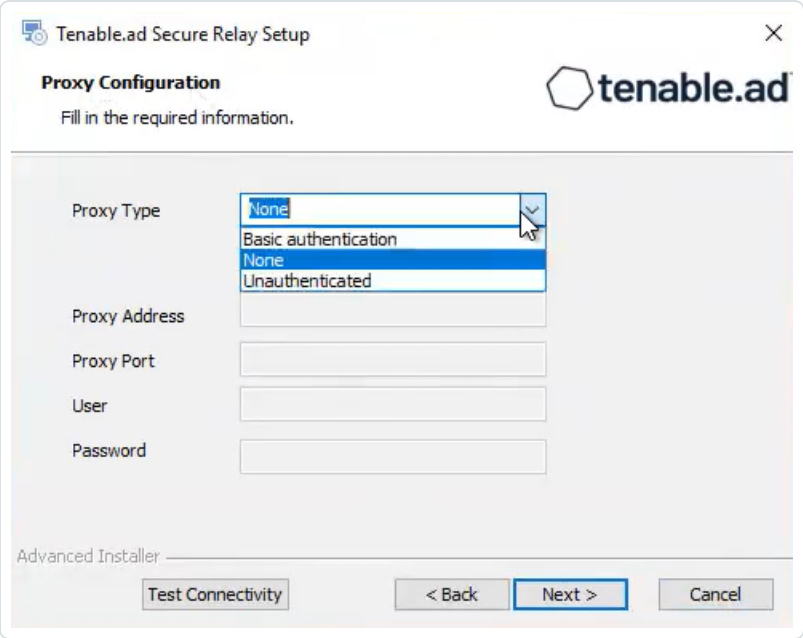
    a. Geben Sie im Feld **Relay Name** einen Namen für Ihr Secure Relay ein.

    b. Fügen Sie im Feld **Linking Key** den Linking Key ein, den Sie aus dem Tenable Identity Exposure-Portal abgerufen haben.

    c. Wenn Sie sich für die Verwendung eines Proxy-Servers entscheiden, aktivieren Sie die Option **Use an HTTP Proxy for your Relay calls** und geben Sie die Proxy-Adresse und die Portnummer an.

7. Klicken Sie auf **Next**.

    Das Fenster „Proxy-Konfiguration“ wird angezeigt:



8. Wählen Sie eine der folgenden Optionen aus:

    a. **Kein**: Es soll kein Proxy-Server verwendet werden.

    b. **Nicht authentifiziert**: Geben Sie die Adresse und den Port für den Proxy-Server ein.

    c. **Standardauthentifizierung**: Geben Sie zusätzlich zu Adresse und Port den Benutzer und das Passwort für den Proxy-Server ein.

    Achtung: Um einen Proxy mit „Nicht authentifiziert" oder „Standardauthentifizierung" zu konfigurieren, unterstützt das Relay nur IPv4-Adressen (wie `192.168.0.1`) oder einen Proxy-URI ohne `http://` oder `https://` (wie `myproxy.mycompany.com`). Das Relay unterstützt keine IPv6-Adressen (wie `2001:0db8:85a3:0000:0000:8a2e:0370:7334`).

9. Klicken Sie auf **Konnektivität testen**. Folgende Ergebnisse sind möglich:

    - **Grünes Licht** – Die Verbindung wurde erfolgreich hergestellt.
    - **Ungültiger Linking Key** – Rufen Sie den Linking Key aus dem Tenable Identity Exposure-Portal ab.
    - **Ungültiger Relay-Name** – Dieses Feld darf nicht leer bleiben. Geben Sie einen Namen für das Relay an.
    - **Verbindung fehlgeschlagen** – Überprüfen Sie Ihren Internetzugriff.

10. Klicken Sie auf **Next**.

Das Fenster **Ready to Install** wird angezeigt.

11. Klicken Sie auf **Install**.
12. Klicken Sie nach Abschluss der Installation auf **Finish**.

Nächste Schritte

- Überprüfungen nach der Installation

Siehe auch

- Secure Relay
- Secure Relay installieren (Tenable Nessus Agent)
- Überprüfungen nach der Installation
- Relay konfigurieren

Secure Relay installieren (Tenable Nessus Agent)

Mit dem folgenden Verfahren wird das Secure Relay über Tenable Nessus Agent installiert.

Bevor Sie beginnen

- Überprüfen Sie, ob Sie Tenable Nessus Agent heruntergeladen und installiert haben.

  Hinweis: Das Tenable Nessus Agent-Installationsprogramm fragt nach einem Agent-Schlüssel. Dieser Schlüssel ist für die Secure Relay-Funktion **nicht erforderlich**.

- Erfüllen Sie die erforderlichen Voraussetzungen und verwenden Sie den **erforderlichen Linking Key**, wie in Secure Relay beschrieben.

So installieren Sie das Secure Relay:

1. Öffnen Sie auf einem Computer, auf dem Tenable Nessus Agent gehostet wird und der als Relay fungiert, ein Administrator-Eingabeaufforderungsfenster im Verzeichnis Tenable Nessus Agent (`c:\Programme\Tenable\Nessus Agent`). Geben Sie dann den folgenden Befehl ein:

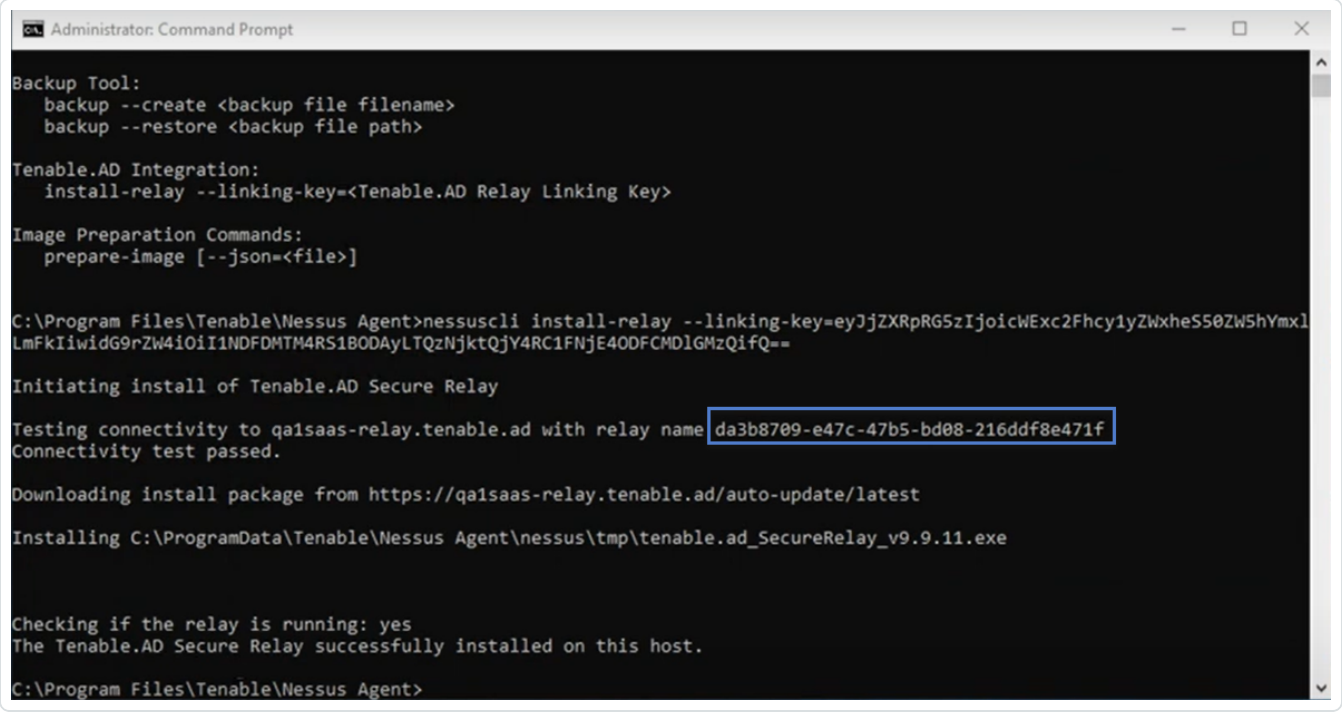
   Installation eines Secure Relay

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

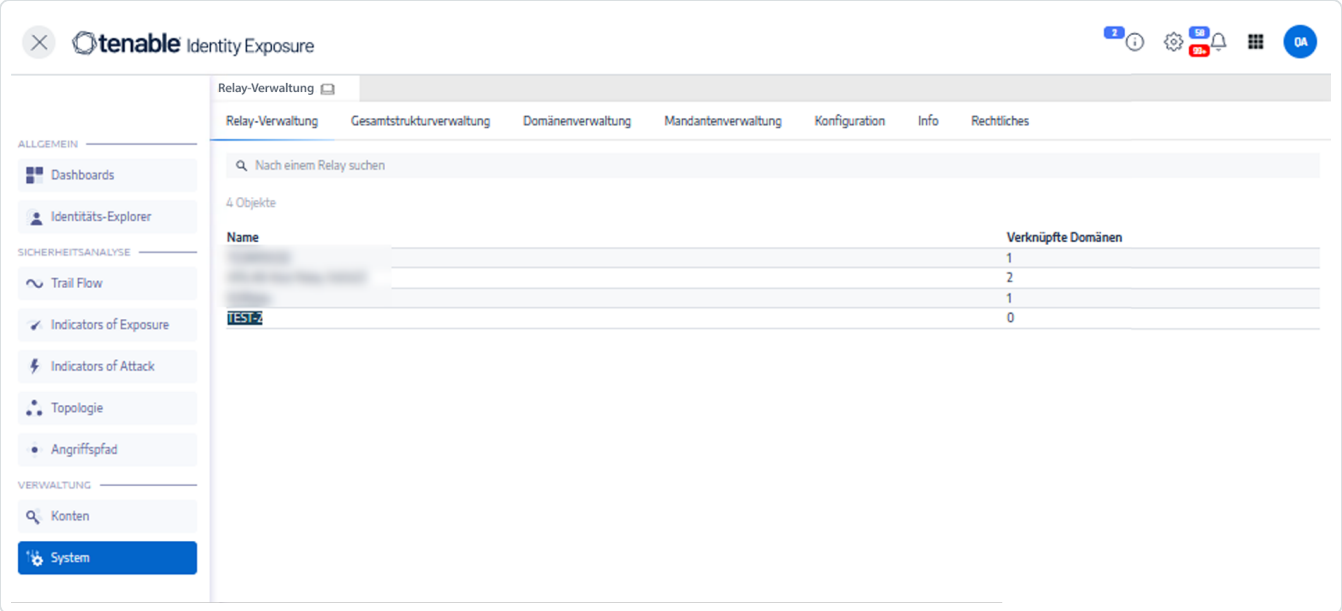
2. Ersetzen Sie <Tenable Identity Exposure Relay Linking Key> durch den Wert, den Sie zuvor aus der Tenable Identity Exposure-Instanz kopiert haben, und geben Sie eine Proxy-Adresse und eine Portnummer an, wenn Sie einen Proxy-Server verwenden.

   Die Installation beginnt. Die Durchführung der Konnektivitätsprüfungen und der Installationsvorgang dauern einige Minuten.

   Wenn die Installation erfolgreich abgeschlossen wurde, wird eine Meldung angezeigt, dass das Relay auf dem Hostcomputer ausgeführt wird.



3. Klicken Sie in Tenable Identity Exposure auf **System** > **Relay-Verwaltung**. Das neu installierte Relay wird in der Liste der Relays mit der im Installationsfenster angezeigten Kennung angezeigt.



Nächste Schritte

- Überprüfungen nach der Installation

Siehe auch

- Secure Relay
- Secure Relay installieren (GUI)
- Überprüfungen nach der Installation
- Relay konfigurieren

Überprüfungen nach der Installation

Überprüfen Sie nach Abschluss der Secure Relay-Installation Folgendes:

Liste der installierten Relays in Tenable Identity Exposure

So zeigen Sie die Liste der installierten Relays an:

- Klicken Sie in Tenable Identity Exposure in der linken Menüleiste auf **Systeme** und wählen Sie die Registerkarte **Relay-Verwaltung** aus.

  Im Fensterbereich wird eine Liste der Secure Relays und ihrer verknüpften Domänen angezeigt.

Dienste

Nach erfolgreicher Installation werden die folgende Dienste ausgeführt:

- `Tenable_Relay`
- `tenable_envoy`

  > **Hinweis**: Sie finden die Envoy-Lizenz in Tenable Identity Exposure unter **Systeme** > **Rechtliches** > **Envoy-Lizenz**.

Umgebungsvariablen

Mit der Installation wurden außerdem vier neue Umgebungsvariablen hinzugefügt, die sich auf Secure Relay beziehen und deren Namen mit „ALSID“ beginnen. Wenn Sie sich für die Verwendung eines Proxy-Servers entschieden haben, gibt es zwei zusätzliche Variablen, die sich auf die Proxy-IP und den Port beziehen.

Protokolle zur Fehlerbehebung

Protokolle befinden sich an diesen Speicherorten:

- **Installationsprotokolle**: `C:\Users\<Ihr Benutzer>\AppData\Local\Temp`
- **Relay-Protokolle**: Auf der VM, auf der Secure Relays gehostet werden, in dem bei der Installation angegebenen Ordner

Nächste Schritte

- Relay konfigurieren

Siehe auch

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

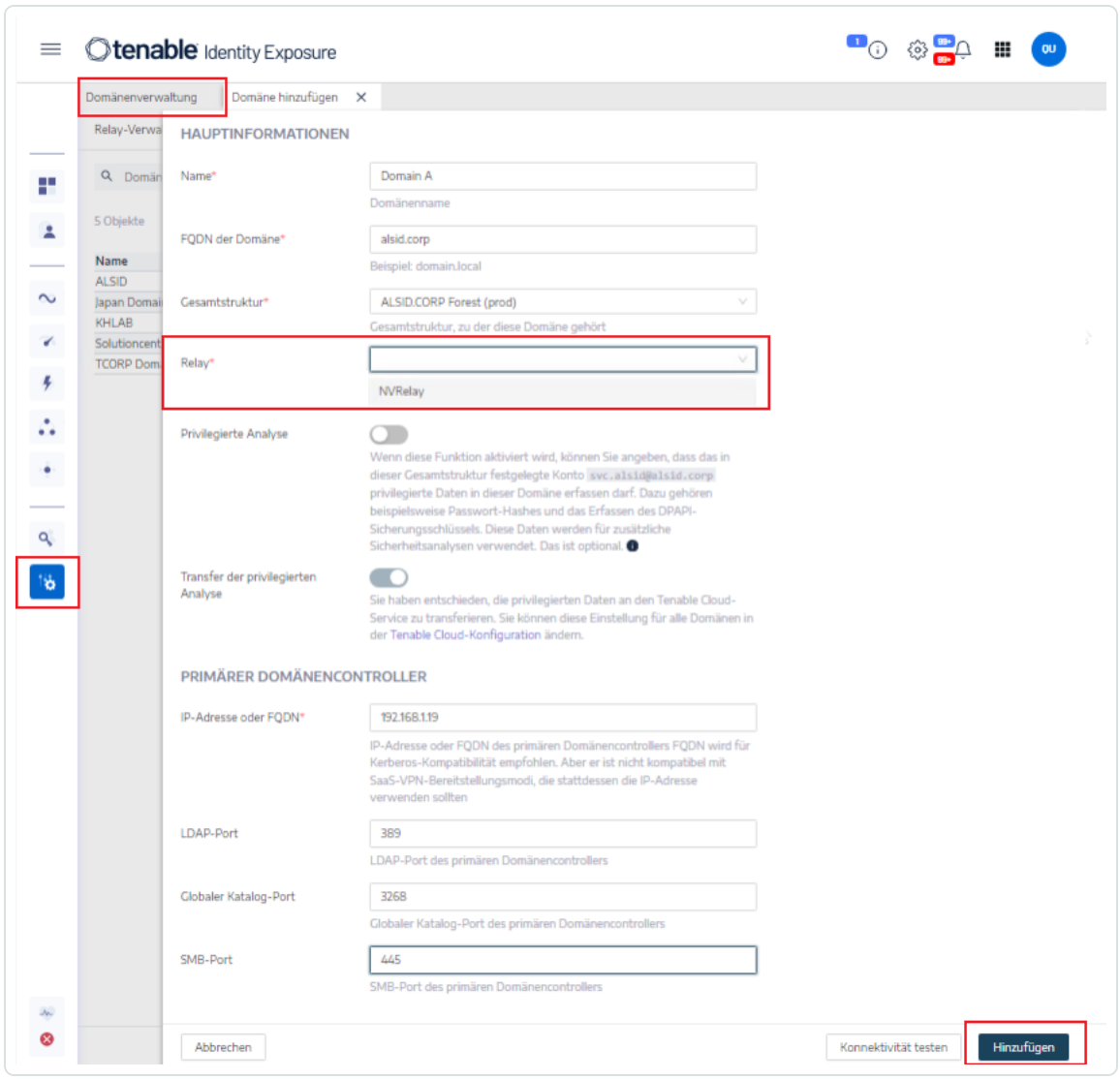
Relay konfigurieren

Nach der Installation und den Überprüfungen im Anschluss an die Installation konfigurieren Sie Ihr Relay in Tenable Identity Exposure, um es mit einer Domäne zu verknüpfen und Warnmeldungen einzurichten.

So verknüpfen Sie eine Domäne mit einem Secure Relay:

1. Klicken Sie in Tenable Identity Exposure in der linken Menüleiste auf **Systeme** und wählen Sie die Registerkarte **Domänenverwaltung** aus.
2. Wählen Sie in der Liste der Domänen eine zu verknüpfende Domäne aus und klicken Sie am Ende der Zeile auf ✎.

   Daraufhin wird der Bereich **Domäne bearbeiten** geöffnet.
3. Klicken Sie im Feld **Relay** auf den Pfeil, um eine Dropdown-Liste der installierten Relays anzuzeigen, und wählen Sie ein Relay aus, das mit der Domäne verknüpft werden soll.



4. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Domäne aktualisiert hat. Sysvol und LDAP werden synchronisiert, um die Änderung zu übernehmen. Der Trail Flow beginnt, neue Ereignisse zu empfangen.

Siehe auch

- Secure Relay
- Secure Relay installieren (GUI)
- Secure Relay installieren (Tenable Nessus Agent)
- Überprüfungen nach der Installation

Bereitstellung von Indicators of Attack

Hinweis: Diese Information gilt nur für Lizenzen, die das Modul „Indicators of Attack" enthalten.

Mit dem Modul **Indicators of Attack** (IoA) von Tenable Identity Exposure können Sie Angriffe auf Ihr Active Directory (AD) erkennen. Für jeden IoA sind spezifische Überwachungsrichtlinien erforderlich, die das Installationsskript automatisch aktiviert. Eine vollständige Liste der Tenable Identity Exposure-IoAs und ihrer Implementierung finden Sie im Tenable Identity Exposure – Referenzhandbuch zu Indicators of Attack im Tenable-Downloads-Portal.

Indicators of Attack und das Active Directory

Tenable Identity Exposure ist eine nicht-intrusive Lösung, die eine Active Directory-Infrastruktur ohne Einsatz von Agents und mit minimalen Konfigurationsänderungen in Ihrer Umgebung überwacht.

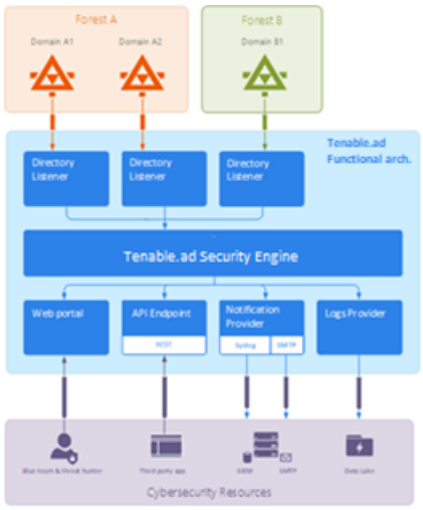
Tenable Identity Exposure verwendet ein normales Benutzerkonto ohne Administratorrechte, um für die Sicherheitsüberwachungsfunktion eine Verbindung zu Standard-APIs herzustellen.

Tenable Identity Exposure verwendet die Replikationsmechanismen von Active Directory zum Abrufen der relevanten Informationen. Dies verbraucht nur wenig Bandbreite zwischen dem PDC der einzelnen Domänen und dem Verzeichnis-Listener von Tenable Identity Exposure.

Um Sicherheitsvorfälle effizient mithilfe von Indicators of Attack zu erkennen, nutzt Tenable Identity Exposure die Informationen der Ereignisablaufverfolgung für Windows (ETW) und die auf den einzelnen Domänencontrollern verfügbaren Replikationsmechanismen. Zur Erfassung dieser Informationen stellen Sie ein dediziertes Gruppenrichtlinienobjekt (GPO) mithilfe eines Skripts von Tenable Identity Exposure bereit, wie unter Indicators of Attack installieren beschrieben.

Dieses GPO aktiviert einen Ereignisprotokoll-Listener mit Windows EvtSubscribe-APIs auf allen Domänencontrollern. Dieser Listener schreibt auf das Systemvolume (SYSVOL), um das AD-Replikationsmodul und die Tenable Identity Exposure-Fähigkeit, SYSVOL-Ereignisse abzuhören, nutzen zu können. Das GPO erstellt für jeden Domänencontroller eine Datei im SYSVOL und leert deren Inhalt in regelmäßigen Abständen.

Zur Initiierung der Sicherheitsüberwachung muss Tenable Identity Exposure Standard-Verzeichnis-APIs von Microsoft kontaktieren.



Domänencontroller

Tenable Identity Exposure muss nur mit dem primären Domänencontrolleremulator (PDCe) über die in der Network Flow Matrix beschriebenen Netzwerkprotokolle kommunizieren.

Wenn mehrere Domänen oder Gesamtstrukturen überwacht werden, muss Tenable Identity Exposure den PDCe jeder Domäne erreichen. Für eine optimale Leistung empfiehlt Tenable, dass Tenable Identity Exposure in einem physischen Netzwerk in der Nähe des zu überwachenden PDCe gehostet wird.

Benutzerkonto

Tenable Identity Exposure verwendet zur Authentifizierung bei der überwachten Infrastruktur ein Benutzerkonto ohne Administratorrechte, um auf den Replikationsfluss zuzugreifen.

Ein einfacher Tenable Identity Exposure-Benutzer kann auf alle erfassten Daten zugreifen. Tenable Identity Exposure greift nicht auf geheime Attribute wie Anmeldeinformationen, Passwort-Hashes oder Kerberos-Schlüssel zu.

Tenable empfiehlt, ein Dienstkonto zu erstellen, das Mitglied der Gruppe „Domänenbenutzer“ ist und die folgenden Anforderungen erfüllt:

- Das Dienstkonto befindet sind in der überwachten Hauptdomäne.
- Das Dienstkonto befindet sich in einer beliebigen Organisationseinheit (OU), vorzugsweise in derjenigen, in der Sie andere Sicherheitsdienstkonten erstellen.

- Das Dienstkonto hat eine Standard-Benutzergruppenmitgliedschaft (z. B. Mitglied der AD-Standardgruppe „Domänenbenutzer“).

Bevor Sie beginnen

- Informieren Sie sich über die Einschränkungen und potenziellen Auswirkungen der Installation von IoAs, wie unter Technische Änderungen und potenzielle Auswirkungen beschrieben.
- Überprüfen Sie, ob auf dem DC die PowerShell-Module für Active Directory und GroupPolicy installiert und verfügbar sind.
- Überprüfen Sie, ob auf dem DC die Funktion RSAT-DFS-Mgmt-Con der DFS-Tools (Verteiltes Dateisystem) aktiviert ist, sodass das Bereitstellungsskript den Replikationsstatus überprüfen kann (es kann kein GPO erstellt werden, während der DC eine Replikation ausführt).
- Tenable Identity Exposure empfiehlt, IoAs außerhalb der Spitzenzeiten zu installieren/aktualisieren, um Unterbrechungen Ihrer Plattform zu begrenzen.
- Berechtigungen überprüfen – Um IoAs zu installieren, benötigen Sie eine Benutzerrolle mit den folgenden Berechtigungen:
  - In **Datenentitäten** „Lesezugriff“ für:
    - Alle Indicators of Attack
    - Alle Domänen
  - In **Schnittstellenentitäten** Zugriff für:
    - Verwaltung > System > Konfiguration
    - Verwaltung > System > Konfiguration > Anwendungsdienste > Indicators of Attack
    - Verwaltung > System > Konfiguration > Anwendungsdienste > Indicators of Attack > Installationsdatei herunterladen

  Weitere Informationen zu rollenbasierten Berechtigungen finden Sie unter Berechtigungen für eine Rolle festlegen.

Siehe auch

- Indicators of Attack installieren
- Indicators of Attack-Installationsskript
- Technische Änderungen und potenzielle Auswirkungen
- Microsoft Sysmon installieren, ein Windows-Systemtool, das einige der Indicators of Attack von Tenable Identity Exposure benötigen, um relevante Systemdaten abzurufen.
- Problembehebung bei Indicators of Attack

Indicators of Attack installieren

Erforderliche Benutzerrolle: Organisationsbenutzer mit der Berechtigung, die Konfiguration der Indicators of Attack in Tenable Identity Exposure zu ändern. Weitere Informationen finden Sie unter Berechtigungen für eine Rolle festlegen.

Für das Tenable Identity Exposure-Modul „Indicators of Attack" (IoA) müssen Sie ein PowerShell-Installationsskript mit einem Administratorkonto ausführen, das ein neues Gruppenrichtlinienobjekt (GPO) erstellen und mit einer Organisationseinheit (OU) verknüpfen kann. Sie können dieses Skript auf einem beliebigen Computer ausführen, der Ihrer von Tenable Identity Exposure überwachten Active Directory-Domäne beigetreten ist und der Domänencontroller über das Netzwerk erreichen kann.

Sie müssen dieses Installationsskript nur einmal in jeder AD-Domäne ausführen, da das erstellte GPO den Event-Listener automatisch auf alle vorhandenen und neuen Domänencontroller (DC) anwendet.

Wenn Sie die Option „Automatische Updates" aktivieren, muss außerdem das Installationsskript nicht erneut ausgeführt werden, selbst wenn Sie die IoA-Konfiguration ändern.

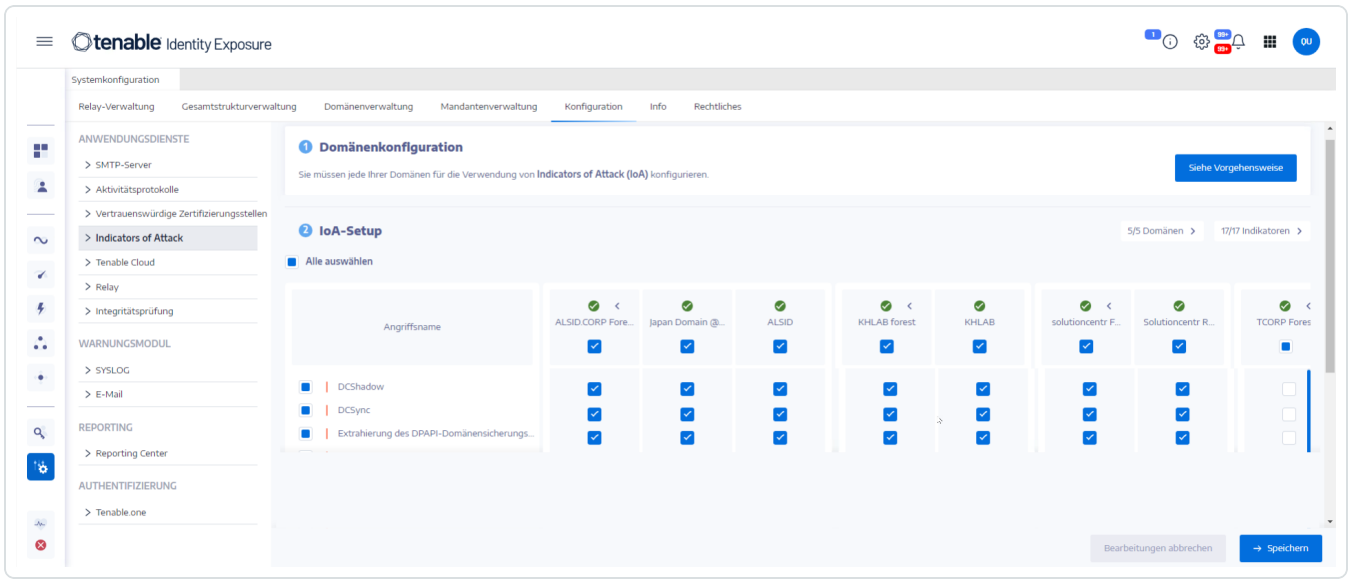
So konfigurieren Sie Domänen für IoAs:

1. Klicken Sie in Tenable Identity Exposure in der linken Menüleiste auf **System** und dann auf die Registerkarte **Konfiguration**.

   Der Fensterbereich **Konfiguration** wird angezeigt.

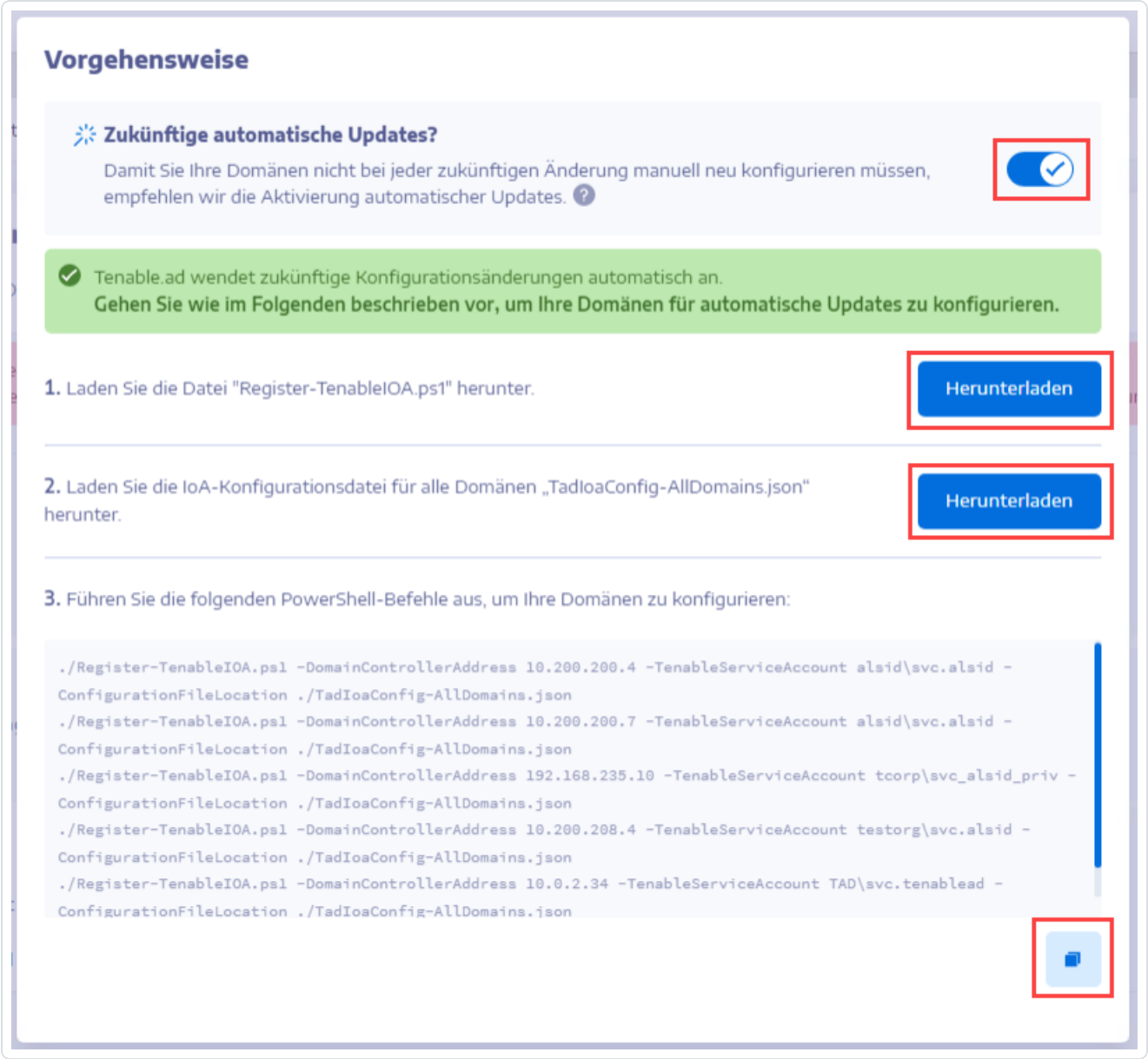
2. Klicken Sie auf **Indicators of Attack**.

   Das IoA-Konfigurationsfenster wird angezeigt.



3. Klicken Sie unter **(1) Domänenkonfiguration** auf **Siehe Vorgehensweise**.

   Ein Verfahrensfenster wird geöffnet.



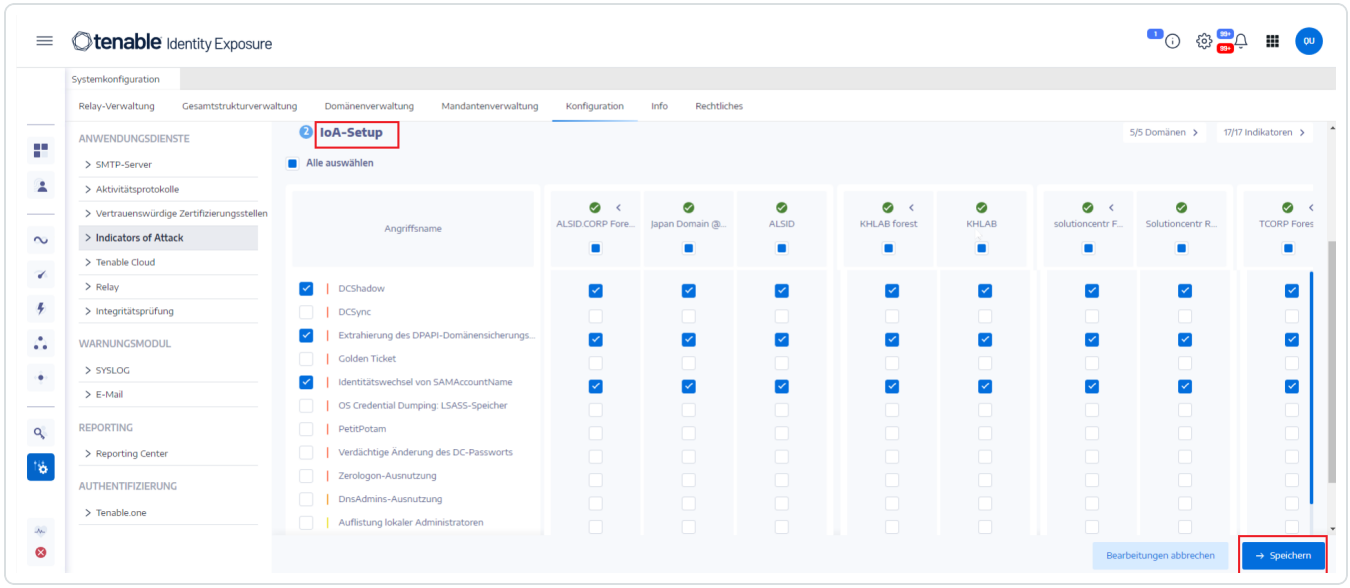
4. Unter **Zukünftige automatische Updates?**:
    - Die Standardoption **Aktivieren** ermöglicht es Tenable Identity Exposure, Ihre IoA-Konfiguration automatisch zu aktualisieren, wenn Sie sie in Zukunft in Tenable Identity Exposure ändern. Damit ist auch eine kontinuierliche Sicherheitsanalyse gewährleistet.
    - Wenn Sie diese Option deaktivieren, werden Sie in einer Meldung aufgefordert, sie zu aktivieren, um zukünftige automatische Updates zu erhalten. Klicken Sie auf **Siehe Vorgehensweise** und schalten Sie die Option auf **Aktivieren** um.

5. Klicken Sie auf **Herunterladen**, um das Skript herunterzuladen, das für jede Domäne ausgeführt werden soll (`Register-TenableIOA.ps1`).
6. Klicken Sie auf **Herunterladen**, um die Konfigurationsdatei für die Domänen herunterzuladen (`TadIoaConfig-AllDomains.json`).
7. Klicken Sie auf , um den PowerShell-Befehl zum Konfigurieren Ihrer Domänen zu kopieren.
8. Klicken Sie auf eine Stelle außerhalb des Verfahrensfensters, um dieses zu schließen.
9. Öffnen Sie ein PowerShell-Terminal mit Administratorrechten und führen Sie die Befehle aus, um Ihre Domänencontroller für IoAs zu konfigurieren.

> **Hinweis**: Das Dienstkonto, das Sie zum Installieren von IoAs und zum Abfragen der Domänen verwenden, muss im GPO-Ordner über Schreibberechtigungen in Tenable Identity Exposure (früher Tenable.ad) verfügen. Das Installationsskript fügt diese Berechtigung automatisch hinzu. Wenn Sie diese Berechtigung entfernen, zeigt Tenable Identity Exposure eine Fehlermeldung an, und automatische Updates funktionieren nicht mehr. Weitere Informationen finden Sie unter Indicators of Attack-Installationsskript.

So richten Sie Ihre IoAs ein:

1. Wählen Sie im IoA-Konfigurationsfenster unter **IoA-Setup** die IoAs aus, die Sie in Ihrer Konfiguration verwenden möchten.

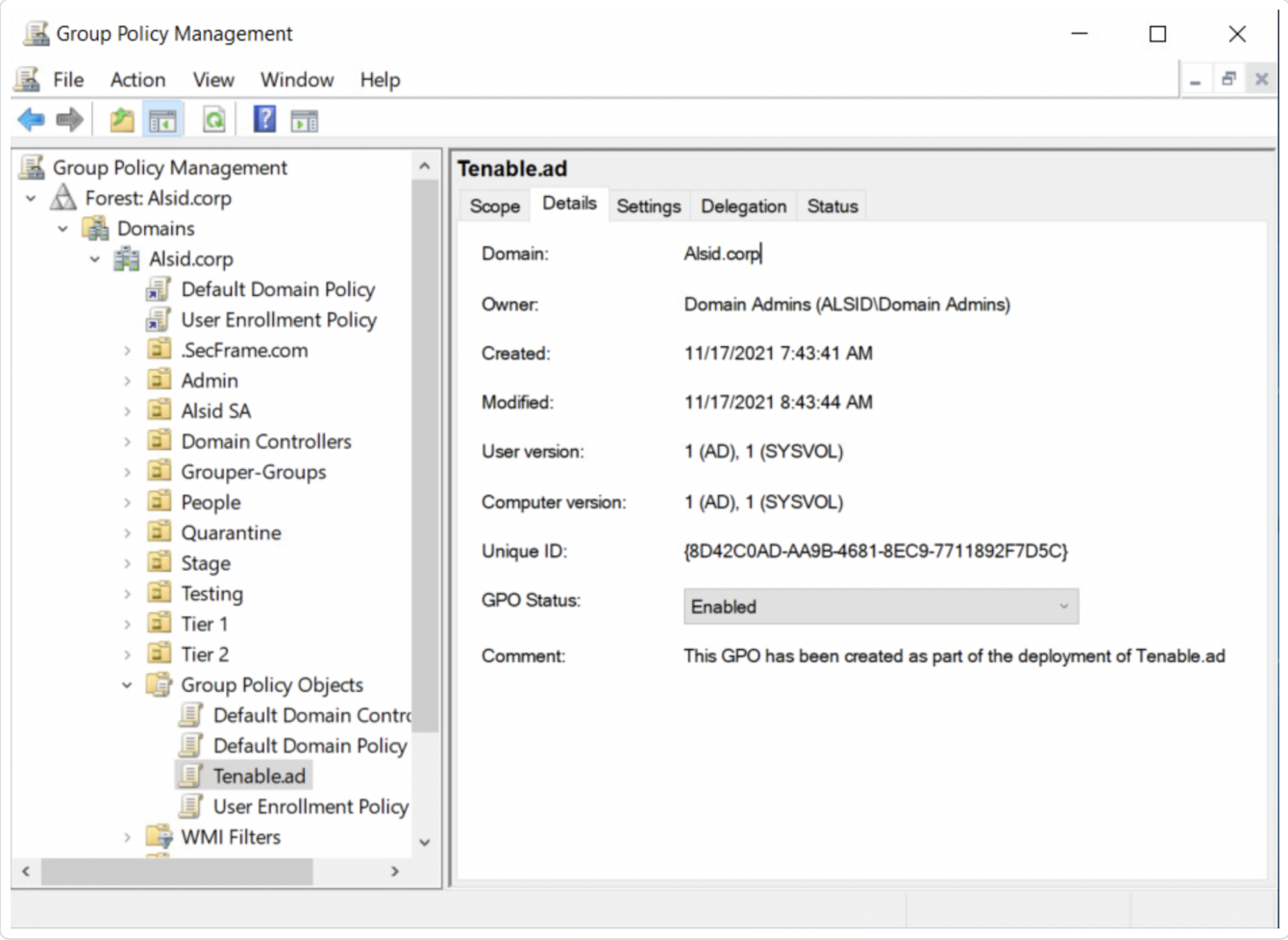


> **Tipp**: Der Indicator of Attack (IoA) **Zerologon-Ausnutzung** stammt aus dem Jahr 2020. Wenn auf allen Ihren Domänencontrollern (DCs) innerhalb der letzten drei Jahre Updates installiert wurden, sind sie vor dieser Schwachstelle geschützt. Informationen über die erforderlichen Patches zum Absichern Ihrer DCs gegen diese Schwachstelle finden Sie im Artikel Sicherheitsanfälligkeit in Netlogon bezüglich Rechteerweiterungen von Microsoft. Nachdem Sie die Sicherheit Ihrer DCs bestätigt haben, können Sie diesen IoA bedenkenlos deaktivieren, um unnötige Warnungen zu vermeiden.

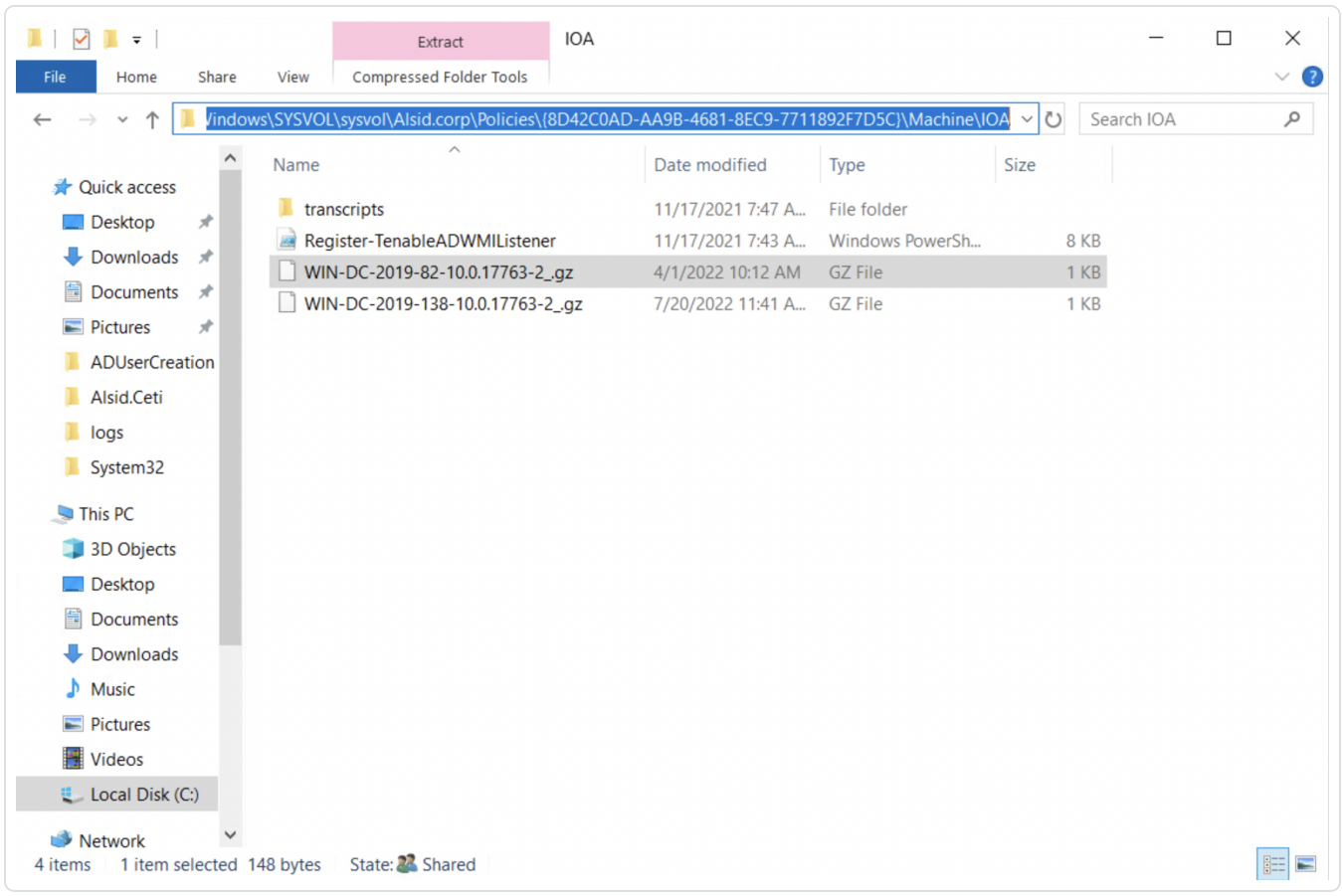
2. Klicken Sie auf **Speichern**.
    - Wenn Sie **Zukünftige automatische Updates** aktiviert haben, speichert Tenable Identity Exposure Ihre neue Konfiguration und aktualisiert sie automatisch. Warten Sie einige Minuten, bis diese Aktualisierung wirksam wird.
    - Wenn Sie **Zukünftige automatische Updates** nicht aktiviert haben, wird ein Verfahrensfenster angezeigt, das Sie anleitet (So konfigurieren Sie Domänen für IoAs:).

So überprüfen Sie die IoA-Installation:

1. Überprüfen Sie in der Gruppenrichtlinienverwaltung, ob das neue Tenable Identity Exposure-GPO vorhanden und mit der OE `Domänencontroller` verknüpft ist:



2. Wechseln Sie zum Pfad `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` und überprüfen Sie, ob die `.gz`-Datei für **alle Domänencontroller** vorhanden ist, bevor Sie die IoAs testen:



So prüfen Sie die Zugriffsberechtigung „Schreiben“ für das Tenable Identity Exposure-Dienstkonto:

1. Gehen Sie im Datei-Manager zu `\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\`.
2. Klicken Sie mit der rechten Maustaste auf den Ordner „IOA“ und wählen Sie **Eigenschaften** aus.
3. Wählen Sie die Registerkarte **Sicherheit** aus und klicken Sie auf **Erweitert**.
4. Klicken Sie auf die Registerkarte **Effektiver Zugriff**.
5. Klicken Sie auf **Einen Benutzer auswählen**.
6. Geben Sie `<TENABLE-SERVICE-ACCOUNT-NAME>` ein und klicken Sie auf **OK**.
7. Klicken Sie auf **Effektiven Zugriff anzeigen**.
8. Überprüfen Sie, ob die Berechtigung „Schreiben“ aktiviert ist.

Alternativ können Sie PowerShell verwenden:

- Führen Sie die folgenden Befehle aus:

```
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>
```

So kalibrieren Sie IoAs

Um falsch positive Angriffe oder die mangelnde Erkennung legitimer Angriffe zu vermeiden, müssen Sie Ihre IoAs entsprechend Ihrer Umgebung kalibrieren, indem Sie sie an die Größe Ihres Active Directory anpassen, bekannte Tools auf die Whitelist setzen usw.

1. Informationen zu den Optionen und empfohlenen Werten zur Auswahl finden Sie im Tenable Identity Exposure – Referenzhandbuch zu Indicators of Attack.
2. Wenden Sie im Sicherheitsprofil die Optionen und Werte auf jeden IoA an, wie in Indikator anpassenbeschrieben.

Fehlerbehebung

Während der Bereitstellung können folgende Fehlermeldungen angezeigt werden:

Meldung	Behebung
„Tenable Identity Exposure kann nicht in die Konfigurationsdatei schreiben, da der Zielordner `<Zielorder>` nicht vorhanden ist. Dies weist darauf hin, dass die Bereitstellung des IoA-Moduls möglicherweise fehlgeschlagen ist.“	Deinstallieren Sie das Skript und klicken Sie auf „Siehe Vorgehensweise“, um Anweisungen zur Neuinstallation des Skripts zu erhalten.
„Tenable Identity Exposure konnte nicht in die Konfigurationsdatei in `<Zieldatei>` schreiben, um sie zu aktualisieren. Dies kann daran liegen,	• Stellen Sie sicher, dass außer dem IoA-Modul kein anderer Prozess die Konfigurationsdatei verwendet. • Überprüfen Sie, ob das Dienstkonto

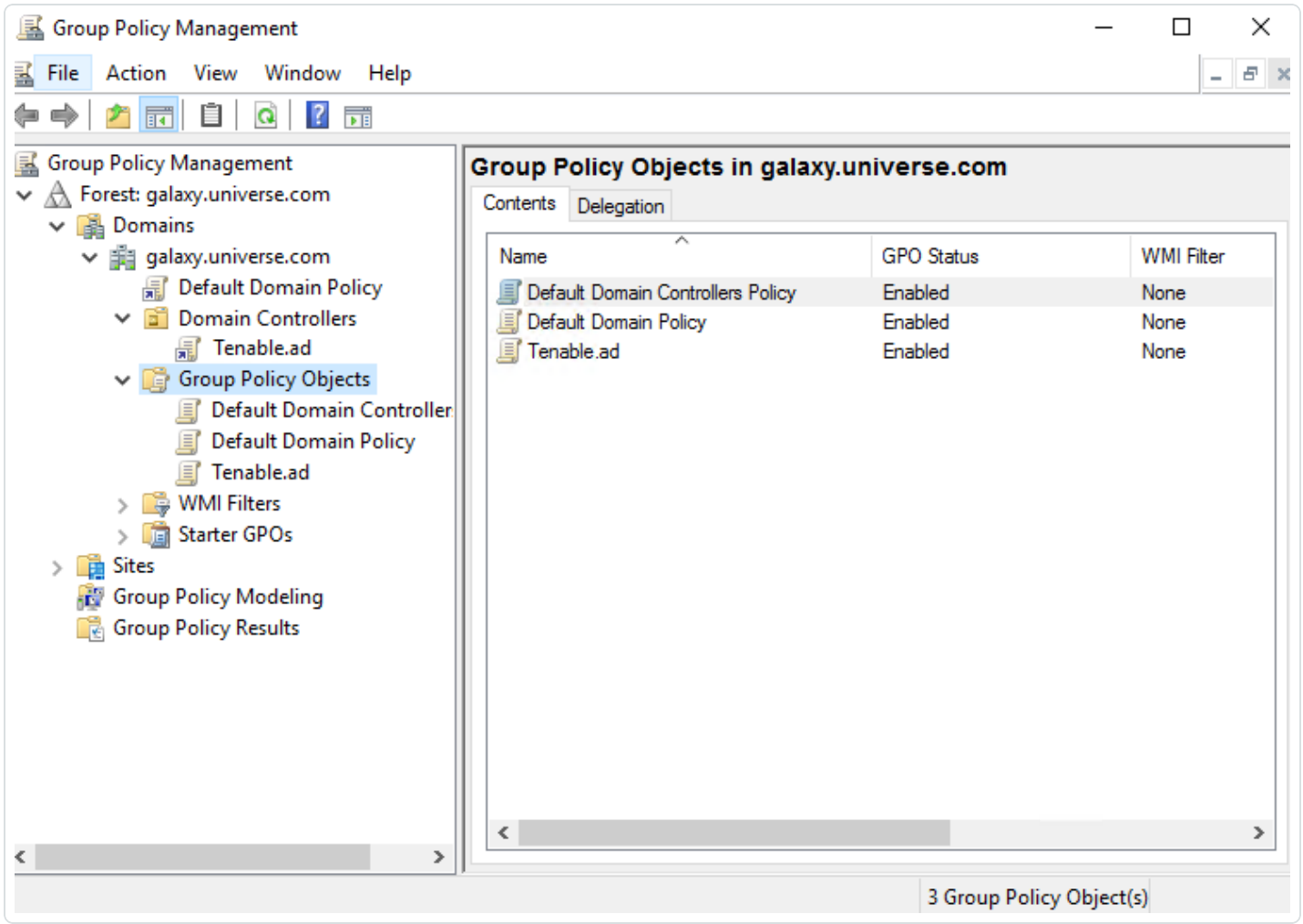
dass ein anderer Prozess die Datei sperrt oder dass Berechtigungen geändert wurden.“	berechtigt ist, den Dateiinhalt zu ändern. • Wenn Sie dem Dienstkonto keine Berechtigung erteilen möchten, deaktivieren Sie den Umschalter „Automatische Updates“ und klicken Sie auf „Siehe Vorgehensweise“, um Anweisungen zum Durchführen eines manuellen Updates zu erhalten, wenn Sie Ihre IoA-Konfiguration ändern.
„Der Zielordner `<Zielordner>` enthält eine Version von Tenable Identity Exposure, die keine automatischen Updates ausführen kann.“	Das derzeit installierte Skript ist eine alte Version, die WMI verwendet. Deinstallieren Sie die aktuelle Version, laden Sie ein neues Installationsskript herunter und führen Sie dieses Skript aus.
„Bei der Bereitstellung der Konfigurationsdatei ist ein unerwarteter Fehler aufgetreten.“	Deinstallieren Sie das Skript und klicken Sie auf „Siehe Vorgehensweise“, um Anweisungen zur Neuinstallation des Skripts zu erhalten. Wenn dies nicht funktioniert, wenden Sie sich an Ihren Kundendienstmitarbeiter.

Weitere Informationen finden Sie in folgenden Ressourcen:

- Indicators of Attack-Installationsskript
- Technische Änderungen und potenzielle Auswirkungen
- Antivirus-Erkennung
- Priorität der erweiterten Überwachungsrichtlinienkonfiguration

Indicators of Attack-Installationsskript

Nachdem Sie die Indicators of Attack (IoA)-Installationsdatei heruntergeladen und ausgeführt haben, erstellt das IoA-Skript in der Active Directory (AD)-Datenbank ein neues Gruppenrichtlinienobjekt (GPO) mit dem Standardnamen `Tenable.ad`. Das System verknüpft das Tenable Identity Exposure-GPO nur mit der Organisationseinheit (OU) der Domänencontroller, die alle Domänencontroller (DCs) enthält. Die neue Richtlinie führt automatisch eine Replikation zwischen allen DCs mit dem GPO-Mechanismus durch.



Installationsskript (Tenable Identity Exposure Version 3.29)

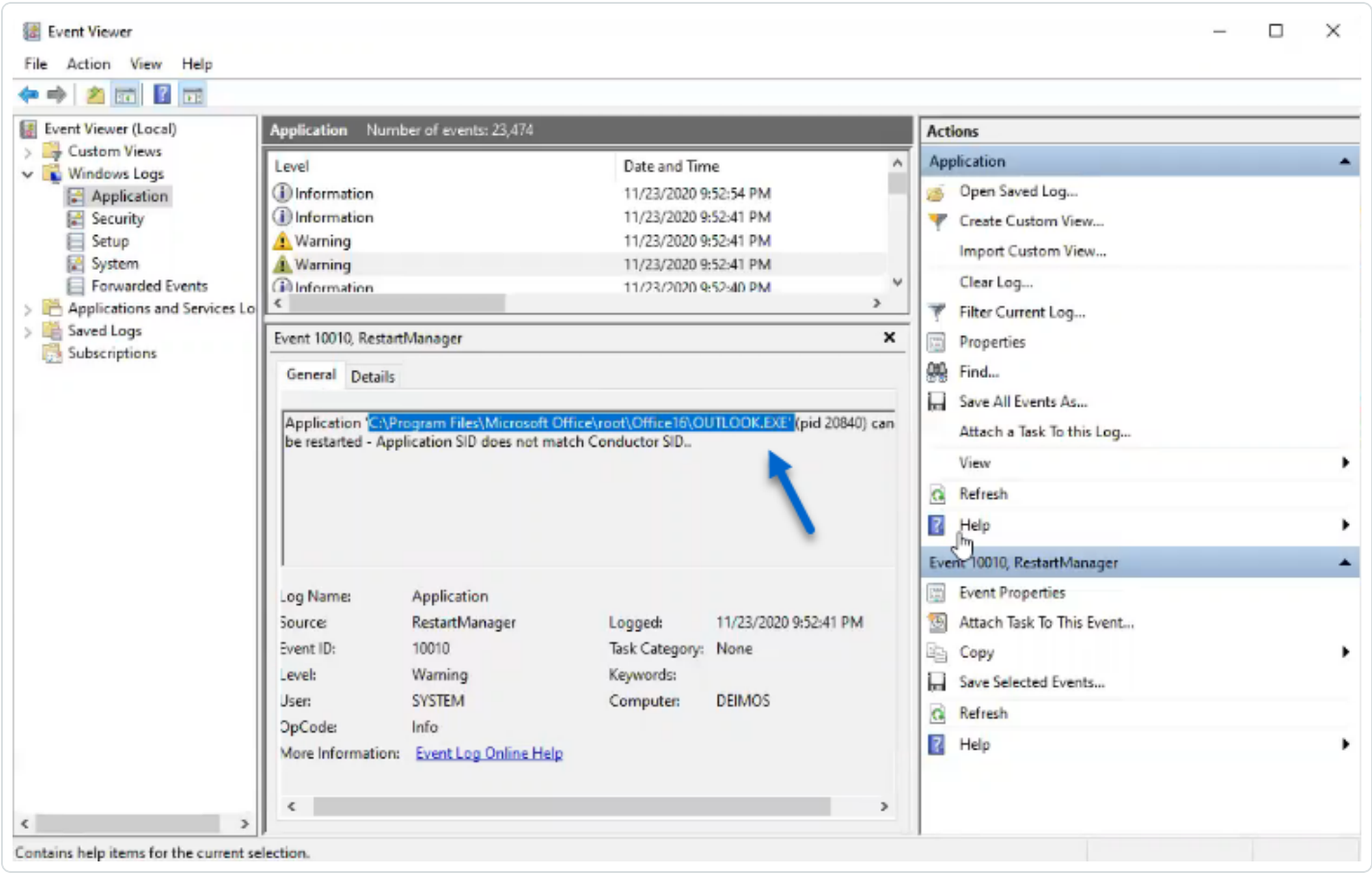
Das GPO enthält PowerShell-Skripts, die alle DCs lokal ausführen, um relevante Daten wie folgt zu erfassen:

- Das Skript konfiguriert mithilfe der Windows EvtSubscribe-API einen Ereignisprotokoll-Listener auf jedem Domänencontroller. Das Skript erstellt ein Abonnement für jeden erforderlichen Ereignisprotokollkanal, wie in der Konfigurationsdatei `TenableADEventsListenerConfiguration.json` angegeben, indem es für jedes übereinstimmende Ereignisprotokoll eine Anfrage und einen von EvtSubscribe ausgelösten Rückruf sendet.
- Der Ereignis-Listener erhält Ereignisprotokolle und puffert sie, bevor er sie in regelmäßigen Abständen in eine Datei leert, die auf einer Netzwerkfreigabe namens „Sysvol" gespeichert ist. Jeder DC leert seinen Inhalt in eine einzige Sysvol-Datei, die erfasste Ereignisse speichert und sie auf andere Domänencontroller repliziert.
- Das Skript erstellt auch einen WMI-Consumer, um sicherzustellen, dass dieser Mechanismus persistent ist. Hierzu wird der Ereignisabonnent beim Neustart eines DC erneut registriert. WMI benachrichtigt den Consumer jedes Mal, wenn ein DC neu gestartet wird, damit der Consumer den Ereignis-Listener erneut registrieren kann.
- An diesem Punkt findet eine DFS-Replikation (Distributed File System, Verteiltes Dateisystem) statt, bei der Dateien automatisch zwischen Domänencontrollern synchronisiert werden. Die Tenable Identity Exposure-Plattform lauscht auf eingehenden DFS-Replikationsdatenverkehr und nutzt diese Daten, um Ereignisse zu sammeln, eine Sicherheitsanalyse auszuführen und IoA-Warnungen zu generieren.

Lokaler Datenabruf

Windows-Ereignisprotokolle zeichnen alle Ereignisse auf, die im Betriebssystem und den Anwendungen eintreten. Ereignisprotokolle basieren auf einem Framework von Komponenten, die in Windows integriert sind.

Mithilfe der EvtSubscribe-API erfasst der IoA-Ereignisprotokoll-Listener von Tenable Identity Exposure nur nützliche Datensegmente von Ereignisprotokollen in Form von Einfügezeichenfolgen, die aus den Ereignisprotokollen extrahiert werden. Tenable Identity Exposure schreibt diese Einfügezeichenfolgen in eine Datei, die im Sysvol-Ordner gespeichert ist, und repliziert sie über das DFS-Modul. Dies erlaubt es Tenable Identity Exposure, genau die richtige Menge an Sicherheitsdaten aus Ereignisprotokollen zu sammeln, um eine Sicherheitsanalyse auszuführen und Angriffe zu erkennen.



IoA-Skript – Zusammenfassung

Die folgende Tabelle enthält eine Übersicht über die Bereitstellung des Tenable Identity Exposure-Skripts.

Schritte	Beschreibung	Beteiligte Komponente	Technische Aktion
1	Tenable Identity Exposure IoA-Bereitstellung registrieren	GPO-Verwaltung	Erstellt das GPO `Tenable.ad` (Standardname) und verknüpft es mit der OU der Domänencontroller.
2	Tenable Identity	Lokales	Jeder DC erkennt das neue anzuwendende GPO,

	Exposure IoA-Bereitstellung auf DC starten	DC-System	abhängig von der AD-Replikation und den Aktualisierungsintervallen der Gruppenrichtlinie.
3	Status der erweiterten Protokollierungsrichtlinie kontrollieren	Lokales DC-System	Das System aktiviert die erweiterte Protokollierungsrichtlinie durch Festlegen des Registrierungsschlüssels `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`.
4	Lokale Protokollierungsrichtlinie aktualisieren	Lokales DC-System	Abhängig von den zu erkennenden IoAs generiert und aktiviert Tenable Identity Exposure dynamisch bestimmte Überwachungsrichtlinien. Diese Richtlinie deaktiviert keine vorhandenen Protokollierungsrichtlinien, sondern erweitert sie lediglich bei Bedarf. Wenn ein Konflikt erkannt wird, wird das GPO-Installationsskript beendet und die folgende Meldung angezeigt: „Tenable Identity Exposure requires the audit policy ... but the current AD configuration prevents its usage.“
5	Event-Listener und WMI-Consumer registrieren	Lokales DC-System	Das System registriert das im GPO enthaltene Skript und führt es aus. Dieses Skript führt einen PowerShell-Prozess aus, um Ereignisprotokolle mit der EvtSubscribe-API zu abonnieren und eine Instanz von `ActiveScriptEventConsumer` für Persistenzzwecke zu erstellen. Tenable Identity Exposure verwendet diese Objekte zum Empfangen und Speichern von Ereignisprotokollinhalten.
6	Ereignisprotokollmeldungen erfassen	Lokales DC-System	Tenable Identity Exposure erfasst relevante Ereignisprotokollmeldungen, puffert sie regelmäßig und speichert sie in Dateien (eine pro DC), die im Sysvol-Ordner gespeichert sind, der dem Tenable Identity Exposure-GPO zugeordnet ist (`...{GPO_GUID}\Machine\IOA<DC-Name>`).

7	Dateien in den angegebenen DC-SYSVOL-Ordner replizieren	Active Directory	Das AD repliziert die Dateien unter Verwendung von DFS in der Domäne und insbesondere im deklarierten DC. Die Tenable Identity Exposure-Plattform erhält eine Benachrichtigung für jede Datei und liest ihren Inhalt.
8	Diese Dateien überschreiben	Active Directory	Jeder DC schreibt die regelmäßig gepufferten Ereignisse automatisch und kontinuierlich in dieselbe Datei.

Installationsskript (Tenable Identity Exposure Version 3.19.11 und früher)

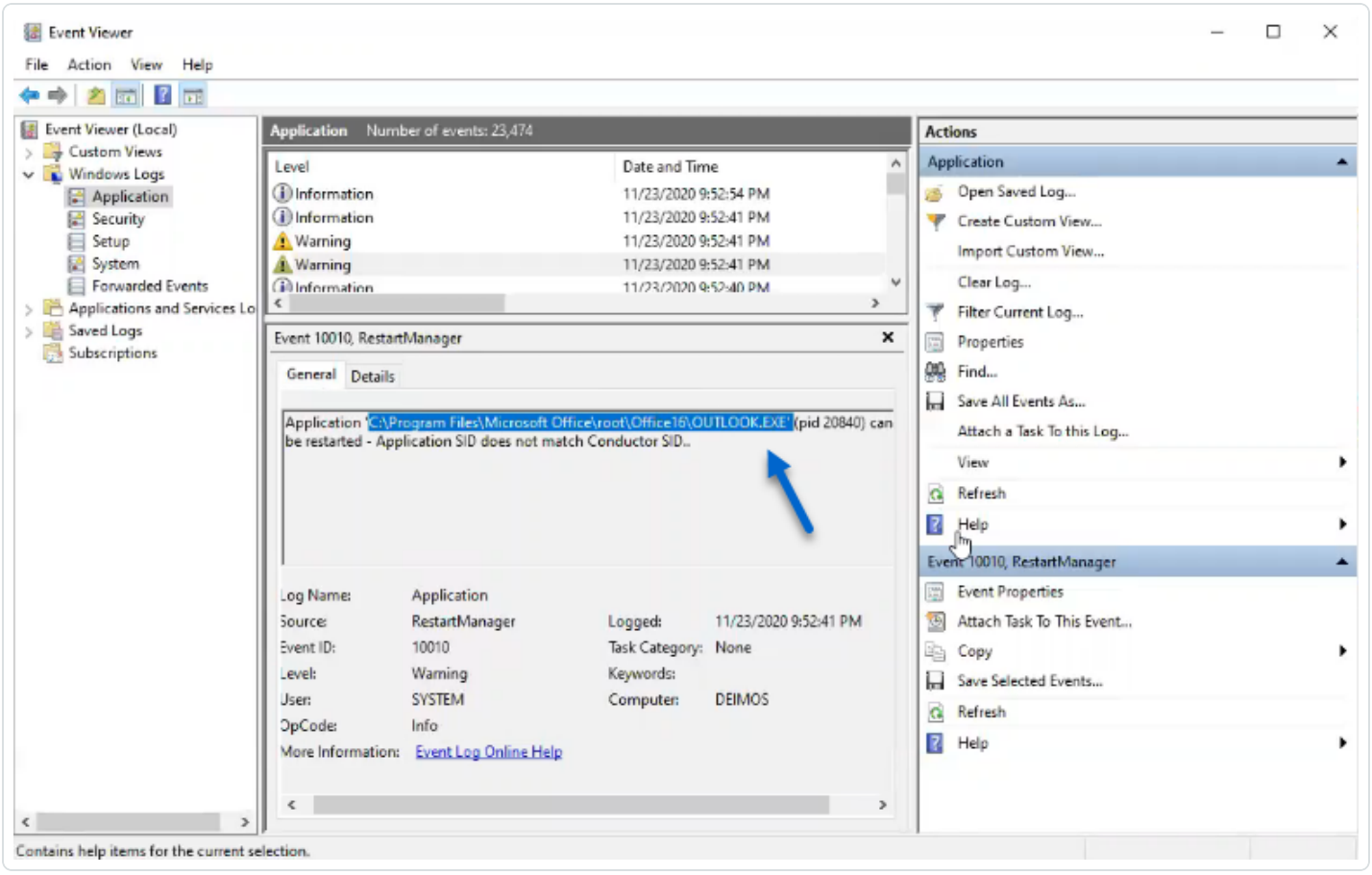
Das GPO enthält PowerShell-Skripts, die alle DCs lokal ausführen, um relevante Daten wie folgt zu erfassen:

- Die Skripts konfigurieren einen Ereignis-Watcher und einen WMI-Producer/Consumer (Windows-Verwaltungsinstrumentation) im Arbeitsspeicher des Computers. WMI ist eine Windows-Komponente, die Ihnen Informationen über den Status von lokalen oder Remote-Computersystemen liefert.
- Der Ereignis-Watcher erhält Ereignisprotokolle und puffert sie regelmäßig, bevor er sie in eine Datei leert, die auf einer Netzwerkfreigabe namens „Sysvol" gespeichert ist. Jeder DC leert seinen Inhalt in eine einzige Sysvol-Datei, die erfasste Ereignisse speichert und sie auf andere Domänencontroller repliziert.
- Der WMI-Consumer macht diesen Mechanismus persistent, indem er den Ereignis-Watcher erneut registriert, wenn ein DC neu gestartet wird. Der Producer wird aktiviert und benachrichtigt den Consumer bei jedem Neustart eines DC. Der Consumer registriert dann den Ereignis-Watcher erneut.
- An diesem Punkt findet eine DFS-Replikation (Verteiltes Dateisystem) statt, bei der Dateien automatisch zwischen Domänencontrollern synchronisiert werden. Die Tenable Identity Exposure-Plattform lauscht auf eingehenden DFS-Replikationsdatenverkehr und nutzt diese Daten, um Ereignisse zu sammeln, eine Sicherheitsanalyse auszuführen und IoA-Warnungen zu generieren.

Lokaler Datenabruf

Windows-Ereignisprotokolle zeichnen alle Ereignisse auf, die im Betriebssystem und den Anwendungen eintreten. Ereignisprotokolle mit der Bezeichnung „Ereignisablaufverfolgung für Windows“ (ETW) basieren auf einem Framework von Komponenten, die in Windows integriert sind. ETW befindet sich im Kernel und erzeugt Daten, die lokal auf DCs gespeichert sind und nicht von AD-Protokollen repliziert werden.

Mithilfe des WMI-Moduls erfasst Tenable Identity Exposure nur nützliche ETW-Datensegmente in Form von Einfügezeichenfolgen, die aus den Ereignisprotokollen extrahiert werden. Tenable Identity Exposure schreibt diese Einfügezeichenfolgen in eine Datei, die im Sysvol-Ordner gespeichert ist, und repliziert sie über das DFS-Modul. Dies erlaubt es Tenable Identity Exposure, genau die richtige Menge an Sicherheitsdaten von ETW zu sammeln, um eine Sicherheitsanalyse auszuführen und Angriffe zu erkennen.



IoA-Skript – Zusammenfassung

Die folgende Tabelle enthält eine Übersicht über die Bereitstellung des Tenable Identity Exposure-Skripts.

Schritte	Beschreibung	Beteiligte Komponente	Technische Aktion
1	Tenable Identity Exposure IoA-Bereitstellung registrieren	GPO-Verwaltung	Erstellt das GPO `Tenable.ad` (Standardname) und verknüpft es mit der OU der Domänencontroller.
2	Tenable Identity Exposure IoA-Bereitstellung auf DC starten	Lokales DC-System	Jeder DC erkennt das neue anzuwendende GPO, abhängig von der AD-Replikation und den Aktualisierungsintervallen der Gruppenrichtlinie.
3	Event-Watcher und WMI-Producer/Consumer registrieren	Lokales DC-System	Das System registriert eine sofortige Aufgabe und führt sie aus. Dieses Aufgabe führt einen PowerShell-Prozess aus, um Instanzen der folgenden Klassen zu erstellen: `ManagementEventWatcher` und `ActiveScriptEventConsumer`. Tenable Identity Exposure verwendet diese Objekte zum Empfangen und Speichern von ETW-Meldungen.
4	Status der erweiterten Protokollierungsrichtlinie kontrollieren	Lokales DC-System	Das System aktiviert die erweiterte Protokollierungsrichtlinie durch Festlegen des Registrierungsschlüssels `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`.
5	Lokale Protokollierungsrichtlinie aktualisieren	Lokales DC-System	Abhängig von den zu erkennenden IoAs generiert und aktiviert Tenable Identity Exposure dynamisch eine erweiterte Protokollierungsrichtlinie. Diese Richtlinie deaktiviert keine vorhandenen Protokollierungsrichtlinien, sondern erweitert sie

			lediglich bei Bedarf. Wenn ein Konflikt erkannt wird, wird das GPO-Installationsskript beendet und die folgende Meldung angezeigt: „Tenable Identity Exposure requires the audit policy ... but the current AD configuration prevents its usage.“
6	ETW-Meldungen erfassen	Lokales DC-System	Tenable Identity Exposure erfasst relevante ETW-Meldungen, puffert sie regelmäßig und speichert sie in Dateien (eine pro DC), die im Sysvol-Ordner gespeichert sind, der dem Tenable Identity Exposure-GPO zugeordnet ist (`...{GPO_GUID}\Machine\IOA<DC_name>`).
7	Dateien auf die Tenable Identity Exposure-Plattform replizieren	Active Directory	Das AD repliziert die Dateien unter Verwendung von DFS in der Domäne. Auch die Tenable Identity Exposure-Plattform erhält die Dateien.
8	Diese Dateien überschreiben	Active Directory	Jeder DC schreibt die regelmäßig gepufferten Ereignisse automatisch und kontinuierlich in dieselbe Datei.

Siehe auch

- Indicators of Attack and the Active Directory
- Indicators of Attack installieren
- Technische Änderungen und potenzielle Auswirkungen

Technische Änderungen und potenzielle Auswirkungen

Das Installationsskript für das Modul „Indicators of Attack“ (IoA) erstellt ein GPO, das die folgenden Änderungen transparent auf die überwachten DCs anwendet:

- Ein neues GPO mit dem Standardnamen „Tenable.ad“, das standardmäßig mit der Organisationseinheit (OU) des Domänencontrollers verknüpft ist.
- Änderung eines Registrierungsschlüssels zur Aktivierung der erweiterten Microsoft-Protokollierungsrichtlinie.
- Aktivierung einer neuen Ereignisprotokollrichtlinie, um Domänencontroller zu zwingen, die von IoAs benötigten ETW-Informationen zu generieren.

  > **Hinweis**: Die Ereignisprotokollrichtlinie ist obligatorisch, damit das ETW-Modul die von Tenable Identity Exposure benötigten Einfügezeichenfolgen generieren kann. Diese Richtlinie deaktiviert keine vorhandene Protokollierungsrichtlinie, sondern stellt eine Ergänzung dar. Im Fall eines Konflikts wird das Bereitstellungsskript mit einer Fehlermeldung beendet.

- Hinzufügung einer Schreibberechtigung für das Tenable Identity Exposure-Dienstkonto, das „automatische Updates“ der im GPO-Ordner gespeicherten IoA-Konfiguration zulässt.

Einschränkungen und potenzielle Auswirkungen

Das Modul **Indicators of Attack** (IoA) kann die folgenden Einschränkungen aufweisen:

- Das IoA-Modul stützt sich auf die ETW-Daten und arbeitet innerhalb der von Microsoft definierten Einschränkungen.
- Das installierte GPO muss über die gesamte Domäne repliziert werden und das GPO-Aktualisierungsintervall muss verstrichen sein, damit der Installationsprozess abgeschlossen wird. Während des Replikationszeitraums kann es zu falsch positiven und falsch negativen Ergebnissen kommen, obwohl Tenable Identity Exposure diesen Effekt minimiert, indem die Prüfungen im Modul „Indicators of Attack“ nicht sofort gestartet werden.
- Tenable nutzt die SYSVOL-Dateifreigabe, um ETW-Informationen von Domänencontrollern abzurufen. Da SYSVOL zu jedem Domänencontroller in der Domäne repliziert, ist während Zeiten mit sehr hoher Active Directory-Aktivität ein erheblicher Anstieg der Replikationsaktivität zu verzeichnen.

- Beim Replizieren von Dateien zwischen Domänencontrollern und Tenable Identity Exposure wird außerdem Netzwerkbandbreite verbraucht. Tenable Identity Exposure beschränkt diese Auswirkungen durch das automatische Entfernen der erfassten Dateien und beschränkt die Größe dieser Dateien (standardmäßig max. 500 MB).
- Probleme mit langsamer oder fehlerhafter DFS-Replikation (Distributed File System). Weitere Informationen finden Sie unter Entschärfung von DFS-Replikationsproblemen.

Siehe auch

- Indicators of Attack and the Active Directory
- Indicators of Attack installieren
- Indicators of Attack-Installationsskript
- Problembehebung bei Indicators of Attack

Angriffsszenarien (< V. 3.36)

Achtung: Diese Funktion zur Konfigurationsaktualisierung für Indicators of Attack ist für Tenable Identity Exposure-Versionen > 3.36 nicht mehr verfügbar.

Erforderliche Benutzerrolle: Organisationsbenutzer mit der Berechtigung, die Konfiguration der Indicators of Attack zu ändern.

Sie definieren ein Angriffsszenario, indem Sie die Arten von Angriffen auswählen, die Tenable Identity Exposure in bestimmten Domänen überwachen soll.

Bevor Sie beginnen

Um das Angriffsszenario ändern zu können, müssen Sie über eine Benutzerrolle mit den folgenden Berechtigungen verfügen:

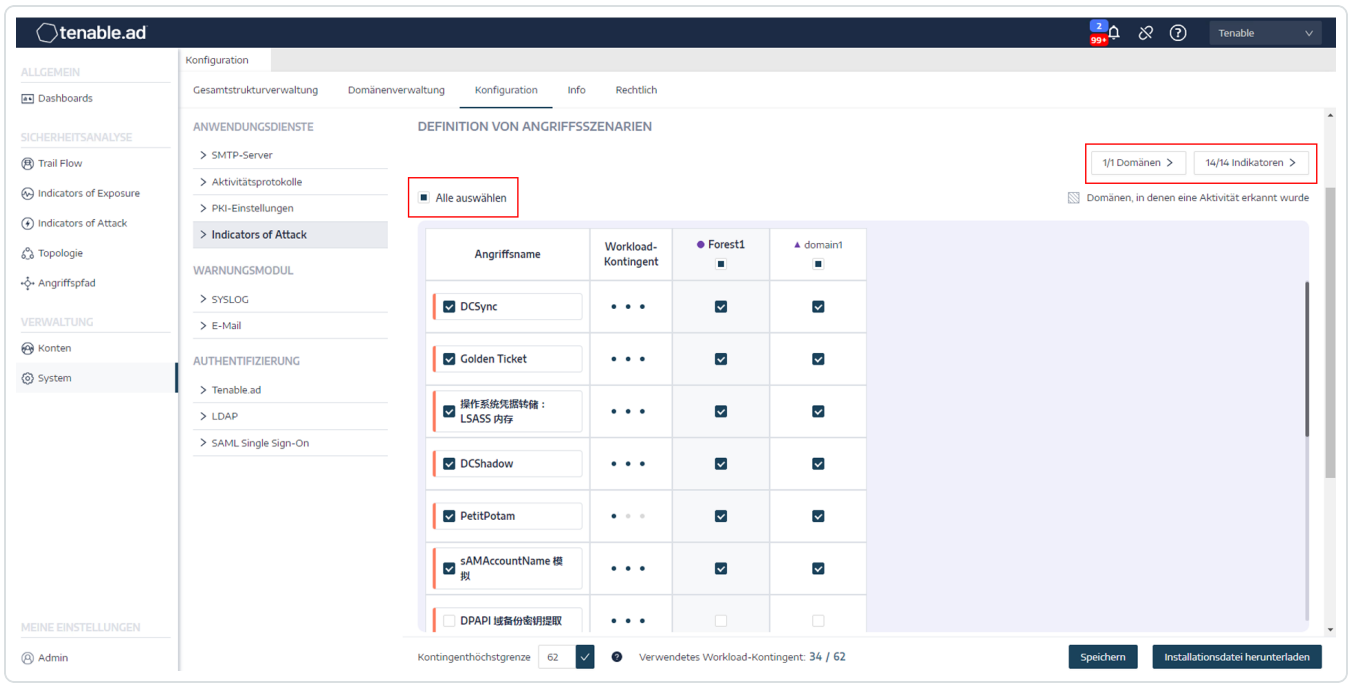
- In **Datenentitäten** „Lesezugriff“ für:
  - Alle Indicators of Attack
  - Alle Domänen
- In **Schnittstellenentitäten** Zugriff für:
  - Verwaltung > System > Konfiguration
  - Verwaltung > System > Konfiguration > Anwendungsdienste > Indicators of Attack
  - Verwaltung > System > Konfiguration > Anwendungsdienste > Indicators of Attack > Installationsdatei herunterladen

Weitere Informationen zu rollenbasierten Berechtigungen finden Sie unter Berechtigungen für eine Rolle festlegen.

So definieren Sie ein Angriffsszenario:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration** > **Indicators of Attack**.

   Der Bereich **Definition von Angriffsszenarien** wird geöffnet.



2. Wählen Sie unter **Angriffsname** den zu überwachenden Angriff aus.
3. Wählen Sie die Domäne aus, die auf den ausgewählten Angriff überwacht werden soll.
4. Optional können Sie eine der folgenden Möglichkeiten nutzen:
    - Klicken Sie auf **Alle auswählen**, um alle Domänen auf alle Angriffe zu überwachen.
    - Klicken Sie auf **n/n Domänen** oder **n/n Indikatoren**, um nach bestimmten Domänen zu filtern, die auf bestimmte Angriffe überwacht werden sollen.
5. Klicken Sie auf **Speichern**.

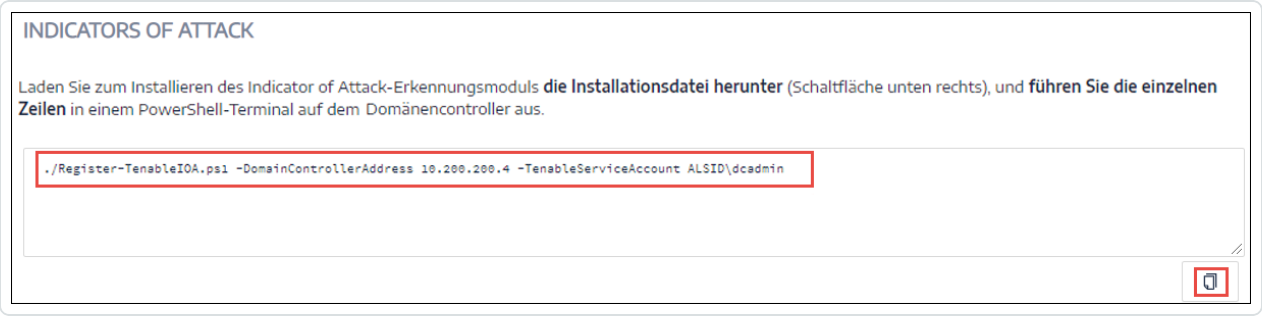
    Eine Bestätigungsmeldung informiert Sie, dass Tenable Identity Exposure den Aktivitätsstatus jedes Angriffs nach dem Speichern der Konfiguration löscht.
6. Klicken Sie auf **Bestätigen**.

    Eine Meldung bestätigt, dass Tenable Identity Exposure die Indicator of Attack-Konfiguration aktualisiert hat.
7. Klicken Sie auf **Installationsdatei herunterladen**.
8. Führen Sie die Installationsdatei aus, damit die neue Angriffskonfiguration wirksam wird:

a. Kopieren Sie die heruntergeladene Installationsdatei und fügen Sie sie auf dem DC in der überwachten Domäne ein.

b. Öffnen Sie als Administrator ein PowerShell-Terminal.

c. Kopieren Sie in Tenable Identity Exposure die Befehle unten im Fenster unter dem Abschnitt „Indicators of Attack“.



d. Fügen Sie im PowerShell-Fenster die Befehle zur Ausführung des Skripts ein.

Workload-Kontingent

Achtung: Die Workload-Kontingent-Funktion ist für Tenable Identity Exposure-Versionen > 3.36 nicht mehr verfügbar.

Erforderliche Benutzerrolle: Organisationsbenutzer mit der Berechtigung, das Workload-Kontingent zu bearbeiten.

Jedem Indicator of Attack in Tenable Identity Exposure ist ein Workload-Kontingent zugeordnet, das den Ressourcenbedarf für die Analyse der Daten eines Angriffs berücksichtigt.

Tenable Identity Exposure berechnet das Workload-Kontingent, um die Anzahl der gleichzeitig ausgeführten Indicators of Attack (IoAs) zu begrenzen. Das wirkt sich auf die Bandbreiten- und CPU-Nutzung für die Ereignisgenerierung auf Domänencontrollern aus.

Nachdem Sie den Grenzwert für das Workload-Kontingent geändert haben, gehen Sie wie folgt vor:

- Erhöhung: Überwachen Sie die Statistiken nach der Erhöhung, um eine komfortable Marge zu gewährleisten.
- Verringerung: Deaktivieren Sie einige IoAs, um unter diesem Kontingent zu bleiben. Das verringert die Sicherheitsabdeckung gegen Angriffe.

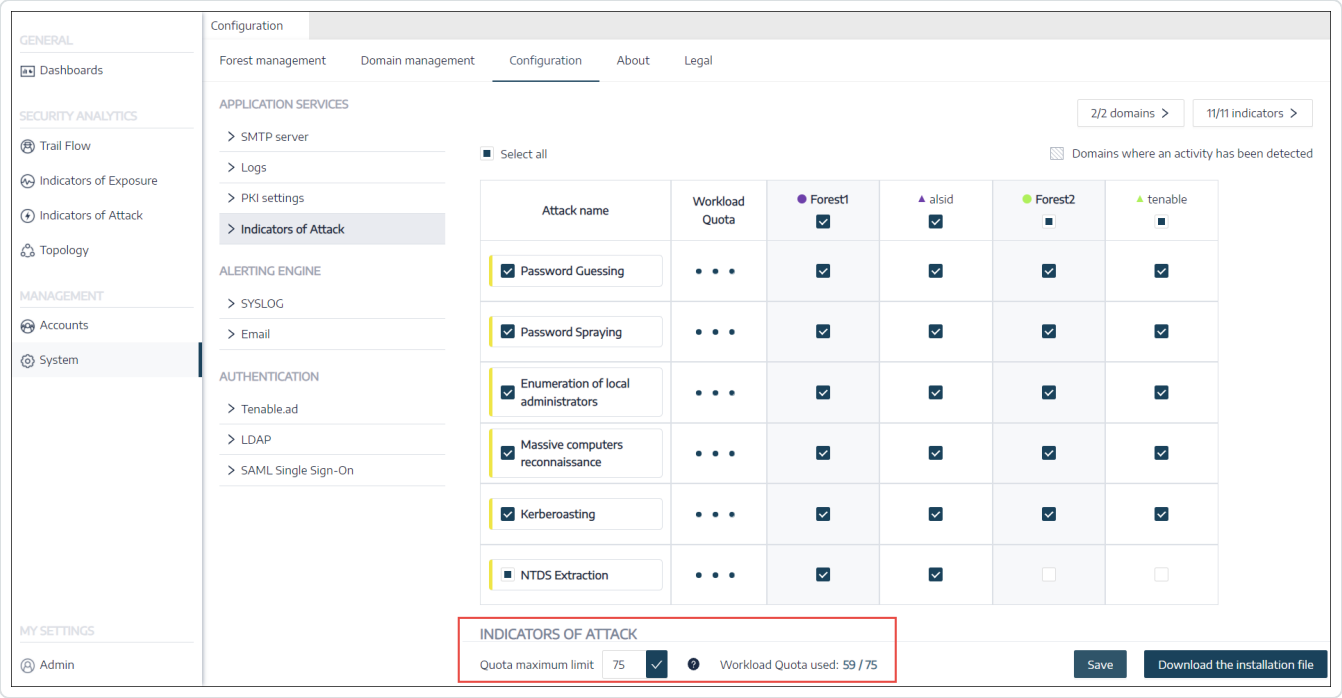
So ändern Sie das Workload-Kontingent:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration** > **Indicators of Attack**.

   Der Fensterbereich **IoA-Konfiguration** wird geöffnet.

2. Wählen Sie die gewünschten IoAs für Ihre Konfiguration aus.

3. Geben Sie unter **Indicators of Attack** im Feld **Kontingenthöchstgrenze** einen Wert für das Workload-Kontingent ein.



4. Klicken Sie auf das Häkchen neben dem von Ihnen eingegebenen Wert.

   Eine Meldung informiert Sie über die Auswirkungen der Änderung auf Tenable Identity Exposure.

   Hinweis: Wenn Sie eine Kontingenthöchstgrenze eingeben, die kleiner ist als die für die aktuelle Angriffskonfiguration erforderliche, müssen Sie die Anzahl der aktiven IoAs anpassen oder die Grenze erhöhen.

5. Klicken Sie auf **Bestätigen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Kontingenthöchstgrenze aktualisiert hat.

6. Klicken Sie auf **Speichern**.

   Eine Bestätigungsmeldung informiert Sie, dass Tenable Identity Exposure den Aktivitätsstatus jedes Angriffs nach dem Speichern der Konfiguration löscht.

7. Klicken Sie auf **Bestätigen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Indicator of Attack-Konfiguration aktualisiert hat.

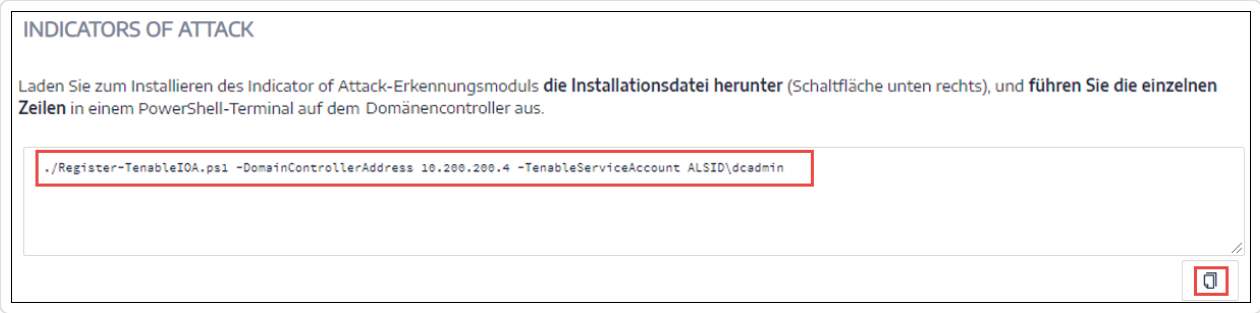
8. Klicken Sie auf **Installationsdatei herunterladen**.

9. Führen Sie die Installationsdatei aus, damit die neue Angriffskonfiguration wirksam wird:

   a. Kopieren Sie die heruntergeladene Installationsdatei und fügen Sie sie auf dem DC in der überwachten Domäne ein.

   b. Öffnen Sie als Administrator ein PowerShell-Terminal.

   c. Kopieren Sie in Tenable Identity Exposure die Befehle unten im Fenster unter dem Abschnitt „Indicators of Attack“.



   d. Fügen Sie im PowerShell-Fenster die Befehle zur Ausführung des Skripts ein.

Microsoft Sysmon installieren

Für einige Indicators of Attack (IoAs) von Tenable Identity Exposure muss der Microsoft System Monitor (Sysmon)-Dienst aktiviert werden.

Sysmon überwacht und protokolliert Systemaktivität im Windows-Ereignisprotokoll, um mehr Sicherheitsinformationen in der ETW-Infrastruktur (Ereignisablaufverfolgung für Windows) bereitzustellen.

Die Installation eines zusätzlichen Windows-Diensts und -Treibers kann die Leistung der Domänencontroller, die die Active Directory-Infrastruktur hosten, beeinträchtigen. Daher stellt Tenable Microsoft Sysmon nicht automatisch bereit. Sie müssen den Dienst manuell installieren oder ein dediziertes GPO verwenden.

Die folgenden IoAs erfordern Microsoft Sysmon.

Name	Grund
OS Credential Dumping: LSASS-Speicher	Erkennt Prozesseinschleusung

Hinweis: Wenn System installiert wird, muss der Dienst auf allen Domänencontrollern installiert werden, nicht nur auf dem PDC, um alle erforderlichen Ereignisse zu erfassen.

Hinweis: Testen Sie Ihre Sysmon-Installation auf Kompatibilitätsprobleme, bevor Sie eine vollständige Bereitstellung von Tenable Identity Exposure vornehmen.

Tipp: Achten Sie darauf, Sysmon nach der Installation regelmäßig zu aktualisieren, um alle Patches zu nutzen, die mögliche Schwachstellen beheben. Die älteste mit Tenable Identity Exposure kompatible Version ist Sysmon 12.0.

So installieren Sie Sysmon:

1. Laden Sie Sysmon von der Microsoft-Website herunter.
2. Führen Sie in der Befehlszeilenschnittstelle den folgenden Befehl aus, um Microsoft Sysmon auf dem lokalen Computer zu installieren:

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

Hinweis: Erläuterungen zur Konfiguration finden Sie in der kommentierten Sysmon-Konfigurationsdatei.

3. Führen Sie den folgenden Befehl aus, um einen Registrierungsschlüssel hinzuzufügen, der WMI-Filtern anzeigt, dass Sysmon installiert ist:

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

So deinstallieren Sie Sysmon:

1. Öffnen Sie ein PowerShell-Terminal.
2. Navigieren Sie zum Ordner mit der Datei `Sysmon64.exe`.
3. Geben Sie den folgenden Befehl ein:

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

So löschen Sie den Registrierungsschlüssel:

- Geben Sie in der Befehlszeilenschnittstelle aller Computer, auf denen Sysmon ausgeführt wird, den folgenden Befehl ein:

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

Sysmon-Konfigurationsdatei

Hinweise:
– Kopieren und speichern Sie die Sysmon-Konfigurationsdatei als XML-Datei, bevor Sie sie verwenden. Im Fall eines Fehlers können Sie die Konfigurationsdatei direkt hier herunterladen.
– Entsperren Sie die Datei in den Dateieigenschaften, bevor Sie sie ausführen.

```
<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>
```

Indicators of Attack deinstallieren

Erforderliche Rolle: Administrator auf dem lokalen Computer.

Um das Modul „Indicators of Attack" (IoA) zu deinstallieren, führen Sie einen Befehl aus, der ein neues Gruppenlinienobjekt (GPO) namens „Tenable Identity Exposure cleaning" erstellt.

Bei der Deinstallation wird dieses neue GPO standardmäßig verwendet, um zuvor installierte GPOs und die zugehörigen SYSVOL-Dateien, die Registrierungseinstellung, die erweiterte Protokollierungsrichtlinie und die WMI-Filter zu bereinigen.

Hinweis: Wenn Sie den anfänglichen Namen des GPO geändert haben, müssen Sie den neuen Namen an das Deinstallationsprogramm übergeben, damit dieses weiß, welches GPO deinstalliert werden soll. Der neue GPO-Name kann mit dem Parameter `-GpoDisplayName` übergeben werden.

So deinstallieren Sie das IoA-Modul:

1. Führen Sie in der Befehlszeilenschnittstelle den folgenden Befehl aus, um das IoA-Modul zu deinstallieren:

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

2. Replizieren Sie dieses neue GPO über die gesamte Domäne. Das Skript erzwingt eine 4-stündige Verzögerung bis zum Abschluss der Replikation.

3. Führen Sie den folgenden Befehl aus, um das Bereinigungs-GPO zu löschen:

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

4. Optional: Führen Sie den folgenden Befehl aus, um zu verifizieren, dass das GPO nicht mehr vorhanden ist:

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

Problembehebung bei Indicators of Attack

- Priorität der erweiterten Überwachungsrichtlinienkonfiguration
- Antivirus-Erkennung
- Tenable Identity Exposure-Protokolldateien
- Listener-Validierung für Ereignisprotokolle
- Entschärfung von DFS-Replikationsproblemen

Antivirus-Erkennung

Tenable und Microsoft empfehlen, auf Domänencontrollern keine Antivirus-, Endpoint Protection Platform (EPP)- oder Endpoint Detection and Response (EDR)-Software zu installieren (oder ein anderes Tool mit einer zentralen Verwaltungskonsole). Wenn Sie dies trotzdem tun, kann es sein, dass die Antivirus-/EPP-/EDR-Software Elemente erkennt und sogar blockiert oder löscht, die für die Erfassung von Indicator of Attack (IoA)-Ereignissen auf Domänencontrollern erforderlich sind.

Das Bereitstellungsskript von Tenable Identity Exposure für Indicators of Attack enthält keinen bösartigen Code und ist auch nicht verschleiert. Da es PowerShell und WMI nutzt und ohne Agent installiert wird, sind gelegentliche Erkennungen jedoch normal.

Folgende Probleme können auftreten:

- Fehlermeldungen während der Installation
- Falsch positive oder falsch negative Ergebnisse bei der Erkennung

So beheben Sie Probleme aufgrund von Antivirus-Erkennung in Installationsskripts:

1. Suchen Sie in den Antivirus-/EPP-/EDR-Sicherheitsprotokollen nach erkannten, blockierten oder gelöschten Tenable Identity Exposure-Komponenten. Antivirus-/EPP-/EDR-Software kann sich auf folgende Komponenten auswirken:
    - Die Datei `ScheduledTasks.xml` in dem auf Domänencontroller angewendeten Tenable Identity Exposure-GPO
    - Die geplante Tenable Identity Exposure-Aufgabe auf Domänencontrollern, die PowerShell.exe startet
    - Den Tenable Identity Exposure-Prozess `Register-TenableADEventsListener.exe`, der auf Domänencontrollern gestartet wurde
2. Fügen Sie Ihren Tools Sicherheitsausnahmen für die betroffenen Komponenten hinzu.
    - Insbesondere Symantec Endpoint Protection kann `CL.Downloader!gen27`-Erkennungen während der IoA-Installation auslösen. Sie können dieses spezifische bekannte Risiko Ihrer Ausnahmenrichtlinie hinzufügen.

- Führen Sie nach der Einrichtung der Aufgabenplanung PowerShell aus, um den Prozess `Register-TenableADEventsListener.exe` zu initiieren. Die Antivirus-/EPP-/EDR-Software kann dieses PowerShell-Skript potenziell blockieren und dadurch die ordnungsgemäße Ausführung von Indicators of Attack behindern. Verfolgen Sie diesen Prozess genau nach und stellen Sie sicher, dass er nur einmal auf allen überwachten Domänencontrollern ausgeführt wird.

  Beispiele für Dateipfadausschlüsse für Antivirus-/EPP-/EDR-Software:

```
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
```

Priorität der erweiterten Überwachungsrichtlinienkonfiguration

Das Gruppenrichtlinienobjekt (GPO), das Tenable Identity Exposure erstellt, um die erforderliche Ereignisprotokollierung zu ermöglichen, ist mit der Organisationseinheit (OU) der Domänencontroller mit aktiviertem Modus „Erzwungen“ verknüpft.

Dies gibt dem GPO zwar eine hohe Priorität, aber ein auf einer höheren Ebene (z. B. Domäne oder Site) konfiguriertes erzwungenes GPO hat Vorrang.

Wenn das GPO mit höherer Priorität, das die Einstellungen für die erweiterte Überwachungsrichtlinienkonfiguration definiert, mit den Anforderungen von Tenable Identity Exposure in Konflikt steht, hat es Vorrang. Tenable Identity Exposure fehlen in diesem Fall für die Angriffserkennung erforderliche Ereignisse.

Da Windows die von GPOs definierten Einstellungen für die erweiterte Überwachungsrichtlinienkonfiguration zusammenführt, können verschiedene GPOs unterschiedliche Einstellungen definieren.

Allerdings wird auf jeder Einstellungsebene nur der vom GPO definierte Wert mit der höheren Priorität verwendet. Beispiel: Tenable Identity Exposure benötigt den Erfolgs- und Fehlerwert für die Einstellung „Überprüfen der Anmeldeinformationen überwachen“. Wenn ein GPO mit höherer Priorität für die Einstellung „Überprüfen der Anmeldeinformationen überwachen“ jedoch nur „Erfolg“ definiert, erfasst Windows nur Erfolgsereignisse, und Tenable Identity Exposure fehlen die benötigten Fehlerereignisse.

So ermitteln Sie die GPO-Priorität:

1. Führen Sie in der Befehlszeilenschnittstelle den folgenden Befehl für einen Domänencontroller aus.

   Der Befehl gibt die geltende erweiterte Überwachungsrichtlinienkonfiguration nach Berücksichtigung aller GPOs und der Priorität aus.

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

2. Vergleichen Sie die Ausgabe mit den Tenable Identity Exposure-Anforderungen für erweiterte Überwachungsrichtlinien. Überprüfen Sie für jede von Tenable Identity Exposure benötigte Einstellung, ob die geltende Richtlinie sie ebenfalls abdeckt.

- Es ist kein Problem, wenn die geltende Richtlinie umfassender ist, wenn also z. B. Tenable Identity Exposure „Erfolg“ oder „Fehler“ benötigt und die Einstellung „Erfolg und Fehler“ lautet.
- Wenn die geltende Richtlinie nicht ausreicht, bedeutet dies, dass ein GPO mit höherer Priorität in Konflikt stehende Einstellungen definiert.

So korrigieren Sie die GPO-Priorität:

1. Suchen Sie nach GPOs, die im Modus „Erzwungen“ mit höheren Ebenen (Domäne oder Site) verknüpft sind, die die erweiterte Überwachungsrichtlinienkonfiguration definieren.
2. Führen Sie in der Befehlszeilenschnittstelle den folgenden Befehl für einen Domänencontroller aus, um das ausschlaggebende GPO zu lokalisieren:

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. Ändern Sie die entsprechende Einstellung der erweiterten Überwachungsrichtlinienkonfiguration im GPO so, dass die Mindestanforderungen von Tenable Identity Exposure erfüllt werden. Beispiel:
   - Wenn Tenable Identity Exposure „Erfolg“ erfordert und das GPO höherer Priorität „Fehler“ definiert, ändern Sie die Einstellung in „Erfolg und Fehler“.
   - Wenn Tenable Identity Exposure „Erfolg und Fehler“ erfordert und das GPO höherer Priorität „Erfolg“ definiert, ändern Sie die Einstellung in „Erfolg und Fehler“.
4. Nachdem Sie die Einstellung geändert haben, können Sie entweder warten, bis das aktualisierte GPO angewendet wird, oder es mit dem Befehl `gpupdate` erzwingen.
5. Wiederholen Sie das Verfahren So ermitteln Sie die GPO-Priorität:, um die neue geltende Richtlinie zu überprüfen.

Listener-Validierung für Ereignisprotokolle

Das Indicator of Attack-Installationsskript konfiguriert einen Ereignis-Watcher und einen WMI-Producer/Consumer (Windows-Verwaltungsinstrumentation) im Arbeitsspeicher des Computers. WMI ist eine Windows-Komponente, die Ihnen Informationen über den Status von lokalen oder Remote-Computersystemen liefert.

So überprüfen Sie die korrekte WMI-Registrierung:

- Führen Sie in PowerShell den folgenden Befehl aus:

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- Wenn mindestens ein Consumer vorhanden ist, erhalten Sie diese Art der Ausgabe:

```
> 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
```

- Wenn kein WMI-Consumer registriert ist, gibt der Befehl nichts zurück.
- Dies ist eine Voraussetzung dafür, dass der Prozess auf dem DC für WMI ausgeführt wird.

So rufen Sie den WMI-Prozess ab (für Versionen = oder < 3.19):

- Führen Sie in PowerShell den folgenden Befehl aus:

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- Beispiel für ein gültiges Ergebnis:

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}

ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472
```

So rufen Sie den Ereignisprotokoll-Listener ab (für Versionen = oder > 3.29):

- Führen Sie in PowerShell den folgenden Befehl aus:

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- Beispiel für ein gültiges Ergebnis:

```
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-Protokolldateien

Wenn nach der GPO- und WMI-Consumer-Validierung immer noch keine Warnungen zu Indicators of Attack angezeigt werden, können Sie die internen Protokolle von Tenable Identity Exposure überprüfen.

CETI-Protokoll

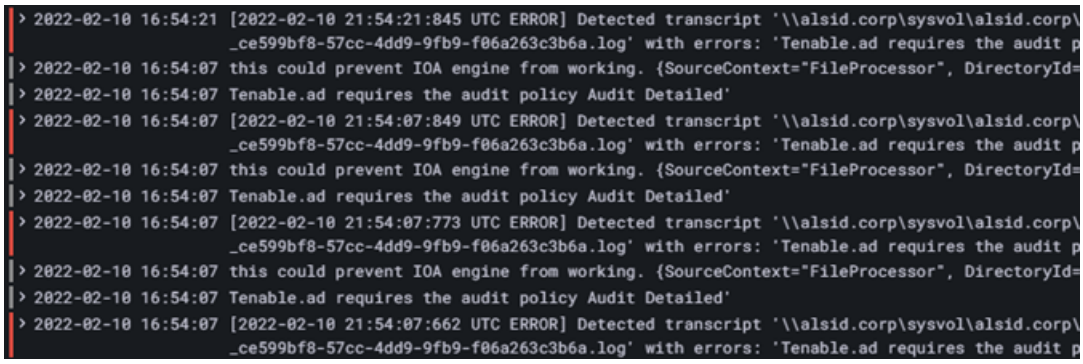
- Suchen Sie im CETI-Protokoll nach der folgenden Fehlermeldung:

```
[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"}
```

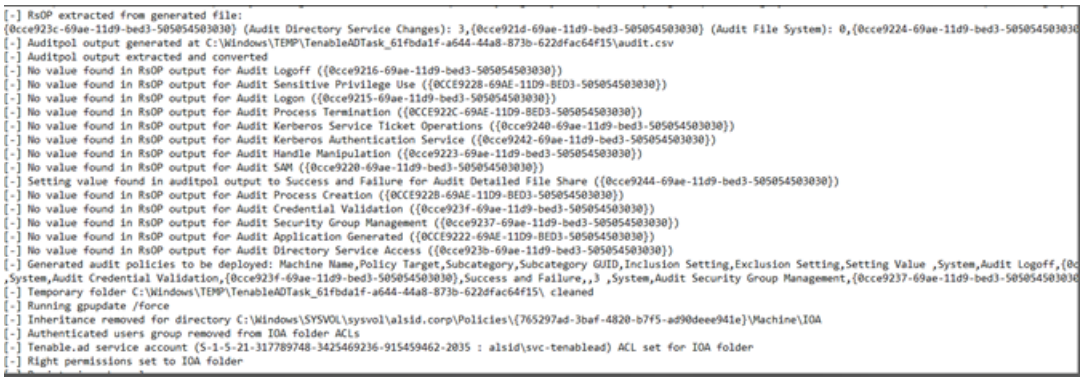
- Wenn diese Meldung angezeigt wird, überprüfen Sie, ob die GPO-Einstellungen und der WMI-Consumer auf dem in der obigen Fehlermeldung aufgeführten Domänencontroller (DC) ausgeführt werden.

Audit-Einstellungen

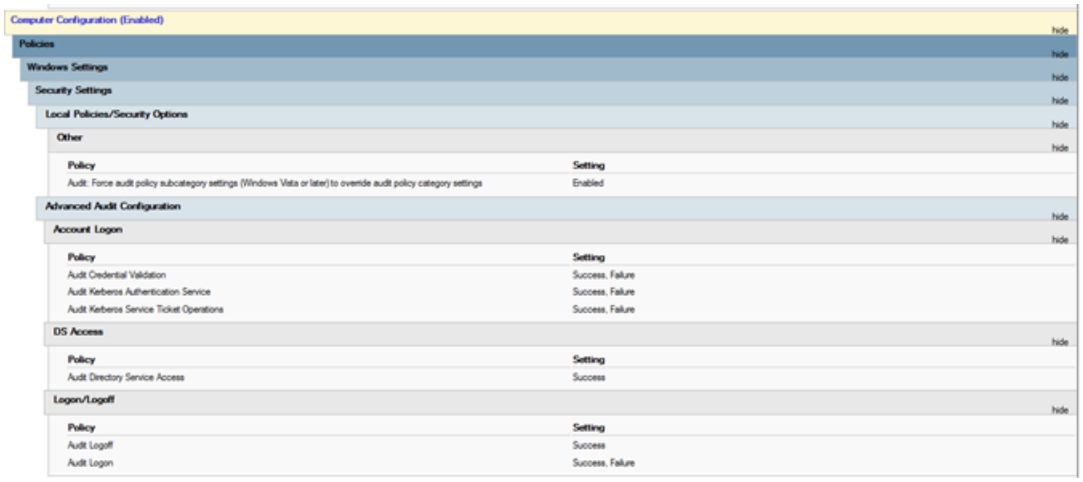
- Wenn ein Fehler ähnlich dem folgenden angezeigt wird: „Tenable Identity Exposure requires the Audit Policy…“, überprüfen Sie Ihre vorhandenen GPOs, um sicherzustellen, dass Sie die erforderlichen Überwachungsrichtlinien nicht auf „Keine Überwachung“ festgelegt haben.



- Wenn Sie eine Fehlermeldung mit folgendem Inhalt erhalten: „RSOP…“:



- Überprüfen Sie die Überwachungsrichtlinien und sehen Sie sich die Protokolldatei im Sysvol-Ordner an, um festzustellen, ob während der Installation Probleme aufgetreten sind.



Cygni-Protokoll

Cygni protokolliert den Angriff und listet die spezifische `.gz`-Datei auf, die Tenable Identity Exposure aufgerufen hat, um die Warnung zu generieren.

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-Protokoll

Die folgenden Protokolleinträge bestätigen, dass Cephei Angriffe notiert. Der Schlüsselwert ist die **attackTypeID**, die die Art des Angriffs angibt. Diese können Sie für die Korrelation mit den Cygni-Einträgen verwenden:

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"}
```

Elektra-Protokoll

Sie sollten den folgenden Eintrag sehen:

[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-Protokoll

Sie sollten den folgenden Eintrag sehen:

```
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)
```

Entschärfung von DFS-Replikationsproblemen

Ein zusätzlicher Parameter, `-EventLogsFileWriteFrequency X`, im Indicator of Attack-Bereitstellungsskript erlaubt Ihnen die Behandlung potenzieller Probleme durch langsame oder fehlerhafte Distributed File System-Replikation (DFS).

Dieser Parameter ist optional und Tenable empfiehlt, ihn nur zu verwenden, wenn Sie DFS-Replikationsprobleme haben oder diese seit der Bereitstellung des IoA-Skripts bemerkt haben. Unter normalen Umständen behält der Parameter seinen Standardwert bei, und Sie müssen ihn beim Ausführen des Skripts nicht in die Befehlszeile einfügen.

Wann der Parameter geändert werden sollte

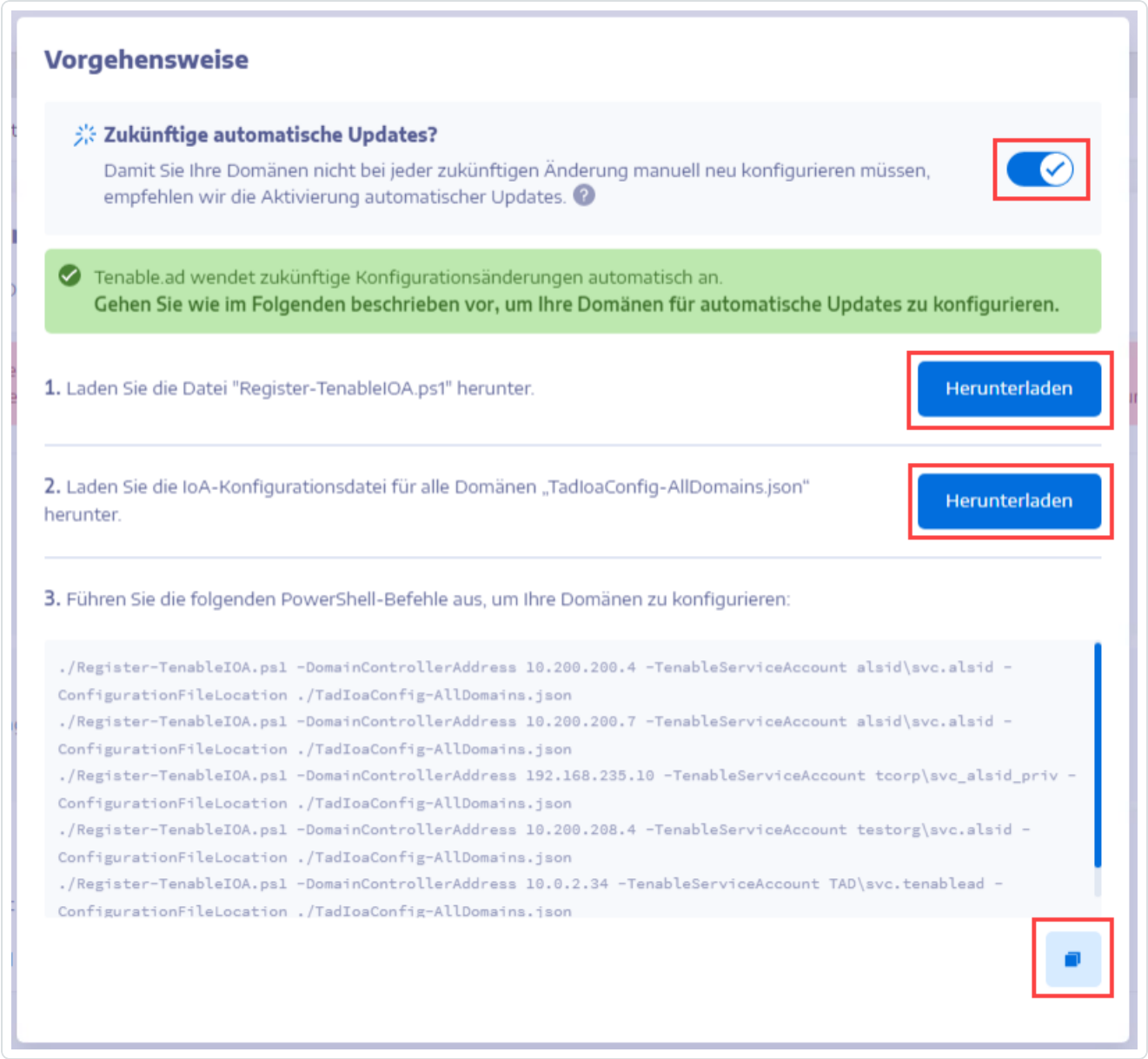
Der Wert [`X`] des Parameters `-EventLogsFileWriteFrequency X` ist die Häufigkeit, mit der der Tenable Identity Exposure-Listener eine Ereignisprotokolldatei auf Nicht-PDCe-Domänencontrollern (DCs) generiert. Der vom Tenable Identity Exposure-Listener verwendete Standard und empfohlene Wert beträgt 15 Sekunden. Der angepasste Wert gilt jedoch nicht für PDCe-DCs und bleibt beim Standardintervall von 15 Sekunden, um sicherzustellen, dass die Funktionen zur Angriffserkennung voll funktionsfähig sind. Tenable empfiehlt, diesen Parameter nur dann zu verwenden und seinen Wert über den Standardwert von 15 Sekunden hinaus auf bis zu 300 Sekunden (5 Minuten) zu erhöhen, wenn in Ihrer Infrastruktur DFS-Replikationsprobleme auftreten oder sie anfällig dafür ist.

Empfehlungen

Beachten Sie, dass eine Erhöhung der Schreibhäufigkeit der Ereignisprotokolldatei dazu führt, dass die Datei seltener erstellt wird, wodurch sich die Verzögerung bei der Angriffserkennung erhöht (z. B. wenn die Datei alle 30 Sekunden statt der standardmäßigen 15 Sekunden auf Nicht-PDCe-DCs generiert wird). Durch die Erhöhung der Verzögerung vergrößert sich außerdem der Umfang der generierten Ereignisprotokolldatei innerhalb der festgelegten Grenzen, wie in Technische Änderungen und potenzielle Auswirkungen definiert. Verwenden Sie diesen Parameter daher nur als Entschärfungsstrategie und nicht als Ersatz für die ordnungsgemäße Untersuchung von DFS-Replikationsproblemen.

So wenden Sie den Parameter an:

1. Konfigurieren Sie Ihre Domänen für IoAs wie im Verfahren beschrieben. Weitere Informationen finden Sie unter [Indicators of Attack installieren].



2. Öffnen Sie als Administrator ein PowerShell-Terminal.
3. Führen Sie das Skript aus, um Ihre Domänencontroller für IoAs zu konfigurieren, und hängen Sie den Parameter `-EventLogsFileWriteFrequency X` an, wobei `[X]` die Häufigkeit ist, die Sie für die Häufigkeit der Ereignisprotokolldateien festlegen möchten.

Authentifizierung

Es gibt mehrere Möglichkeiten, Tenable Identity Exposure-Benutzer zu authentifizieren:

- Authentifizierung über ein Tenable Identity Exposure-Konto
- Authentifizierung mit LDAP
- Authentifizierung mit SAML

Authentifizierung mit Tenable One

Erforderliche Lizenz: Tenable One

Hinweis: Mit einer Tenable One-Lizenz verwalten Sie alle Authentifizierungseinstellungen in Tenable Vulnerability Management. Weitere Informationen finden Sie unter *„Access Control" im Tenable Vulnerability Management User Guide*.

So konfigurieren Sie die Authentifizierung mit Tenable One:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration**.

   Daraufhin öffnet sich der Konfigurationsbereich.

2. Klicken Sie im Abschnitt **Authentifizierung** auf **Tenable One**.

3. Wählen Sie im Dropdown-Feld **Standardprofil** das Profil für den Benutzer aus.

4. Im Feld **Standardrollen** wählen Sie die Rollen für den Benutzer aus.

   Tipp: Authentifizierte Benutzer in Tenable One, die sich noch nicht mit Tenable Identity Exposure verbunden haben, verfügen automatisch über ein Konto, wenn sie sich bei Tenable Identity Exposure einloggen. Für den Benutzer gelten standardmäßig das Standardprofil und die Standardrolle. **Ausnahme**: Benutzer mit der Rolle „Administrator" in Tenable Vulnerability Management haben auch die Rolle „Globaler Administrator" in Tenable Identity Exposure.

5. Klicken Sie auf **Speichern**.

Authentifizierung über ein Tenable Identity Exposure-Konto

Die einfachste Authentifizierungsmethode ist über ein Tenable Identity Exposure-Konto, für das ein Benutzername und ein Passwort erforderlich ist.

Diese Authentifizierungsmethode bietet eine Standardsperrrichtlinie, eine Sicherheitskontrolle, die Brute-Force-Angriffe auf Authentifizierungsmechanismen eindämmen soll. Benutzerkonten werden nach zu vielen fehlgeschlagenen Login-Versuchen gesperrt. Ist ein Konto gesperrt, haben Benutzer keinen Zugriff auf die APIs von Tenable Identity Exposure.

So konfigurieren Sie die Authentifizierung mit einem Tenable Identity Exposure-Konto:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration**.

   Daraufhin öffnet sich der Konfigurationsbereich.

2. Klicken Sie im Abschnitt **Authentifizierung** auf **Tenable Identity Exposure**.

3. Wählen Sie im Dropdown-Feld **Standardprofil** das Profil für den Benutzer aus.

4. Im Feld **Standardrollen** wählen Sie die Rollen für den Benutzer aus.

5. Konfigurieren Sie die Einstellungen für die Sperrrichtlinie:

Einstellung	Beschreibung	Standardwert
Aktiviert	• **Aktiviert** – Tenable Identity Exposure sperrt das Konto nach einer bestimmten Anzahl von fehlgeschlagenen Login-Versuchen. • **Deaktiviert** – Tenable Identity Exposure sperrt das Konto nicht nach fehlgeschlagenen Login-Versuchen.	Aktiviert
Sperrdauer	Die Zeitspanne, in der Tenable Identity Exposure das Konto für jegliche Login-Versuche sperrt. Tenable Identity Exposure gibt das Konto nach Ablauf dieser Zeit automatisch wieder frei, damit sich der Benutzer erneut einloggen kann. So konfigurieren Sie die Sperrdauer: 1. Klicken Sie auf den Schieberegler, um die Sperrdauer festzulegen. 2. Wählen Sie **Endlos**, wenn Sie die Kontosperre nicht automatisch nach einer bestimmten Dauer aufheben möchten. **Hinweis**: Wenn alle Konten innerhalb der Gruppe „Globaler Administrator" gesperrt werden, entsperrt Tenable Identity Exposure das Standardadministratorkonto nach 10 Sekunden.	300 Sekunden
Anzahl Versuche vor Sperre	Die Anzahl der fehlgeschlagenen Login-Versuche, bevor Tenable Identity Exposure	3

	das Konto sperrt.	
Einlösungsfrist	Das Zeitintervall, in dem Tenable Identity Exposure die Anzahl der erfolglosen Login-Versuche zählt. Nach einer bestimmten Anzahl von erfolglosen Login-Versuchen sperrt Tenable Identity Exposure das Konto. So legen Sie die Einlösungsfrist fest: 1. Klicken Sie auf den Schieberegler, um ein Zeitintervall festzulegen. 2. Wählen Sie „Unendlich“, wenn Sie kein Zeitintervall für die Anzahl der erfolglosen Login-Versuche festlegen möchten, bevor Tenable Identity Exposure das Konto sperrt.	900 Sekunden

6. Klicken Sie auf **Speichern**.

So deaktivieren Sie die Sperrrichtlinie:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration**.

   Daraufhin öffnet sich der Konfigurationsbereich.

2. Klicken Sie auf die Schaltfläche **Aktiviert**, um die Sperrrichtlinie zu deaktivieren.

Hinweis: Wenn Sie die Sperrrichtlinie deaktivieren, können gesperrte Benutzerkonten versuchen, sich erneut zu verbinden.

So zeigen Sie die Liste der gesperrten Konten an:

- Gehen Sie in Tenable Identity Exposure zu **Konten** > **Benutzerkontenverwaltung**.

  In der Liste der Benutzer zeigt Tenable Identity Exposure die gesperrten Konten mit einem roten Vorhängeschloss-Symbol an. Tenable Identity Exposure zeigt Benutzern mit gesperrten

Konten die folgende Meldung an: „Ihr Konto ist aufgrund zu vieler fehlgeschlagener Authentifizierungsversuche gesperrt. Sie müssen einen Administrator kontaktieren."

So entsperren Sie ein Konto:

Sie müssen über die Berechtigung zum Bearbeiten von Benutzern verfügen, um Konten freizuschalten.

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Benutzerkontenverwaltung**.

   Das Fenster zur Benutzerkontenverwaltung wird angezeigt.

2. Suchen Sie in der Liste der Benutzer das gesperrte Konto.
3. Klicken Sie auf das Bleistiftsymbol, um das gesperrte Benutzerkonto zu bearbeiten.

   Der Bereich mit den Benutzerinformationen wird angezeigt.

4. Klicken Sie auf die Schaltfläche **Sperre aufheben**.

So erteilen Sie den Benutzerrollen die Berechtigung, die Sperrrichtlinie zu konfigurieren:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Rollenverwaltung**.

   Daraufhin wird der Bereich **Rollenverwaltung** angezeigt.

2. Klicken Sie auf das Bleistiftsymbol neben einem Rollennamen, um die Rolle zu bearbeiten.

   Der Bereich **Rolle bearbeiten** wird angezeigt.

3. Klicken Sie auf die Registerkarte **Systemkonfigurationsentitäten**.
4. Aktivieren Sie im Abschnitt **Berechtigungsverwaltung** das Kontrollkästchen **Kontosperrrichtlinie**.
5. Klicken Sie auf die Umschalttaste, um **Autorisierung aufgehoben** oder **Erteilt** festzulegen.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Berechtigungen des Benutzers aktualisiert hat.

   Hinweis: Tenable Identity Exposure deaktiviert die Sperrrichtlinieneinstellungen für Benutzer, die für diesen Bereich nur über Lesezugriff verfügen.

Authentifizierung mit LDAP

Tenable Identity Exposure ermöglicht Ihnen die Authentifizierung über das Lightweight Directory Access Protocol (LDAP).

Um die LDAP-Authentifizierung zu aktivieren, müssen folgende Voraussetzungen erfüllt sein:

- Ein vorkonfiguriertes Dienstkonto mit einem Benutzer und einem Passwort für den Zugriff auf das Active Directory.
- Eine vorkonfigurierte Active Directory-Gruppe.

Nachdem Sie die LDAP-Authentifizierung eingerichtet haben, wird die LDAP-Option auf einer Registerkarte auf der Login-Seite angezeigt.

So konfigurieren Sie die LDAP-Authentifizierung:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration**.

   Daraufhin öffnet sich der Konfigurationsbereich.

2. Klicken Sie unter dem Abschnitt **Authentifizierung** auf **LDAP**.
3. Klicken Sie auf die Umschalttaste **LDAP-Authentifizierung aktivieren**, um sie zu aktivieren.

   Daraufhin wird ein Formular mit LDAP-Informationen angezeigt.

4. Geben Sie folgende Informationen an:

   - Geben Sie im Feld **Adresse des LDAP-Servers** die IP-Adresse des LDAP-Servers ein, die mit `ldap://` beginnt und mit dem Domänennamen und der Portnummer endet.

     Hinweis: Wenn Sie einen LDAPS-Server verwenden, geben Sie dessen Adresse ein, die mit `ldaps://` beginnt und mit dem Domänennamen und der Portnummer endet. Siehe die Vorgehensweise So fügen Sie ein benutzerdefiniertes Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA) für LDAPS hinzu:, um die Konfiguration für LDAPS abzuschließen.

   - Geben Sie im Feld **Dienstkonto zum Abfragen des LDAP-Servers** den Distinguished Name (DN), SamAccountName oder UserPrincipalName ein, den Sie für den Zugriff auf den LDAP-Server verwenden.

- Geben Sie im Feld **Dienstkontopasswort** das Passwort für dieses Dienstkonto ein.
- Geben Sie im Feld **LDAP-Suchbasis** das LDAP-Verzeichnis ein, das Tenable Identity Exposure verwendet, um nach Benutzern zu suchen, die versuchen, eine Verbindung herzustellen, beginnend mit `DC=` oder `OU=`. Das kann ein Stammverzeichnis oder eine bestimmte Organisationseinheit sein.
- Geben Sie im Feld **LDAP-Suchfilter** das Attribut ein, das Tenable Identity Exposure zum Filtern von Benutzern verwendet. Ein Standardattribut für die Authentifizierung in Active Directory ist `sAMAccountname={{login}}`. Der Wert für `Login` ist der Wert, den der Benutzer bei der Authentifizierung angibt.

5. Wenn Sie **SASL-Bindungen aktivieren** möchten, gehen Sie wie folgt vor:
   - Wenn Sie SamAccountName für das Dienstkonto verwenden, klicken Sie auf die Umschalttaste **SASL-Bindungen aktivieren**, um sie zu aktivieren.
   - Wenn Sie den Distinguished Name oder UserPrincipalName für das Dienstkonto verwenden, lassen Sie die Option **SASL-Bindungen aktivieren** deaktiviert.
6. Klicken Sie unter dem Abschnitt **Standardprofil und Rollen** auf **LDAP-Gruppe hinzufügen**, um die Gruppen anzugeben, die sich authentifizieren dürfen.

   Daraufhin wird ein Formular mit LDAP-Gruppeninformationen angezeigt.
   - Geben Sie im Feld **LDAP-Gruppenname** den Distinguished Name der Gruppe ein (Beispiel: `CN=TAD_User,OU=Groups,DC=Tenable,DC=ad`)
   - Wählen Sie im Dropdown-Feld **Standardprofil** das Profil für die zulässige Gruppe aus.
   - Wählen Sie im Feld **Standardrollen** die Rollen für die zulässige Gruppe aus.
7. Sofern erforderlich, klicken Sie auf das Symbol ⊕, um eine neue zulässige Gruppe hinzuzufügen.
8. Klicken Sie auf **Speichern**.

So fügen Sie ein benutzerdefiniertes Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA) für LDAPS hinzu:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme**.
2. Klicken Sie auf die Registerkarte **Konfiguration**, um den Konfigurationsbereich anzuzeigen.
3. Klicken Sie im Abschnitt **Anwendungsdienste** auf **Vertrauenswürdige Zertifizierungsstellen**.
4. Fügen Sie in das Feld **Zusätzliche Zertifikate** das PEM-kodierte vertrauenswürdige CA-Zertifikat Ihres Unternehmens ein, das Tenable Identity Exposure verwenden soll.
5. Klicken Sie auf **Speichern**.

Weitere Informationen zu Sicherheitsprofilen und Rollen finden Sie in folgenden Ressourcen:

- Sicherheitsprofile
- Benutzerrollen

Authentifizierung mit SAML

Sie können die SAML-Authentifizierung so konfigurieren, dass Tenable Identity Exposure-Benutzer beim Einloggen bei Tenable Identity Exposure das vom Identitätsanbieter initiierte Single Sign-On (SSO) nutzen können.

Bevor Sie beginnen:

- Im Leitfaden Tenable SAML Configuration Quick-Reference finden Sie eine Schrittanleitung zur Konfiguration von SAML für die Verwendung mit Tenable Identity Exposure.
- Vergewissern Sie sich, dass für den Identitätsanbieter (IDP) Folgendes vorhanden ist:
  - Nur SAML v2.
  - „Assertion-Verschlüsselung“ ist aktiviert.
  - IDP-Gruppen, die Tenable Identity Exposure verwendet, um im Tenable Identity Exposure-Webportal Zugriff zu gewähren.
  - URL des SAML-Servers.
  - Vertrauenswürdige Zertifizierungsstelle (CA), die das SAML-Serverzertifikat im PEM-kodierten Format signiert hat, beginnend mit `-----BEGIN CERTIFICATE -----` und endend mit `-----END CERTIFICATE-----`.

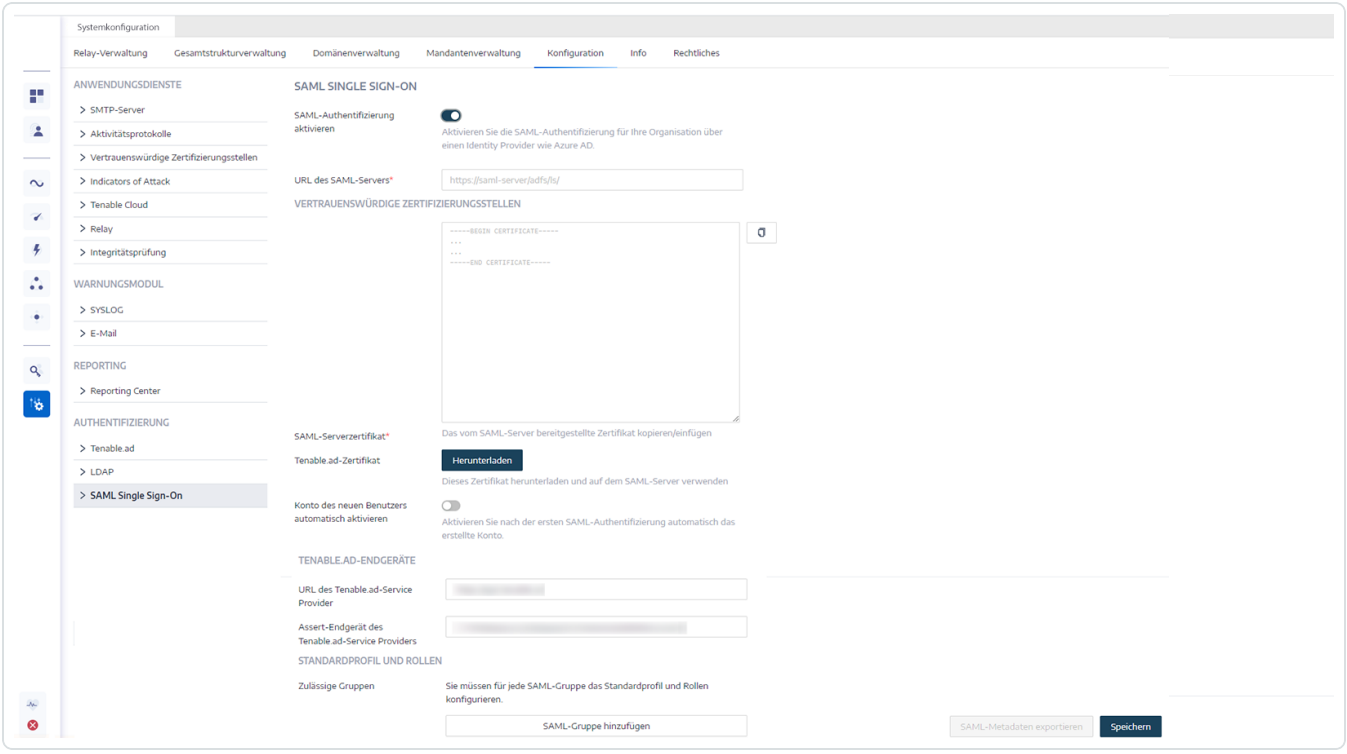
So konfigurieren Sie die SAML-Authentifizierung:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme** > **Konfiguration**.

   Daraufhin öffnet sich der Konfigurationsbereich.

2. Klicken Sie im Bereich **Authentifizierung** auf **SAML Single Sign-On**.
3. Klicken Sie auf die Umschalttaste **SAML-Authentifizierung aktivieren**.

   Es wird eine SAML-Information angezeigt.



4. Geben Sie folgende Informationen an:

    - Geben Sie im Feld **URL des SAML-Servers** die vollständige URL des SAML-Servers des IDP ein, mit dem sich Tenable Identity Exposure verbinden muss.
    - Fügen Sie im Feld **Vertrauenswürdige Zertifizierungsstellen** die Zertifizierungsstelle (CA) ein, die das Zertifikat des SAML-Servers signiert hat.

5. Klicken Sie im Feld **Tenable Identity Exposure-Zertifikat** auf **Herunterladen**. Dadurch wird ein neues selbstsigniertes Zertifikat generiert, die SAML-Konfiguration wird in der Datenbank aktualisiert und es wird ein neues Zertifikat zurückgegeben, das Sie herunterladen können.

    Achtung: Wenn Sie auf diese Schaltfläche klicken, wird Ihre SAML-Konfiguration unterbrochen, da Tenable Identity Exposure erwartet, dass sich der IDP sofort mit dem zuletzt generierten Zertifikat authentifiziert, während der IDP noch ein früheres Zertifikat verwendet (falls vorhanden). Wenn Sie ein neues Tenable Identity Exposure-Zertifikat generieren, müssen Sie Ihren IDP so umkonfigurieren, dass er das neue Zertifikat verwendet.

6. Klicken Sie auf den Umschalter **Konto des neuen Benutzers automatisch aktivieren**, um neue Benutzerkonten nach dem ersten SAML-Login zu aktivieren.

7. Geben Sie unter **Tenable Identity Exposure-Endpunkte** die folgenden Informationen an:

- URL des Tenable Identity Exposure-Dienstanbieters
- Assert-Endpunkt des Tenable Identity Exposure-Dienstanbieters

8. Klicken Sie unter **Standardprofil und Rollen** auf **SAML-Gruppe hinzufügen**, um anzugeben, welche Gruppen sich authentifizieren können.

   Es wird eine SAML-Information angezeigt.

9. Geben Sie folgende Informationen an:
   - Geben Sie im Feld **SAML-Gruppenname** den Namen der zulässigen Gruppe ein, wie er im SAML-Server erscheint.
   - Wählen Sie im Dropdown-Feld **Standardprofil** das Profil für die zulässige Gruppe aus.
   - Wählen Sie im Feld **Standardrollen** die Rollen für die zulässige Gruppe aus.
10. Sofern erforderlich, klicken Sie auf das Symbol ⊕, um eine neue zulässige Gruppe hinzuzufügen.
11. Klicken Sie auf **Speichern**.

    Nachdem Sie die SAML-Authentifizierung eingerichtet haben, wird die SAML-Option auf einer Registerkarte auf der Login-Seite angezeigt.

Weitere Informationen zu Sicherheitsprofilen und Rollen finden Sie in folgenden Ressourcen:

- Sicherheitsprofile
- Benutzerrollen

Benutzerkonten

Auf der Seite **Benutzerkontenverwaltung** können Sie Benutzerkonten hinzufügen, bearbeiten, löschen oder die Details von Tenable Identity Exposure-Benutzerkonten einsehen.

Benutzer gehören zwei Kategorien an:

- Globaler Administrator: eine Administratorrolle, die alle Berechtigungen umfasst
- Benutzer: eine einfache Benutzerrolle mit reinen Leseberechtigungen für Geschäftsdaten

Weitere Informationen finden Sie in folgenden Ressourcen:

- Benutzer erstellen
- Benutzer bearbeiten
- Benutzer deaktivieren
- Benutzer löschen

Benutzer erstellen

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

Hinweis: Die folgenden Anweisungen gelten für eigenständige Instanzen von Tenable Identity Exposure. Für Instanzen, die mit Tenable Vulnerability Management verknüpft sind, erstellen Sie Benutzer in Tenable Vulnerability Management, die anschließend an Tenable Identity Exposure übertragen werden.

So erstellen Sie einen Benutzer:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Benutzerkontenverwaltung**.

   Daraufhin öffnet sich der Bereich **Benutzerkontenverwaltung**.

2. Klicken Sie auf der rechten Seite auf die Schaltfläche **Benutzer erstellen**.

   Daraufhin öffnet sich der Fensterbereich **Benutzer erstellen**.

3. Geben Sie unter dem Abschnitt **Hauptinformationen** die folgenden Informationen zum Benutzer ein:

   - Vorname
   - Nachname
   - E-Mail
   - Passwort: mindestens 12 Zeichen, davon mindestens 1 Kleinbuchstabe, 1 Großbuchstabe, 1 Zahl und 1 Sonderzeichen
   - Passwortbestätigung
   - Abteilung
   - Biografie

4. Klicken Sie auf die Umschalttaste **Authentifizierung zulassen**, um den Benutzer zu aktivieren.

5. Wählen Sie im Abschnitt **Rollenverwaltung** eine Rolle aus, die dem Benutzer zugewiesen werden soll.

6. Klicken Sie auf **Erstellen**.

Eine Meldung bestätigt, dass Tenable Identity Exposure den Benutzer mit der ausgewählten Rolle erstellt hat.

Siehe auch

- Benutzer bearbeiten
- Benutzer deaktivieren
- Benutzer löschen

Benutzer bearbeiten

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

So bearbeiten Sie einen Benutzer:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Benutzerkontenverwaltung**.

   Daraufhin öffnet sich der Bereich **Benutzerkontenverwaltung**.

2. Fahren Sie mit dem Mauszeiger in der Benutzerliste über die Zeile, in der der Name des Benutzers erscheint, und klicken Sie auf das Symbol ✎ am Ende der Zeile.

   Daraufhin wird der Bereich **Benutzer bearbeiten** angezeigt.

3. Bearbeiten Sie im Abschnitt **Hauptinformationen** wie gewünscht die Informationen zum Benutzer:

   - Vorname
   - Nachname
   - E-Mail
   - Passwort: mindestens 8 Zeichen erforderlich
   - Passwortbestätigung
   - Abteilung
   - Biografie

4. Bearbeiten Sie im Abschnitt **Rollenverwaltung** die Rolle des Benutzers nach Bedarf.

5. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure den Benutzer mit der ausgewählten Rolle aktualisiert hat.

Siehe auch

- Benutzer erstellen
- Benutzer deaktivieren
- Benutzer löschen

Benutzer deaktivieren

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

So deaktivieren Sie einen Benutzer:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Benutzerkontenverwaltung**.

   Daraufhin öffnet sich der Bereich **Benutzerkontenverwaltung**.

2. Fahren Sie mit dem Mauszeiger in der Benutzerliste über die Zeile, in der der Name des Benutzers erscheint, und klicken Sie auf das Symbol ✎ am Ende der Zeile.

   Daraufhin wird der Bereich **Benutzer bearbeiten** angezeigt.

3. Klicken Sie auf die Umschalttaste **Authentifizierung zulassen**, um den Benutzer zu deaktivieren.

4. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure den Benutzer aktualisiert hat.

Siehe auch

- Benutzer erstellen
- Benutzer bearbeiten
- Benutzer löschen

Benutzer löschen

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

So löschen Sie einen Benutzer:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Benutzerkontenverwaltung**.

   Daraufhin öffnet sich der Bereich **Benutzerkontenverwaltung**.

2. Fahren Sie in der Benutzerliste mit dem Mauszeiger über die Zeile, in der der Name des Benutzers angezeigt wird, den Sie löschen möchten, und klicken Sie am Ende der Zeile auf das Symbol .

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.

3. Klicken Sie auf **Löschen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure den Benutzer gelöscht hat.

Siehe auch

- Benutzer erstellen
- Benutzer bearbeiten
- Benutzer deaktivieren

Sicherheitsprofile

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

Mithilfe von Profilen können Sie Ihre eigene Ansicht der Risiken, die Ihr Active Directory betreffen, erstellen und anpassen.

Jedes Profil zeigt Exposure- und Angriffsszenarien, die für Benutzer mit diesem Profil konfiguriert sind. So kann die allgemeine Sicht eines IT-Administrators auf die Datenanalyse eine andere sein als die des Sicherheitsteams, die einen umfassenden Überblick über alle Risiken von AD-Infrastrukturen zeigt.

Durch die Anwendung eines Sicherheitsprofils können verschiedene Arten von Benutzern die Datenanalyse unter verschiedenen Gesichtspunkten überprüfen, wie durch die Indikatoren für dieses Sicherheitsprofil definiert.

Im Bereich „Sicherheitsprofilverwaltung“ können Sie verschiedene Arten von Benutzern verwalten, die die Sicherheitsanalyse unter verschiedenen Gesichtspunkten überprüfen können. Sicherheitsprofile bieten auch die Möglichkeit, das Verhalten von Indicators of Exposure und Indicators of Attack anzupassen.

Hinweis: Tenable Identity Exposure stellt ein Standard-Sicherheitsprofil namens „Tenable“ bereit. **Sie können das Tenable-Profil nicht ändern oder löschen**, aber Sie können es als Vorlage verwenden, um andere Sicherheitsprofile mit Einstellungen zu erstellen, die an Ihre Anforderungen angepasst sind.

So erstellen Sie ein neues Sicherheitsprofil:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Sicherheitsprofilverwaltung**.

   Daraufhin wird der Bereich **Sicherheitsprofilverwaltung** angezeigt.

2. Klicken Sie auf der rechten Seite auf die Schaltfläche **Profil erstellen**.

   Daraufhin wird der Bereich **Profil erstellen** angezeigt.

3. Im Dropdown-Feld „Aktion“ haben Sie folgende Möglichkeiten:

- **Erstellen Sie ein neues Profil**.
- **Kopieren** Sie ein bestehendes Sicherheitsprofil, aus dem Sie ein neues Profil erstellen können (z. B. das Profil „Tenable“).

4. Geben Sie im Feld **Name des Profils** einen Namen für das neue Profil ein.

   Hinweis: Tenable Identity Exposure Tenable.ad akzeptiert nur alphanumerische Zeichen und Unterstriche.

5. Klicken Sie unten rechts auf die Schaltfläche **Erstellen**.

   Eine Meldung zeigt an, dass Tenable Identity Exposure das Profil erstellt hat. Daraufhin wird der Bereich **Profilkonfiguration** angezeigt.

So löschen Sie ein Sicherheitsprofil:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Sicherheitsprofilverwaltung**.

   Daraufhin wird der Bereich **Sicherheitsprofilverwaltung** angezeigt.

2. Fahren Sie mit dem Mauszeiger in der Liste der Sicherheitsprofile über das zu löschende Sicherheitsprofil und klicken Sie auf das Symbol 🗑 am Ende der Zeile.

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.

3. Klicken Sie auf **Löschen**.

   In einer Meldung wird bestätigt, dass Tenable Identity Exposure das Profil gelöscht hat.

Nächste Schritte

Weitere Informationen zum Abschließen der Profilerstellung finden Sie unter Indikator anpassen.

Weitere Informationen finden Sie in folgenden Ressourcen:

- Indikator anpassen
- Anpassung eines Indikators präzisieren

Indikator anpassen

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

Sie können Indicators of Exposure und Indicators of Attack für ein Sicherheitsprofil anpassen.

Jedes Sicherheitsprofil arbeitet unabhängig, um sicherzustellen, dass ein Profil die Ergebnisse eines anderen nicht beeinflusst. Sie sollten das Profil „Tenable“ ausschließlich als Referenz verwenden, da Sie es nicht anpassen oder verwenden können, um Abweichungen auf die Zulassungsliste zu setzen. Sie müssen Ihre eigenen benutzerdefinierten Profile erstellen, um bestimmte Anforderungen zu erfüllen.

Der Begriff „Globale Anpassung“ im Bereich zur Indikatoranpassung **bezieht sich auf alle Domänen** und nicht auf alle Profile. Folglich wirken sich Einstellungen, die Sie auf die „globale Anpassung“ für ein Sicherheitsprofil anwenden, nicht auf das Profil „Tenable“ oder ein anderes Profil aus.

Tipp: Um die Einstellungen für das Sicherheitsprofil „Tenable“ anzuzeigen, klicken Sie auf das Symbol 👁 am Ende der Zeile.

So passen Sie einen Indikator an:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Sicherheitsprofilverwaltung**.

   Daraufhin wird der Bereich **Sicherheitsprofilverwaltung** angezeigt.

2. Fahren Sie mit dem Mauszeiger in der Liste der Sicherheitsprofile auf das Sicherheitsprofil, das den Indikator enthält, den Sie anpassen möchten. Klicken Sie auf das Symbol ✎ am Ende der Zeile, in der der Dateiname des Sicherheitsprofils erscheint.

   Daraufhin wird der Bereich **Profilkonfiguration** angezeigt.

3. Wählen Sie die Registerkarte für **Indicators of Exposure** oder **Indicators of Attack**.

4. (Optional) Geben Sie im Feld **Indikator suchen** einen Indikatornamen ein.

5. Klicken Sie auf den Namen des Indikators, der angepasst werden soll.

   Daraufhin wird der Bereich **Indikatoranpassung** angezeigt.

6. Nehmen Sie die erforderlichen Anpassungen am Indikator vor.

Hinweis: Bestimmte Indikatoroptionen erfordern die Verwendung von regulären Ausdrücken (regex). Regex ist eine „contain"-Übereinstimmung anstelle einer „equal"-Übereinstimmung. Beispiel: Wenn Sie „`admin`" als Eingabeoption angeben, können Sie sowohl einen Benutzer mit „`samAccountName=admin`" als auch einen Benutzer mit „`samAccountName=admintoto`" auf die Zulassungsliste setzen.
– Um eine exakte Übereinstimmung zu erzielen, müssen Sie die regex-Syntax für Sonderzeichen („`^...$`") verwenden.
– Bei Verwendung von regex müssen Sie Sonderzeichen außerdem mit einem umgekehrten Schrägstrich als Escape-Zeichen versehen. Beispiel: Um „`domain\user`" und „`CN=Vincent C. (Test),DC=tenable,DC=corp`" zu deklarieren, geben Sie „`domain\\user`" und „`CN=Vincent C. \(Test\),DC=tenable,DC=corp`" ein.

7. Klicken Sie auf **Als Entwurf speichern**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Anpassungsoptionen gespeichert hat.

So wenden Sie die Anpassung an:

1. Sie haben folgende Möglichkeiten:

   - Klicken Sie im Bereich **Profilkonfiguration** in der unteren rechten Ecke auf **Ausstehende Anpassungen anwenden** oder
   - Klicken Sie im Bereich **Sicherheitsprofilverwaltung** auf das Symbol ✓ am Ende der Zeile, in der der Name des Sicherheitsprofils erscheint.

   Es wird eine Meldung angezeigt, um Sie zu informieren, dass bei der Anwendung der Anpassung alle Daten gelöscht werden und eine vollständige Analyse des überwachten Active Directory erforderlich ist, was einige Zeit dauern kann.

2. Klicken Sie auf **OK**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Anpassungsoptionen gespeichert hat. In der Spalte *Sicherheitsanalyse* in der Tabelle **Sicherheitsprofile** wird **Warten** angezeigt. Das bedeutet, dass die Analyse gemäß Ihrem Sicherheitsprofil darauf wartet, ausgeführt zu werden.

So verwerfen Sie die Anpassung:

- Sie haben folgende Möglichkeiten:
  - Klicken Sie im Bereich **Profilkonfiguration** in der unteren linken Ecke auf **Ausstehende Anpassungen wiederherstellen** oder
  - Klicken Sie im Bereich **Sicherheitsprofilverwaltung** auf das Symbol ↶ am Ende der Zeile, in der der Name des Sicherheitsprofils erscheint.

  Eine Meldung bestätigt, dass Tenable Identity Exposure die Anpassungsoptionen verworfen hat.

Siehe auch

- Anpassung eines Indikators präzisieren

Anpassung eines Indikators präzisieren

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

Zusätzliche Anpassungen an einem Indikator für ein Sicherheitsprofil ermöglichen es Ihnen, Indikatoroptionen für bestimmte Domänen auszuwählen. Standardmäßig gilt die globale Anpassung für alle Domänen.

So präzisieren Sie die Anpassung eines Indikators:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Sicherheitsprofilverwaltung**.

   Daraufhin wird der Bereich **Sicherheitsprofilverwaltung** angezeigt.

2. Fahren Sie mit dem Mauszeiger in der Liste der Sicherheitsprofile auf das Sicherheitsprofil, das den Indikator enthält, den Sie anpassen möchten. Klicken Sie auf das Symbol ✎ am Ende der Zeile, in der der Dateiname des Sicherheitsprofils erscheint.

   Daraufhin wird der Bereich **Profilkonfiguration** angezeigt.

3. Wählen Sie die Registerkarte für **Indicators of Exposure** oder **Indicators of Attack**.

4. (Optional) Geben Sie im Feld **Indikator suchen** einen Indikatornamen ein.

5. Klicken Sie auf den Namen des Indikators, der angepasst werden soll.

   Daraufhin wird der Bereich **Indikatoranpassung** angezeigt.

6. Klicken Sie neben der Registerkarte **Globale Anpassung** auf das Symbol +.

   Die Registerkarte **Anpassung Nr. 1** wird angezeigt.

7. Klicken Sie auf das Feld **Anwenden auf**.

   Der Fensterbereich **Gesamtstrukturen und Domänen** wird angezeigt.

8. (Optional) Geben Sie in das Suchfeld den Namen der Gesamtstruktur oder der Domäne ein.

9. Wählen Sie die Domäne aus.

10. Klicken Sie auf **Auswahlbasierter Filter**.

11. Nehmen Sie bei Bedarf weitere Anpassungen des Indikators für den ausgewählten Bereich vor.
12. Klicken Sie auf **Als Entwurf speichern**.

So verwerfen Sie die Anpassung:

1. Klicken Sie auf die Registerkarte für die Anpassung.
2. Klicken Sie unten im Bereich auf **Diese Konfiguration entfernen**.

Siehe auch

- Indikator anpassen

Benutzerrollen

Tenable Identity Exposure nutzt die rollenbasierte Zugriffssteuerung (RBAC), um den Zugang zu Daten und Funktionen in Ihrer Organisation abzusichern. Rollen bestimmen, auf welche Art von Informationen ein Benutzer über sein Konto zugreifen kann, abhängig von seiner Rolle.

Benutzer mit den entsprechenden Berechtigungen können anderen Benutzern auf der Grundlage ihrer jeweiligen Rolle Berechtigungen zur Durchführung der folgenden Aktionen zuweisen:

- Inhalte und Menüs sowie System- und Indicator of Exposure-Konfigurationen lesen.
- Inhalte und Menüs sowie System- und Indicator of Attack-Konfigurationen bearbeiten.
- Konten, Sicherheitsprofile und Rollen erstellen.

Siehe auch

- Rollen verwalten
- Berechtigungen für eine Rolle festlegen
- Berechtigungen für Entitäten der Benutzeroberfläche festlegen (Beispiel)

Rollen verwalten

So erstellen Sie eine neue Rolle:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Rollenverwaltung**.
2. Klicken Sie oben rechts auf die Schaltfläche **Rolle erstellen**.

   Daraufhin wird der Bereich **Rolle erstellen** angezeigt.
3. Geben Sie in das Feld „Name“ einen Namen für die Rolle ein.
4. Geben Sie in das Feld „Beschreibung“ einige Informationen zur Rolle ein.
5. Klicken Sie unten rechts auf **Hinzufügen**.

   Es erscheint eine Meldung, die bestätigt, dass Tenable Identity Exposure die Rolle erstellt hat. Der Bereich **Rolle bearbeiten** wird angezeigt. Dort können Sie die Berechtigungen für die Rolle festlegen.

Hinweis: Sie können die Tenable Identity Exposure-Administratorrolle („Globaler Administrator“ genannt) nicht ändern. Klicken Sie auf das Symbol 👁, um die Rolleneinstellungen von Tenable Identity Exposure anzuzeigen.

So löschen Sie eine Rolle:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Rollenverwaltung**.
2. Fahren Sie mit dem Mauszeiger in der Liste der Rollen über die Rolle, die Sie löschen möchten, und klicken Sie rechts auf das Symbol 🗑.

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.
3. Klicken Sie auf „Löschen“.

   Es erscheint eine Meldung, die das Löschen der Rolle bestätigt.

Siehe auch

- Berechtigungen für eine Rolle festlegen

Berechtigungen für eine Rolle festlegen

Erforderliche Benutzerrolle: Administrator oder Organisationsbenutzer mit entsprechenden Berechtigungen.

Tenable Identity Exposure nutzt die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC), um den Zugang zu seinen Daten abzusichern. Eine Rolle bestimmt, auf welche Art von Informationen Benutzer abhängig von ihrer funktionalen Rolle im Unternehmen zugreifen können. Wenn Sie einen neuen Benutzer in Tenable Identity Exposure anlegen, weisen Sie diesem Benutzer eine bestimmte Rolle mit den dazugehörigen Berechtigungen zu.

So legen Sie Berechtigungen für eine Rolle fest:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Rollenverwaltung**.
2. Fahren Sie mit dem Mauszeiger über die Rolle, für die Sie Berechtigungen festlegen möchten, und klicken Sie rechts auf das Symbol .

   Der Bereich **Rolle bearbeiten** wird angezeigt.
3. Wählen Sie unter **Berechtigungsverwaltung** einen Entitätstypen:
   - Datenentitäten
   - Benutzerentitäten
   - Systemkonfigurationsentitäten
   - Schnittstellenentitäten
4. Wählen Sie in der Liste der Entitätsnamen die Entität aus, für die Sie Berechtigungen festlegen möchten.
5. Klicken Sie unter den Spalten **Lesen**, **Bearbeiten** oder **Erstellen** auf die Umschaltschaltfläche „Erteilt“ oder „Nicht autorisiert“.
6. Sie haben folgende Möglichkeiten:
   - Klicken Sie auf „Anwenden“, um die Berechtigung zu übernehmen, und lassen Sie den Fensterbereich **Rolle bearbeiten** für weitere Änderungen geöffnet.

- Klicken Sie auf „Anwenden“, um die Berechtigung zu übernehmen, und schließen Sie den Fensterbereich **Rolle bearbeiten**.

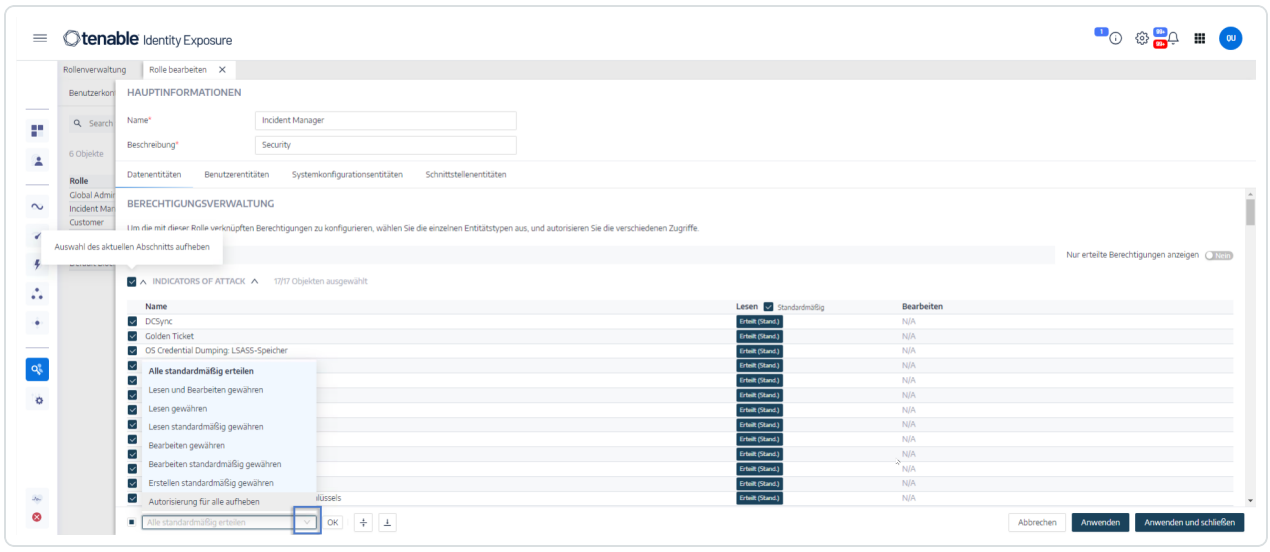
Eine Meldung bestätigt, dass Tenable Identity Exposure die Rolle aktualisiert hat.

So legen Sie Berechtigungen für eine Rolle per Massenvorgang fest:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Rollenverwaltung**.
2. Fahren Sie mit dem Mauszeiger über die Rolle, für die Sie Berechtigungen festlegen möchten, und klicken Sie rechts auf das Symbol .

   Der Bereich **Rolle bearbeiten** wird angezeigt.
3. Wählen Sie unter **Berechtigungsverwaltung** einen Entitätstypen.
4. Wählen Sie die Entitäten oder den/die Abschnitt(e) von Entitäten (z. B. Indicators of Exposure) aus, für die Sie Berechtigungen festlegen möchten.
5. Klicken Sie unten auf der Seite auf den Pfeil im Dropdown-Feld, um eine Liste der Berechtigungen anzuzeigen.
6. Wählen Sie die Berechtigung(en) für die Rolle aus.
7. Klicken Sie auf **OK**.

   Eine Nachricht bestätigt, dass Tenable Identity Exposure die Berechtigungen für die Entitäten festgelegt hat.



Berechtigungsarten

Berechtigung	Beschreibung
Lesen	Berechtigung zum Anzeigen eines Objekts oder einer Konfiguration
Bearbeiten	Berechtigung zum Bearbeiten eines Objekts oder einer Konfiguration. Erfordert Leseberechtigung, um Änderungen anzuwenden.
Erstellen	Berechtigung zum Erstellen eines Objekts oder einer Konfiguration. Die Berechtigung **Erstellen** erfordert die Berechtigungen **Lesen** und **Bearbeiten**, um erlaubte Aktionen für erlaubte Ressourcen durchzuführen.

Entitätstypen

Es gibt vier Arten von Entitäten in Tenable Identity Exposure, für die Zugriffsrechte erforderlich sind, die Sie für jede Benutzerrolle in Ihrer Organisation individuell anpassen können:

Entitätstyp	Enthält	Berechtigungen
Datenentitäten		
Diese Entität steuert die Berechtigungen zum Einrichten des überwachten Active Directory und zum Konfigurieren der Datenanalyse in Tenable Identity Exposure.	• Indicators of Attack • Indicators of Exposure • Gesamtstrukturen • Domänen • Profile • Benutzer • Warnungen per E-Mail • Warnungen per Syslog • Rollen • Entitäts-Relay • Berichte	Lesen, Bearbeiten, Erstellen
Benutzerentitäten		

Diese Entität steuert die Fähigkeit eines Benutzers, Informationen zu konfigurieren, die Tenable Identity Exposure für die Datenanalyse anzeigt, und persönliche Informationen und Einstellungen zu ändern.	• Voreinstellungen • Dashboards • Widgets • API-Schlüssel • Persönliche Informationen	Bearbeiten, Erstellen
Systemkonfigurationsentitäten		
Diese Entität steuert den Zugang zur Plattform und den Diensten von Tenable Identity Exposure.	• Anwendungsdienste (SMTP, Protokolle, Authentifizierung, Tenable Identity Exposure, Indicators of Attack, vertrauenswürdige Zertifizierungsstellen) • Bewertungen über öffentliche API • Lizenzen • LDAP-Authentifizierung • SAML-Authentifizierung **Hinweis**: Berechtigungen für die LDAP- und SAML-Authentifizierung sind nicht verfügbar, wenn Sie über eine Tenable Vulnerability Management-Lizenz verfügen. • Topologie	Lesen, Bearbeiten

	• Kontosperrrichtlinie • Domänen erneut durchforsten • Aktivitätsprotokolle • Tenable Cloud-Service (Tenable Cloud-Datensammlung) • Microsoft Entra ID-Unterstützung • Integritätsprüfungen • Nur die Spuren der Benutzer anzeigen	
Schnittstellenentitäten		
Diese Entität definiert die Zugriffsrechte auf bestimmte Teile der Benutzeroberfläche und Funktionen von Tenable Identity Exposure.	Zugangspfade zu bestimmten Tenable Identity Exposure-Funktionen. Weitere Informationen finden Sie unter Berechtigungen für Entitäten der Benutzeroberfläche festlegen (Beispiel).	Erteilt, Nicht autorisiert

Siehe auch

- Benutzerkonten
- Benutzerrollen

Berechtigungen für Entitäten der Benutzeroberfläche festlegen (Beispiel)

Tenable Identity Exposure wendet Berechtigungen entlang des Pfades an, über den der Zugriff auf eine bestimmte Funktion der Benutzeroberfläche erfolgt. Das folgende Beispiel zeigt, wie Sie Berechtigungen festlegen, um die Konfiguration von Syslog zu ermöglichen.

Um zu den Syslog-Parametern zu gelangen, benötigen die Benutzer unter Tenable Identity Exposure die Berechtigung **System** > **Konfiguration** > **SYSLOG**:

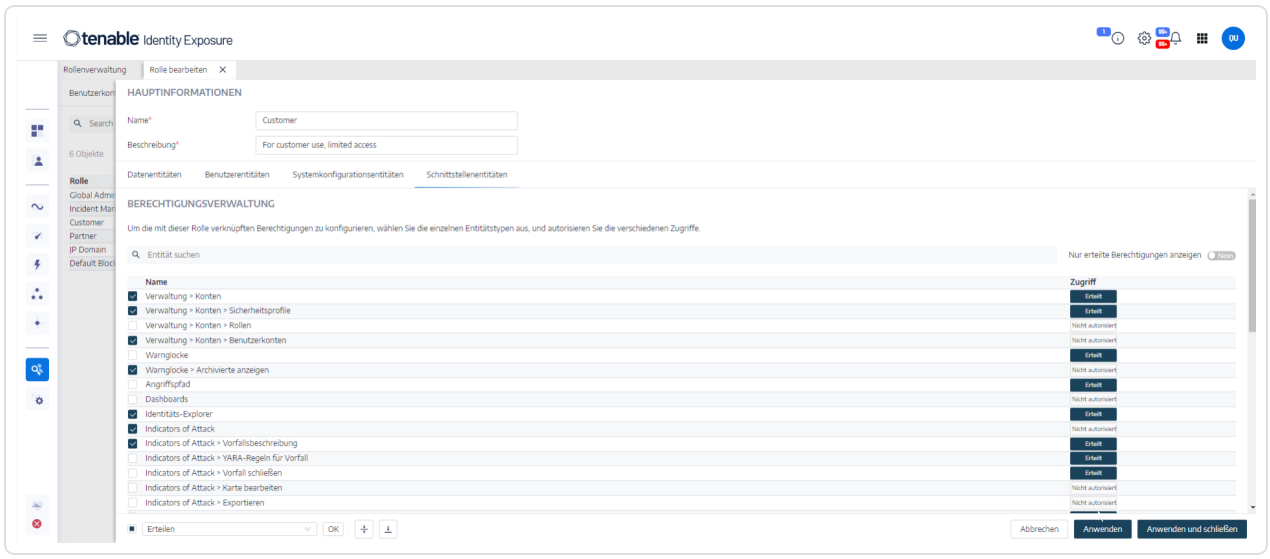
- Systemkonfiguration: **Verwaltung** > **System**
- Konfigurationsparameter: **Verwaltung** > **System** > **Konfiguration**
- Syslog-Warnungen: **Verwaltung** > **System** > **Konfiguration** > **Warnungsmodul** > **SYSLOG**

So legen Sie die Berechtigungen für die Syslog-Konfiguration fest:

1. Klicken Sie in Tenable Identity Exposure auf **Konten** > **Rollenverwaltung**.
2. Fahren Sie mit dem Mauszeiger über die Rolle, für die Sie Berechtigungen festlegen möchten, und klicken Sie rechts auf das Symbol .

   Der Bereich **Rolle bearbeiten** wird angezeigt.
3. Wählen Sie unter **Berechtigungsverwaltung** die Option **Schnittstellenentitäten**.
4. Gehen Sie in der Liste der Entitäten wie folgt vor:
   - Wählen Sie **Verwaltung** > **System** und klicken Sie auf die Umschalttaste „Zugriff“, um sie auf **Erteilt** zu stellen.
   - Wählen Sie **Verwaltung** > **System** > **Konfiguration** und klicken Sie auf die Umschalttaste „Zugriff“, um sie auf **Erteilt** zu stellen.
   - Wählen Sie **Verwaltung** > **System** > **Konfiguration** > **Warnungsmodul** > **SYSLOG** und klicken Sie auf die Umschalttaste „Zugriff“, um sie auf **Erteilt** zu stellen.
5. Klicken Sie auf **Anwenden**.

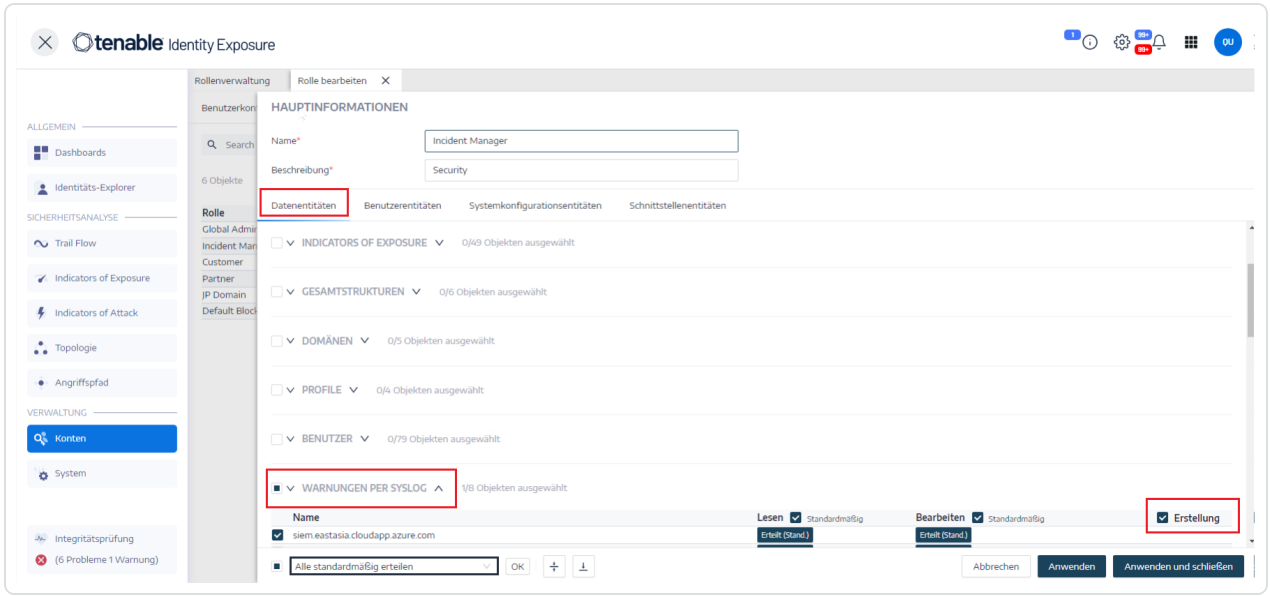
   Eine Meldung bestätigt, dass Tenable Identity Exposure die Berechtigungen für die Entitäten aktualisiert hat.



6. Wählen Sie unter **Berechtigungsverwaltung** die Option **Datenentitäten**.
7. Wählen Sie in der Liste der Entitätsabschnitte die Option **Warnungen per Syslog**.
8. Wählen Sie die Berechtigung **Erstellung**.

   Tenable Identity Exposure gewährt implizit die Berechtigungen zum Lesen und Bearbeiten.
9. Klicken Sie auf **Anwenden und schließen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Berechtigungen für die Entitäten aktualisiert hat.



Gesamtstrukturen

Eine Active Directory (AD)-Gesamtstruktur ist eine Sammlung von Domänen, die ein gemeinsames Schema, eine gemeinsame Konfiguration und gemeinsame Vertrauensstellungen aufweisen. Sie bietet eine hierarchische Struktur für die Verwaltung und Organisation von Ressourcen und ermöglicht so eine zentrale Verwaltung und sichere Authentifizierung über mehrere Domänen innerhalb eines Unternehmens.

Gesamtstrukturen verwalten

So fügen Sie eine Gesamtstruktur hinzu:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Gesamtstrukturverwaltung**.
2. Klicken Sie auf der rechten Seite auf **Gesamtstruktur hinzufügen**.

   Der Fensterbereich „Gesamtstruktur hinzufügen“ wird angezeigt.
3. Geben Sie im Feld **Name** den Namen für die Gesamtstruktur ein.
4. Geben Sie im Abschnitt **Konto** Folgendes für das Dienstkonto an, das Tenable Identity Exposure verwendet:

   - **Login**: Geben Sie den Namen des Dienstkontos ein.
     Format: Benutzerprinzipalname, wie `tenablead@domain.example.com` (empfohlen für Kompatibilität mit Kerberos-Authentifizierung) oder NetBIOS, wie `DomainNetBIOSName\SamAccountName`.
   - **Passwort**: Geben Sie das Passwort für das Dienstkonto ein.

   > **Hinweis**: Wenn Sie das AD-Dienstkonto von Tenable Identity Exposure als Mitglied der Gruppe „Geschützte Benutzer“ festlegen müssen, stellen Sie sicher, dass Ihre Tenable Identity Exposure-Konfiguration Kerberos-Authentifizierung unterstützt, da geschützte Benutzer die NTLM-Authentifizierung nicht verwenden können.
5. Klicken Sie auf **Hinzufügen**.

   Eine Meldung bestätigt das Hinzufügen der neuen Gesamtstruktur.

So bearbeiten Sie eine Gesamtstruktur:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Gesamtstrukturverwaltung**.
2. Fahren Sie in der Liste der Gesamtstrukturen mit dem Mauszeiger über die Gesamtstruktur, die Sie bearbeiten möchten, und klicken Sie rechts auf das Symbol ✎.

   Der Fensterbereich **Gesamtstruktur bearbeiten** wird angezeigt.
3. Ändern Sie diese nach Bedarf.

4. Klicken Sie auf **Bearbeiten**.

   In einer Meldung werden Sie informiert, dass Tenable Identity Exposure die Gesamtstruktur aktualisiert hat.

Schutz von Dienstkonten

Tenable empfiehlt, Dienstkonten zur Gewährleistung der Sicherheit zu schützen. Hierzu werden die Attribute der Benutzerkontensteuerung (User Account Control, UAC) ordnungsgemäß festgelegt, um eine Delegierung zu verhindern, eine Vorauthentifizierung zu erfordern, eine stärkere Verschlüsselung zu verwenden, den Ablauf und die Anforderungen von Passwörtern zu erzwingen sowie autorisierte Passwortänderungen zuzulassen. Durch diese Maßnahmen wird das Risiko eines unbefugten Zugriffs und möglicher Sicherheitsverletzungen gemindert und die Integrität der Systeme und Daten eines Unternehmens gewährleistet.

So ändern Sie Einstellungen mit einem Windows-Richtlinien-Editor:

Sie können die Einstellungen der Benutzerkontensteuerung mit dem Editor für lokale Sicherheitsrichtlinien oder dem Gruppenrichtlinien-Editor von Windows mit den entsprechenden Administratorrechten ändern.

- Navigieren Sie im Editor zu **Lokale Richtlinien** -> **Sicherheitsoptionen**, um die folgenden Einstellungen zu suchen und zu konfigurieren: (Dies kann je nach Windows-Version variieren.)
    - *„Netzwerkzugriff: Speicherung von Kennwörtern und Anmeldeinformationen für die Netzwerkauthentifizierung nicht zulassen“*: Legen Sie die Option auf **Aktiviert** fest.
    - *„Konten: Kerberos-Vorauthentifizierung nicht erforderlich“*: Legen Sie diese Option auf **Deaktiviert** fest.
    - *„Netzwerksicherheit: Für Kerberos zulässige Verschlüsselungstypen konfigurieren“*: Stellen Sie sicher, dass die Option *„Kerberos DES-Verschlüsselungstypen für diese Kontooption“* **nicht** aktiviert ist.
    - *„Konten: Maximales Kennwortalter“*: Legen Sie den Ablaufzeitraum des Passworts fest (z. B. 30, 60 oder 90 Tage, damit Folgendes gilt: `PasswordNeverExpires = FALSE`).
    - *„Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken“*: Legen Sie die Option auf **Deaktiviert** fest.
    - *„Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)“*: Legen Sie den gewünschten Wert fest, z. B. „10“, um Benutzern das Ändern ihrer Passwörter zu ermöglichen.

So ändern Sie Einstellungen mit PowerShell:

- Öffnen Sie PowerShell mit den entsprechenden Administratorrechten auf einem Computer, der AD hostet, und führen Sie den folgenden Befehl aus:

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

  Hierbei ist `<AD_ACCOUNT>` der Name des Active Directory-Kontos, das Sie ändern möchten.

Domänen

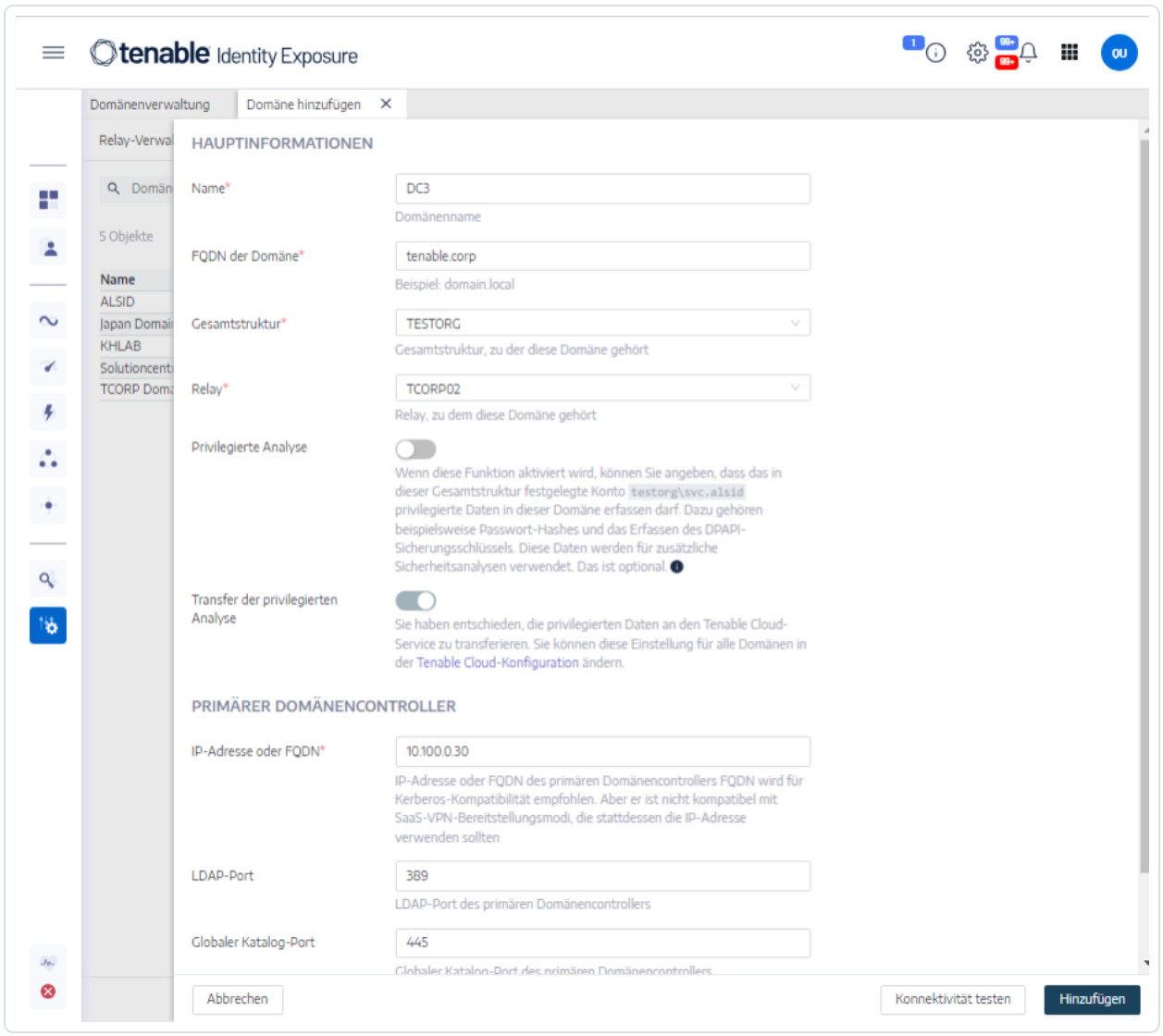
Tenable Identity Exposure überwacht Domänen, die Objekte mit gemeinsamen Einstellungen auf logische Weise für eine zentrale Verwaltung gruppieren.

So fügen Sie eine Domäne hinzu:

1. Klicken Sie in Tenable Identity Exposure auf **System**.
2. Klicken Sie auf die Registerkarte **Domänenverwaltung**.

   Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.
3. Klicken Sie oben rechts auf **Domäne hinzufügen**.

   Daraufhin wird der Fensterbereich **Domäne hinzufügen** angezeigt.



4. Geben Sie im Bereich **Hauptinformationen** folgende Informationen an:
    - Geben Sie den Domänennamen im Feld **Name** ein.
    - Geben Sie in das Feld **FQDN der Domäne** den vollständig qualifizierten Domänennamen (FQDN) für die Domäne ein.
    - Wählen Sie im Dropdown-Feld **Gesamtstruktur** die Gesamtstruktur aus, zu der die Domäne gehört.
5. **Privilegierte Analyse** (optional): Wenn Sie den Umschalter aktivieren, gestatten Sie dem Konto „dcadmin“ in dieser Gesamtstruktur, privilegierte Daten zu dieser Domäne zu erfassen, um erweiterte Sicherheitsanalysen durchzuführen.

6. **Transfer der privilegierten Analyse**: Weitere Informationen zu dieser Option finden Sie unter Tenable Cloud-Datensammlung.
7. Geben Sie im Abschnitt **Primärer Domänencontroller** folgende Informationen an:
    - Geben Sie im Feld **IP-Adresse oder Hostname** den Hostnamen des primären Domänencontrollers (erforderlich für Kompatibilität mit Kerberos-Authentifizierung, aber nicht kompatibel mit SaaS-VPN-Bereitstellungsmodi) oder die IP-Adresse ein.

      Tenable Identity Exposure unterstützt keinen Lastenausgleich.

    - Geben Sie in das Feld **LDAP-Port** den LDAP-Port des primären Domänencontrollers ein.

      Hinweis: Wenn Sie Port TCP/636 (LDAPS) verwenden, um eine Verbindung zu Ihrer Domäne herzustellen, muss Tenable Identity Exposure Zugriff auf das Zertifikat Ihrer Active Directory-Zertifizierungsstelle (CA) haben, um Ihr AD-Zertifikat zu validieren, damit die Verbindung hergestellt werden kann. In Secure Relay-Umgebungen können Sie das CA-Zertifikat auf dem Relay-Computer installieren. In VPN-Umgebungen ist diese Konfiguration nicht möglich.

    - Geben Sie in das Feld **Globaler Katalog-Port** den globalen Katalog-Port des primären Domänencontrollers ein.
    - Geben Sie in das Feld **SMB-Port** den SMB-Port des primären Domänencontrollers ein.
8. Klicken Sie auf **Hinzufügen**.

    Es wird eine Meldung angezeigt, die bestätigt, dass Tenable Identity Exposure die Domäne hinzugefügt hat.

So bearbeiten Sie eine Domäne:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme**.
2. Klicken Sie auf die Registerkarte **Domänenverwaltung**.

    Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.
3. Fahren Sie mit dem Mauszeiger über den Namen der Domäne, die Sie bearbeiten möchten, um das Symbol ✎ auf der rechten Seite anzuzeigen.

4. Klicken Sie auf das Symbol .

   Daraufhin wird der Fensterbereich **Domäne bearbeiten** angezeigt.

5. Bearbeiten Sie die Informationen für die Domäne.

6. Klicken Sie auf **Bearbeiten**.

   In einer Meldung wird bestätigt, dass Tenable Identity Exposure die Domäne aktualisiert hat.

So löschen Sie eine Domäne:

1. Klicken Sie in Tenable Identity Exposure auf **Systeme**.

2. Klicken Sie auf die Registerkarte **Domänenverwaltung**.

   Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.

3. Fahren Sie mit dem Mauszeiger über den Namen der Domäne, die Sie löschen möchten, um das Symbol anzuzeigen.

4. Klicken Sie auf das Symbol .

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.

5. Klicken Sie auf **Löschen**.

   In einer Meldung wird bestätigt, dass Tenable Identity Exposure die Domäne gelöscht hat.

Siehe auch

- Datenaktualisierung für eine Domäne erzwingen
- Honey-Konten
- Kerberos-Authentifizierung

Datenaktualisierung für eine Domäne erzwingen

So erzwingen Sie eine Datenaktualisierung für eine Domäne:

1. Klicken Sie in Tenable Identity Exposure auf **System**.
2. Klicken Sie auf die Registerkarte **Domänenverwaltung**.

   Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.
3. Fahren Sie mit dem Mauszeiger über den Namen der Domäne, für die Sie eine Datenaktualisierung erzwingen möchten, um das Symbol ↻ auf der rechten Seite anzuzeigen.
4. Klicken Sie auf das Symbol ↻.

   Es erscheint eine Meldung mit Informationen über die Datenaktualisierung.
5. Klicken Sie auf **Bestätigen**.

Siehe auch

- Honey-Konten

Honey-Konten

Erforderliche Benutzerrolle: Administrator auf dem lokalen Computer.

Bei einem Honey-Konto handelt es sich um ein Scheinkonto, dessen einziger Zweck es ist, einen Angreifer zu erkennen, der versucht, das Netzwerk über Active Directory zu kompromittieren.

Es ist eine Voraussetzung für Indicators of Attack von Tenable Identity Exposure, um Kerberoasting-Angriffsversuche zu erkennen, die darauf abzielen, Zugang zu Dienstkonten zu erhalten, indem sie Diensttickets anfordern und extrahieren und dann die Anmeldedaten des Dienstkontos offline knacken. Der Kerberoasting-Indicator of Attack sendet Warnmeldungen aus, wenn das Honey-Konto Login-Versuche oder Ticketanfragen erhält.

Pro Domäne weisen Sie ein Honey-Konto zu. Honey-Konten sind nicht mit Sicherheitsprofilen verbunden.

So fügen Sie ein Honey-Konto hinzu:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Domänenverwaltung**.

   Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.

2. Bewegen Sie den Mauszeiger über die Domäne, für die Sie ein Honey-Konto hinzufügen möchten.

3. Klicken Sie unter **Honey-Konto-Konfigurationsstatus** auf **+**.

   Der Fensterbereich **Honey-Konto hinzufügen** wird angezeigt.

4. Geben Sie im Feld **Name** einen Distinguished Name (DN) für das Benutzerkonto ein, das als Honey-Konto verwendet werden soll.

   Tipp: Sie können eine beliebige Zeichenfolge eingeben. Tenable Identity Exposure sucht dann nach übereinstimmenden Benutzerkontonamen und zeigt diese im Dropdown-Feld an, wenn das Benutzerkonto bereits im Active Directory vorhanden ist.

5. Im Abschnitt **Bereitstellung** generiert Tenable Identity Exposure ein Skript mit den entsprechenden Einstellungen, das Sie zur Bereitstellung des Honey-Kontos ausführen können. Klicken Sie auf ❐, um dieses Skript zu kopieren.

6. Klicken Sie auf **Hinzufügen**.

Es wird eine Meldung angezeigt, die bestätigt, dass Tenable Identity Exposure das Honey-Konto hinzugefügt hat. Im Bereich „Domänenverwaltung“ wird der **Honey-Konto-Konfigurationsstatus** für die ausgewählte Domäne orange (●) angezeigt. Das weist darauf hin, dass Sie das Skript zur Bereitstellung des Honey-Kontos ausführen müssen, um es zu aktivieren.

> **Hinweis**: Wenn der **Honey-Konto-Konfigurationsstatus** rot angezeigt wird (●), bedeutet das, dass Tenable Identity Exposure dieses Benutzerkonto nicht im Active Directory gefunden hat. Sie müssen dieses Benutzerkonto erstellen und mit dem nächsten Schritt fortfahren.

7. Führen Sie in einer Windows-PowerShell auf einem Computer mit dem Active Directory-Modul das kopierte Skript zur Bereitstellung des Honey-Kontos aus.

   Im Bereich **Domänenverwaltung** wird der **Honey-Konto-Konfigurationsstatus** der ausgewählten Domäne mit einem grünen Status (●) angezeigt. Das weist darauf hin, dass es aktiv ist.

   > **Hinweis**: In Tenable Identity Exposure kann es einige Zeit dauern, bis das Honey-Konto bearbeitet und aktiviert ist.

So bearbeiten Sie ein Honey-Konto:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Domänenverwaltung**.

   Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.

2. Bewegen Sie den Mauszeiger über die Domäne, für die Sie ein Honey-Konto hinzufügen möchten.

3. Klicken Sie unter **Honey-Konto-Konfigurationsstatus** rechts auf das Symbol .

   Der Fensterbereich **Honey-Konto bearbeiten** wird angezeigt.

4. Ändern Sie im Feld **Name** das Benutzerkonto nach Bedarf.

5. Klicken Sie im Abschnitt **Bereitstellung** auf , um das Bereitstellungsskript des Honey-Kontos zu kopieren.

6. Klicken Sie auf **Bearbeiten**.

Es wird eine Meldung angezeigt, die bestätigt, dass Tenable Identity Exposure das Honey-Konto aktualisiert hat. Im Bereich „Domänenverwaltung“ wird der **Honey-Konto-Konfigurationsstatus** für die ausgewählte Domäne orange (●) angezeigt. Das weist darauf hin, dass Sie das Skript zur Bereitstellung des Honey-Kontos ausführen müssen, um es zu aktivieren.

> **Hinweis**: Wenn der **Honey-Konto-Konfigurationsstatus** rot angezeigt wird (●), bedeutet das, dass Tenable Identity Exposure dieses Benutzerkonto nicht im Active Directory gefunden hat. Sie müssen dieses Benutzerkonto erstellen und mit dem nächsten Schritt fortfahren.

7. Führen Sie in einer Windows-PowerShell auf einem Computer mit dem Active Directory-Modul das kopierte Skript zur Bereitstellung des Honey-Kontos aus.

   Im Bereich **Domänenverwaltung** wird der **Honey-Konto-Konfigurationsstatus** der ausgewählten Domäne mit einem grünen Status (●) angezeigt. Das weist drauf hin, dass es konfiguriert ist.

   > **Hinweis**: In Tenable Identity Exposure kann einige Zeit dauern, bis das Honey-Konto bearbeitet und aktiviert ist.

So löschen Sie ein Honey-Konto:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Domänenverwaltung**.

   Daraufhin wird der Fensterbereich **Domänenverwaltung** angezeigt.

2. Bewegen Sie den Mauszeiger über die Domäne, für die Sie ein Honey-Konto hinzufügen möchten.

3. Klicken Sie unter **Honey-Konto-Konfigurationsstatus** rechts auf das Symbol .

   Der Fensterbereich **Honey-Konto bearbeiten** wird angezeigt.

4. Klicken Sie auf **Löschen**.

   Es wird eine Meldung angezeigt, die bestätigt, dass Tenable Identity Exposure das Honey-Konto gelöscht hat.

Siehe auch

- Datenaktualisierung für eine Domäne erzwingen

Kerberos-Authentifizierung

Tenable Identity Exposure authentifiziert sich bei den konfigurierten Domänencontrollern mit den von Ihnen bereitgestellten Anmeldeinformationen. Diese DCs akzeptieren entweder NTLM- oder Kerberos-Authentifizierung. NTLM ist ein älteres Protokoll mit dokumentierten Sicherheitsproblemen. Microsoft und alle Cybersicherheitsstandards raten jetzt von seiner Verwendung ab. Kerberos hingegen ist ein robusteres Protokoll, das Sie in Betracht ziehen sollten. Windows versucht die Authentifizierung immer zuerst über Kerberos und greift nur auf NTLM zurück, wenn Kerberos nicht verfügbar ist.

Tenable Identity Exposure ist mit wenigen Ausnahmen sowohl mit NTLM als auch mit Kerberos kompatibel. Tenable Identity Exposure priorisiert Kerberos als bevorzugtes Protokoll, wenn alle erforderlichen Bedingungen erfüllt sind. In diesem Abschnitt werden die Anforderungen beschrieben und Sie erfahren, wie Sie Tenable Identity Exposure konfigurieren müssen, um die Verwendung von Kerberos sicherzustellen.

Die Verwendung von NTLM anstelle von Kerberos ist auch der Grund, warum die SYSVOL-Härtung die Funktion von Tenable Identity Exposure stört. Weitere Informationen finden Sie unter Störung des Tenable Identity Exposure-Betriebs durch SYSVOL-Härtung.

Kompatibilität mit Tenable Identity Exposure-Bereitstellungsmodi

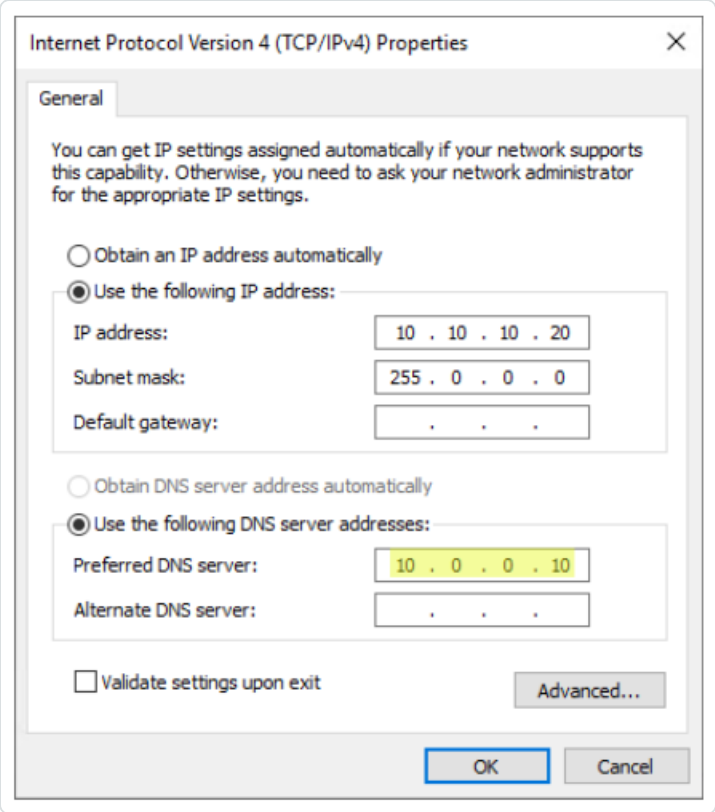
Bereitstellungsmodus	Kerberos-Unterstützung
On-Premises	Ja
SaaS-TLS (älter)	Ja
SaaS mit Secure Relay	Ja
SaaS mit VPN	Nein – Sie müssen für Ihre Installation in den Secure Relay-Bereitstellungsmodus wechseln.

Technische Anforderungen

- **Das in Tenable Identity Exposure konfigurierte AD-Dienstkonto muss einen UserPrincipalName (UPN) haben.** Entsprechende Anweisungen finden Sie unter Konfiguration

von Dienstkonto und Domäne.

- **Die DNS-Konfiguration und der DNS-Server müssen die Auflösung aller erforderlichen DNS-Einträge zulassen** – Sie müssen den Directory Listener- oder Relay-Computer so konfigurieren, dass er DNS-Server verwendet, die die Domänencontroller kennen. Wenn der Directory Listener- oder Relay-Computer in eine Domäne eingebunden ist, (wird von Tenable Identity Exposure nicht empfohlen), sollte diese Anforderung bereits erfüllt sein. Am einfachsten ist es, den Domänencontroller selbst als bevorzugten DNS-Server zu verwenden, da er normalerweise auch DNS ausführt. Beispiel:



> **Hinweis**: Wenn der Directory Listener- oder Relay-Computer mit mehreren Domänen und möglicherweise in mehreren Gesamtstrukturen verbunden ist, stellen Sie sicher, dass die konfigurierten DNS-Server alle erforderlichen DNS-Einträge für alle Domänen auflösen können. Andernfalls müssen Sie mehrere Directory Listener- oder Relay-Computer einrichten.

- **Erreichbarkeit des Kerberos-„Servers" (KDC)** – Dies erfordert eine Netzwerkverbindung vom Directory Listener- oder Relay-Computer zu Domänencontrollern über Port TCP/88. Wenn der Directory Listener- oder Relay-Computer in eine Domäne eingebunden ist, (wird von Tenable nicht empfohlen), sollte diese Anforderung bereits erfüllt sein. Jede konfigurierte Tenable

Identity Exposure-Gesamtstruktur erfordert eine Kerberos-Netzwerkverbindung zu mindestens einem Domänencontroller in ihrer jeweiligen Domäne, die das Dienstkonto enthält, sowie mindestens einem Domänencontroller in jeder verbundenen Domäne.

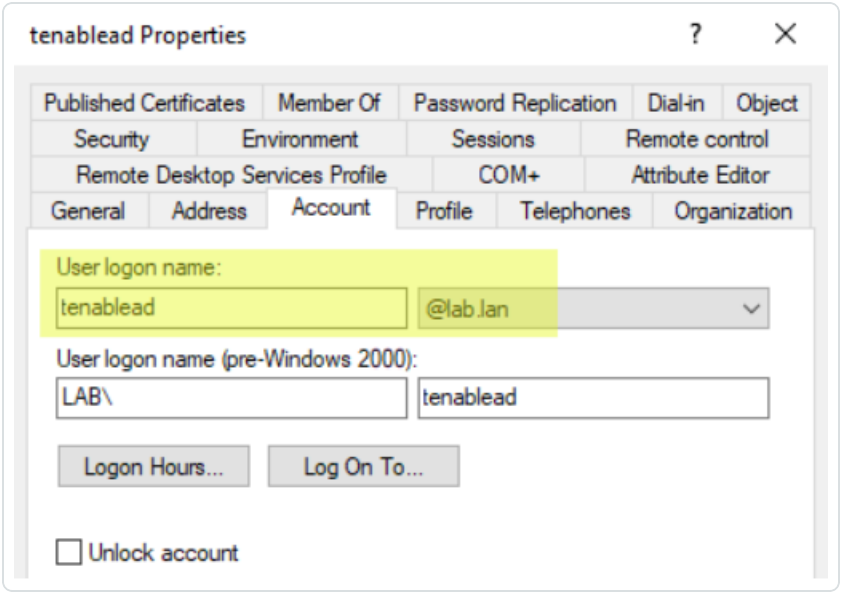
Weitere Informationen zu den Anforderungen finden Sie unter Network Flow Matrix und TLS Network Matrix.

> **Hinweis**: Der Directory Listener- oder Relay-Computer muss nicht in eine Domäne eingebunden sein, um Kerberos zu verwenden.

Konfiguration von Dienstkonto und Domäne

So konfigurieren Sie das AD-Dienstkonto und die AD-Domäne in Tenable Identity Exposure für die Verwendung von Kerberos:

1. Verwenden Sie für den Login das UserPrincipalName (UPN)-Format. In diesem Beispiel lautet das UPN-Attribut „`tenablead@lab.lan`“.
    a. Suchen Sie wie folgt nach dem UPN-Attribut in der Domäne der Gesamtstruktur, die das Dienstkonto enthält:



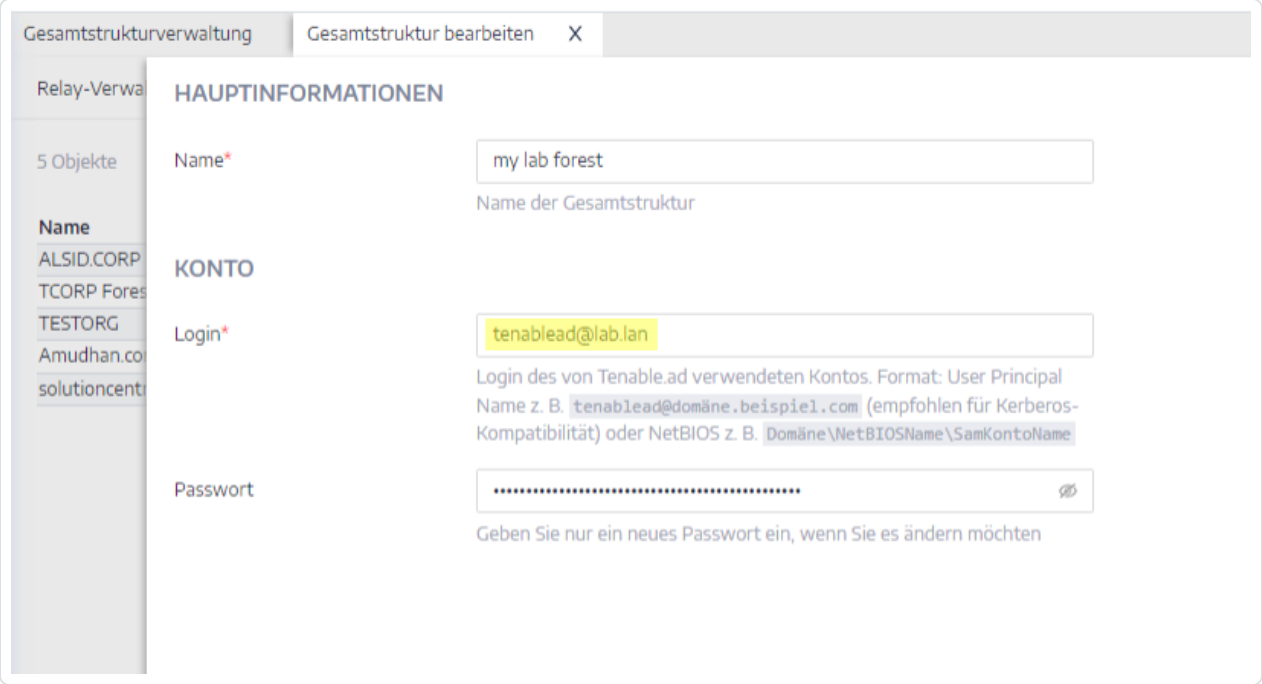

```
PS C:\Users\admin> Get-ADUser tenablead


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
```

> **Hinweis**: Der UPN sieht aus wie eine E-Mail-Adresse und ist sogar oft – aber nicht immer – mit der E-Mail-Adresse des Benutzers identisch.

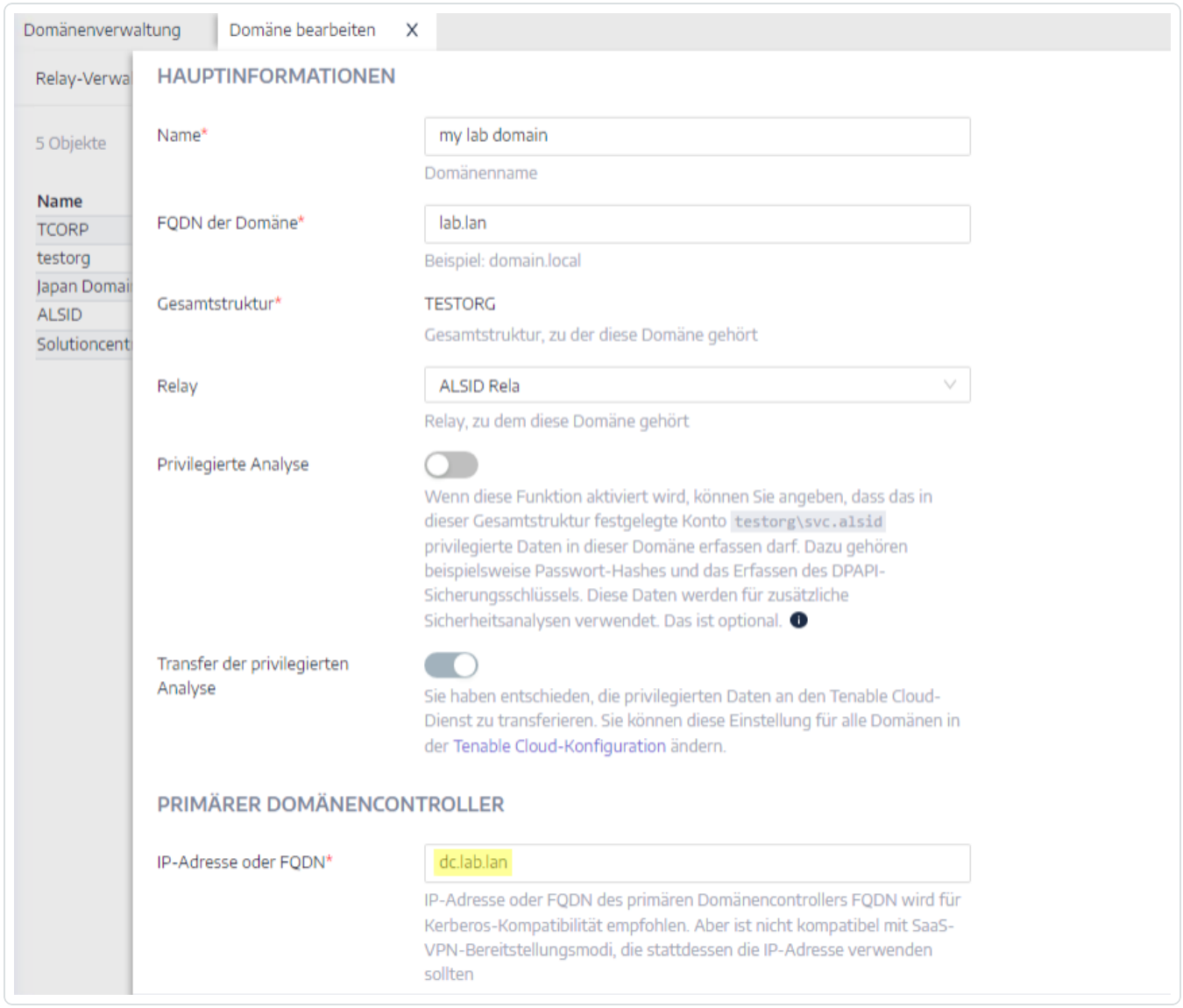
b. Legen Sie in Tenable Identity Exposure im Abschnitt zur Konfiguration der Gesamtstruktur diesen UPN anstelle des kurzen Format „`Benutzername`“ oder des

NetBIOS-Formats „`Domäne\Benutzername`“ wie folgt fest:



2. Verwenden Sie den vollständig qualifizierten Domänennamen (FQDN). Legen Sie in der Domänenkonfiguration in Tenable Identity Exposure für den primären Domänencontroller

(PDC) den FQDN anstelle der IP-Adresse fest.

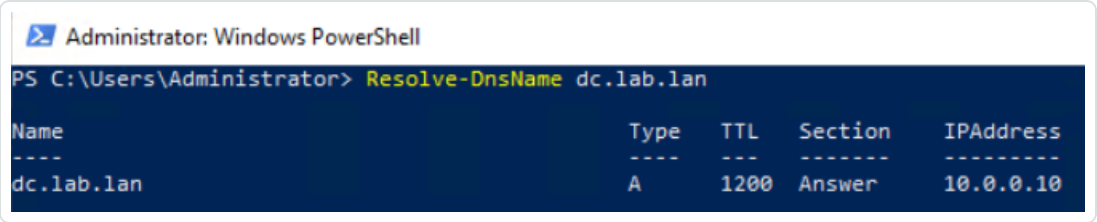


Fehlerbehebung

Für die ordnungsgemäße Funktion von Kerberos sind mehrere Konfigurationsschritte erforderlich. Andernfalls greift Windows – und durch die Erweiterung auch Tenable Identity Exposure – stillschweigend auf die NTLM-Authentifizierung zurück.

DNS

Stellen Sie sicher, dass die DNS-Server, die auf dem Directory Listener- oder Relay-Computer verwendet werden, den bereitgestellten PDC-FQDN auflösen können, wie z. B.:



Kerberos

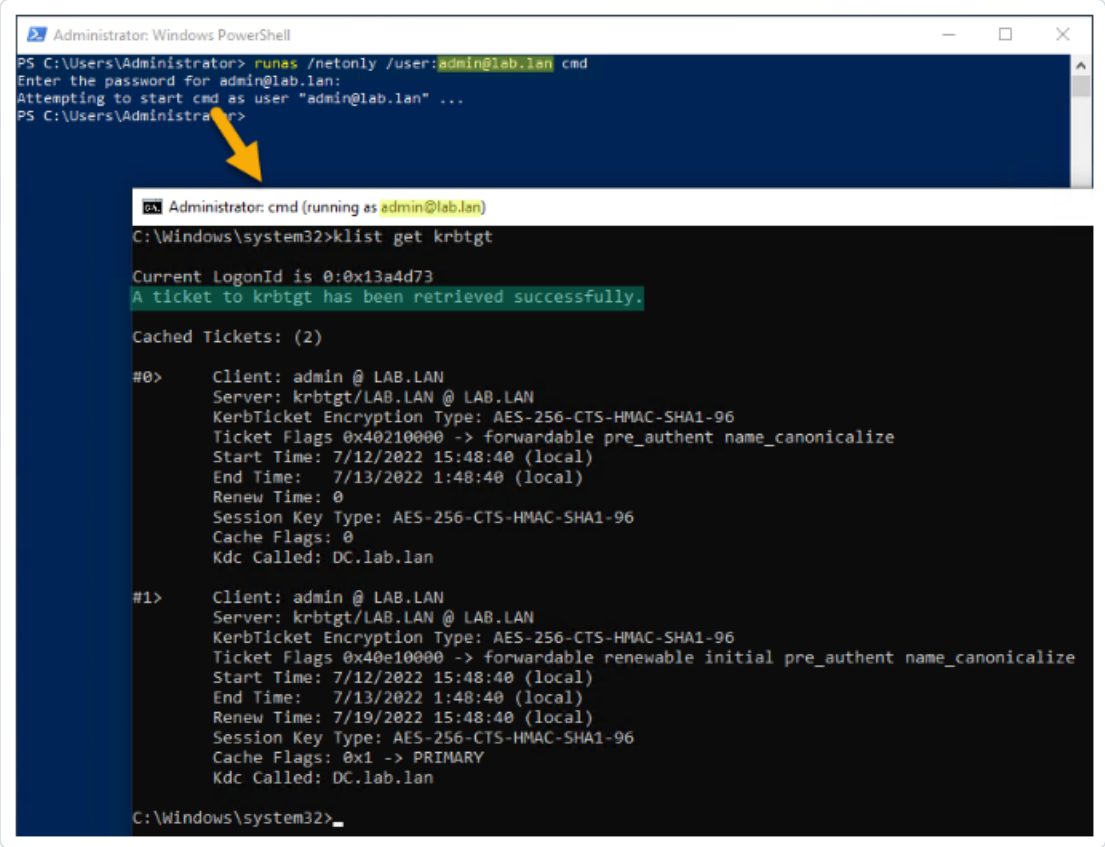
So überprüfen Sie, ob Kerberos mit den Befehlen funktioniert, die Sie auf dem Directory Listener- oder Relay-Computer ausführen:

1. Stellen Sie sicher, dass das in Tenable Identity Exposure konfigurierte AD-Dienstkonto ein TGT abrufen kann:

    a. Führen Sie in einer Befehlszeile oder in PowerShell den Befehl „`runas /netonly /user:<UPN> cmd`“ aus und geben Sie das Passwort ein. Seien Sie beim Eingeben oder Einfügen des Passworts besonders vorsichtig, da aufgrund des Flags „`/netonly`“ keine Überprüfung erfolgt.

    b. Führen Sie an der zweiten Eingabeaufforderung „`klist get krbtgt`“ aus, um ein TGT-Ticket anzufordern.

    Das folgende Beispiel zeigt ein erfolgreiches Ergebnis:



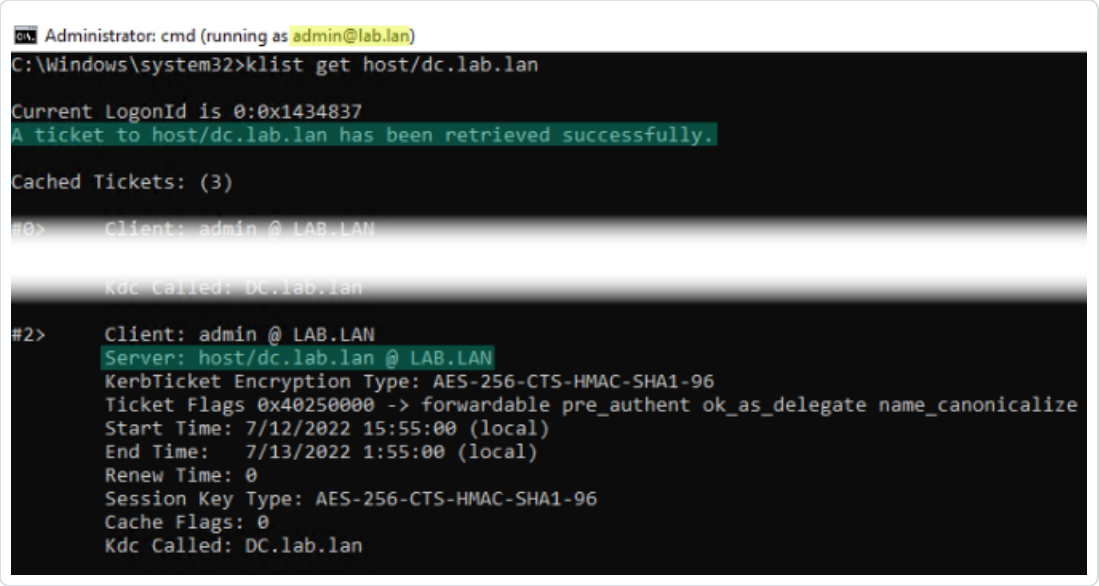
Mögliche Fehlercodes:

- `0xc0000064`: „Benutzeranmeldung mit falsch geschriebenem oder ungültigem Benutzerkonto“ -> Überprüfen Sie den Login (d. h. den Teil vor dem „@“ im UPN).
- `0xc000006a`: „Benutzeranmeldung mit falsch geschriebenem oder ungültigem Passwort“ -> Überprüfen Sie das Passwort.
- `0xc000005e`: „Zurzeit sind keine Anmeldeserver verfügbar, um die Anmeldeanforderung zu verarbeiten.“ -> Überprüfen Sie, ob die DNS-Auflösung funktioniert und ob der Server die zurückgegebenen KDCs kontaktieren kann usw.
- Andere Fehlercodes: Siehe die Microsoft-Dokumentation zu 4625-Ereignissen.

2. Stellen Sie sicher, dass der in Tenable Identity Exposure konfigurierte Domänencontroller ein Dienstticket abrufen kann. Führen Sie in derselben zweiten Eingabeaufforderung „`klist get`

host/<DC_FQDN>“ aus (ersetzen Sie „<DC_FQDN>“).

Das folgende Beispiel zeigt ein erfolgreiches Ergebnis:



Warnmeldungen

Lizenz erforderlich: Je nach Art der Warnmeldung, die Sie senden möchten, benötigen Sie möglicherweise Lizenzen für Indicators of Attack oder Indicators of Exposure.

Das Warnsystem von Tenable Identity Exposure hilft Ihnen, Sicherheitsmängel und/oder Angriffe auf Ihr überwachtes Active Directory zu erkennen. Es liefert Analysedaten zu Schwachstellen und Angriffen in Echtzeit per E-Mail oder Syslog-Benachrichtigung.

- SMTP-Serverkonfiguration
- E-Mail-Warnmeldungen
- Syslog-Warnmeldungen
- Details zu Syslog- und E-Mail-Warnungen

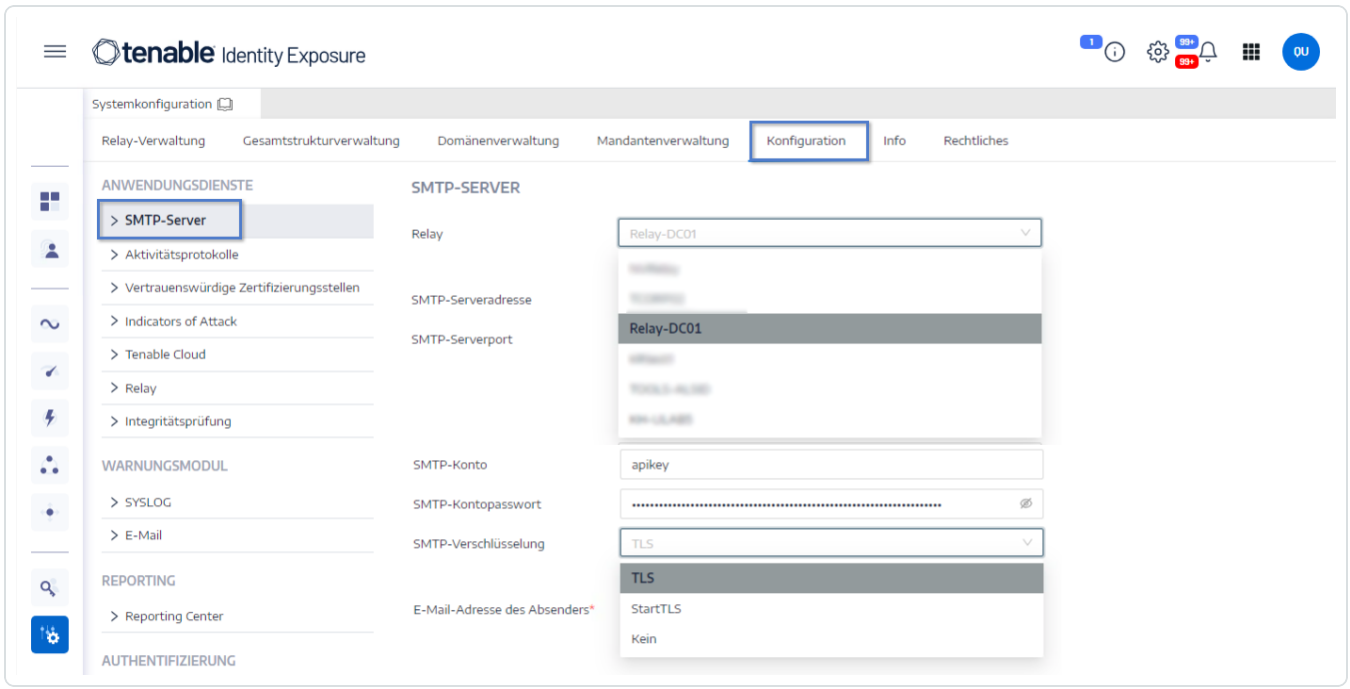
SMTP-Serverkonfiguration

Tenable Identity Exposure erfordert die Konfiguration des Simple Mail Transfer Protocol (SMTP), um Warnmeldungen zu versenden.

So konfigurieren Sie den SMTP-Server:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration**.
2. Wählen Sie unter **Anwendungsdienste** die Option **SMTP-Server**.

   Der Bereich **SMTP-Server** wird geöffnet.



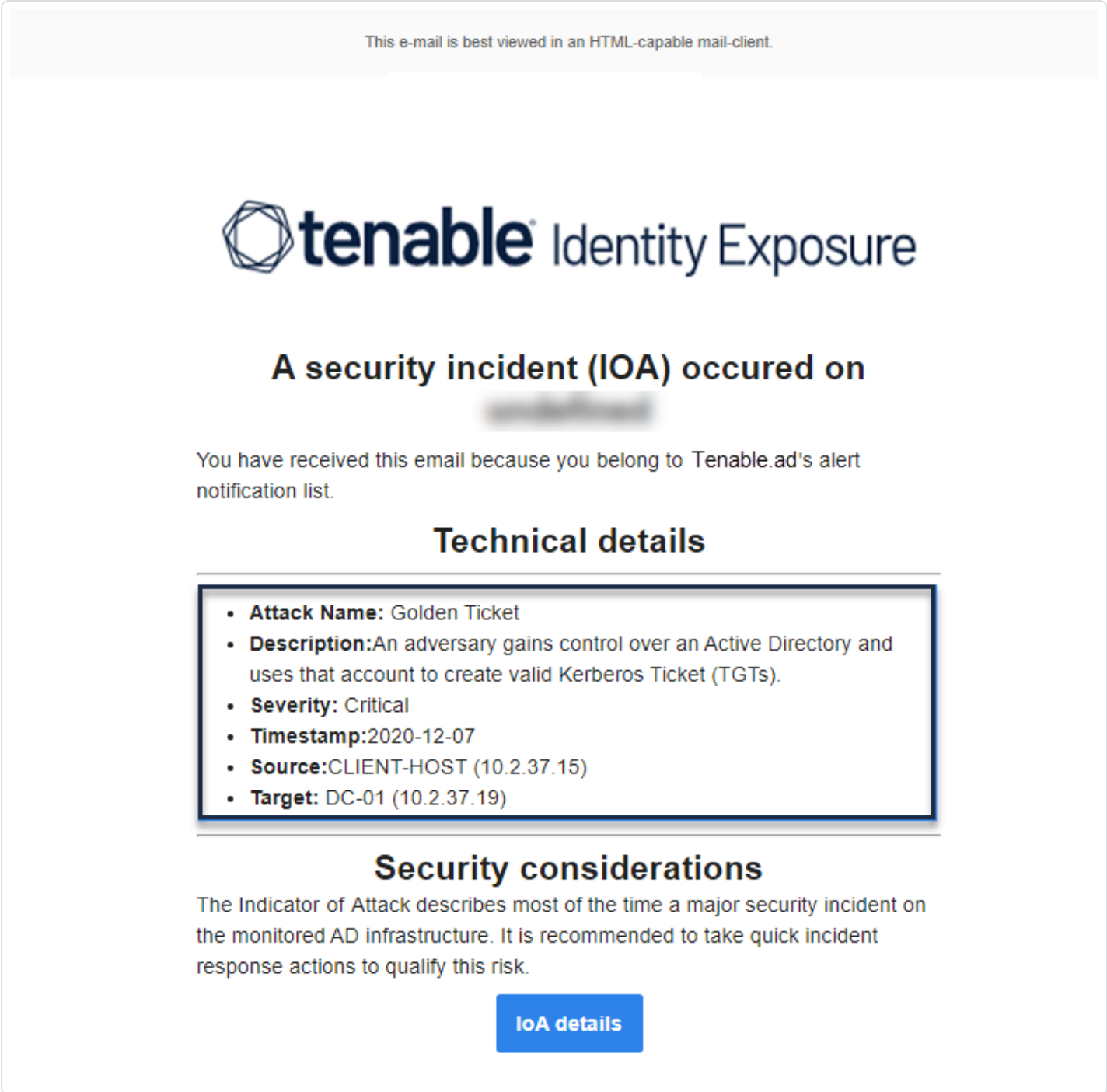
3. **Wenn Ihr Netzwerk Secure Relay verwendet:** Klicken Sie im Feld **Relay** auf den Pfeil, um aus der Dropdown-Liste ein Relay auszuwählen, das mit Ihrem SMTP-Server kommunizieren soll.
4. Geben Sie folgende Informationen an:
   - SMTP-Serveradresse
   - SMTP-Serverport
   - SMTP-Konto
   - SMTP-Kontopasswort

5. Klicken Sie im Feld „SMTP-Verschlüsselung“ auf den Pfeil, um eine Verschlüsselungsmethode in der Dropdown-Liste auszuwählen.
6. Geben Sie im Feld **E-Mail-Adresse des Absenders** eine E-Mail-Adresse an, die Tenable Identity Exposure beim Senden von E-Mails verwenden soll.
7. Klicken Sie auf **Speichern**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die SMTP-Parameter aktualisiert hat.

E-Mail-Warnmeldungen

Tenable Identity Exposure versendet E-Mail-Warnungen, um Sie automatisch zu benachrichtigen, wenn Ereignisse einen bestimmten Schweregrad erreichen und Behebungsmaßnahmen erfordern. Im Folgenden finden Sie ein Beispiel für eine E-Mail-Warnung:



So fügen Sie eine E-Mail-Warnung hinzu:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration** > **E-Mail**.
2. Klicken Sie auf der rechten Seite auf die Schaltfläche **E-Mail-Warnung hinzufügen**.

   Daraufhin öffnet sich der Bereich **E-Mail-Warnung hinzufügen**.
3. Geben Sie unter dem Abschnitt **Hauptinformationen** Folgendes an:
   - Geben Sie in das Feld **E-Mail-Adresse** die E-Mail-Adresse des Empfängers ein, der benachrichtigt werden soll.
   - Geben Sie in das Feld **Beschreibung** eine Beschreibung für die Empfängeradresse ein.
4. Wählen Sie in der Dropdown-Liste **Warnung auslösen** eine der folgenden Optionen:
   - **Bei jeder Abweichung**: Tenable Identity Exposure sendet eine Benachrichtigung bei jeder abweichenden IoA-Erkennung.
   - **Bei jedem Angriff**: Tenable Identity Exposure sendet eine Benachrichtigung bei jeder abweichenden IoA-Erkennung.
   - **Bei Integritätsprüfung-Statusänderung**: Tenable Identity Exposure sendet eine Benachrichtigung, wenn sich der Status für eine Integrationsprüfung ändert.
5. Klicken Sie in das Feld **Profile**, um Profile auszuwählen, die für diese E-Mail-Warnung verwendet werden sollen (falls zutreffend).
6. **Warnungen senden, wenn während der anfänglichen Analysephase Abweichungen festgestellt werden**: Führen Sie eine der folgenden Aktionen aus (falls zutreffend):
   - Aktivieren Sie das Kontrollkästchen: Tenable Identity Exposure verschickt eine große Anzahl von E-Mail-Benachrichtigungen, wenn ein Systemneustart Warnungen auslöst.
   - Deaktivieren Sie das Kontrollkästchen: Tenable Identity Exposure verschickt keine E-Mail-Benachrichtigungen, wenn ein Systemneustart Warnungen auslöst.
7. **Schweregrad-Schwellenwert**: Klicken Sie auf den Pfeil des Dropdown-Feldes, um den Schwellenwert auszuwählen, bei dem Tenable Identity Exposure Warnungen sendet (falls zutreffend).
8. Abhängig von dem zuvor ausgewählten Warnungsauslöser:

- **Indicators of Exposure**: Wenn Sie festgelegt haben, dass Warnungen **bei jeder Abweichung** ausgelöst werden, klicken Sie auf den Pfeil neben den einzelnen Schweregradstufen, um die Liste der Indicators of Exposure zu erweitern und die Indikatoren auszuwählen, für die Warnungen gesendet werden sollen.
- **Indicators of Attack**: Wenn Sie festgelegt haben, dass Warnungen **bei jedem Angriff** ausgelöst werden, klicken Sie auf den Pfeil neben jeder Schweregradstufe, um die Liste der Indicators of Attack zu erweitern und die Indikatoren auszuwählen, für die Warnungen gesendet werden sollen.
- **Bei Integritätsprüfung-Statusänderung**: Klicken Sie auf **Integritätsprüfungen**, um den Typ der Integritätsprüfung auszuwählen, bei dem eine Warnung ausgelöst werden soll. Klicken Sie dann auf **Auswahlbasierter Filter**.

9. Klicken Sie auf das Feld **Domänen**, um die Domänen auszuwählen, für die Tenable Identity Exposure Warnungen versendet.

   Der Fensterbereich „Gesamtstrukturen und Domänen“ wird angezeigt.

   a. Wählen Sie die Gesamtstruktur oder Domäne aus.

   b. Klicken Sie auf **Auswahlbasierter Filter**.

10. Klicken Sie auf **Konfiguration testen**.

    Eine Meldung bestätigt, dass Tenable Identity Exposure eine E-Mail-Warnung an den Server gesendet hat.

11. Klicken Sie auf **Hinzufügen**.

    Eine Meldung bestätigt, dass Tenable Identity Exposure die E-Mail-Warnung erstellt hat.

So bearbeiten Sie eine E-Mail-Warnung:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration** > **E-Mail**.
2. Fahren Sie mit dem Mauszeiger in der Liste der E-Mail-Warnungen über die Warnung, die Sie ändern möchten, und klicken Sie auf das Symbol ✎ am Ende der Zeile.

   Daraufhin öffnet sich der Bereich **E-Mail-Warnung bearbeiten**.

3. Nehmen Sie die erforderlichen Änderungen wie in der Vorgehensweise So fügen Sie eine E-Mail-Warnung hinzu: beschrieben vor.
4. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Warnung aktualisiert hat.

So löschen Sie eine E-Mail-Warnung:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration** > **E-Mail**.
2. Fahren Sie mit dem Mauszeiger in der Liste der E-Mail-Warnungen über die Warnung, die Sie löschen möchten, und klicken Sie auf das Symbol 🗑 am Ende der Zeile.

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.
3. Klicken Sie auf **Löschen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Warnung gelöscht hat.

Siehe auch

- SMTP-Serverkonfiguration
- Details zu Syslog- und E-Mail-Warnungen

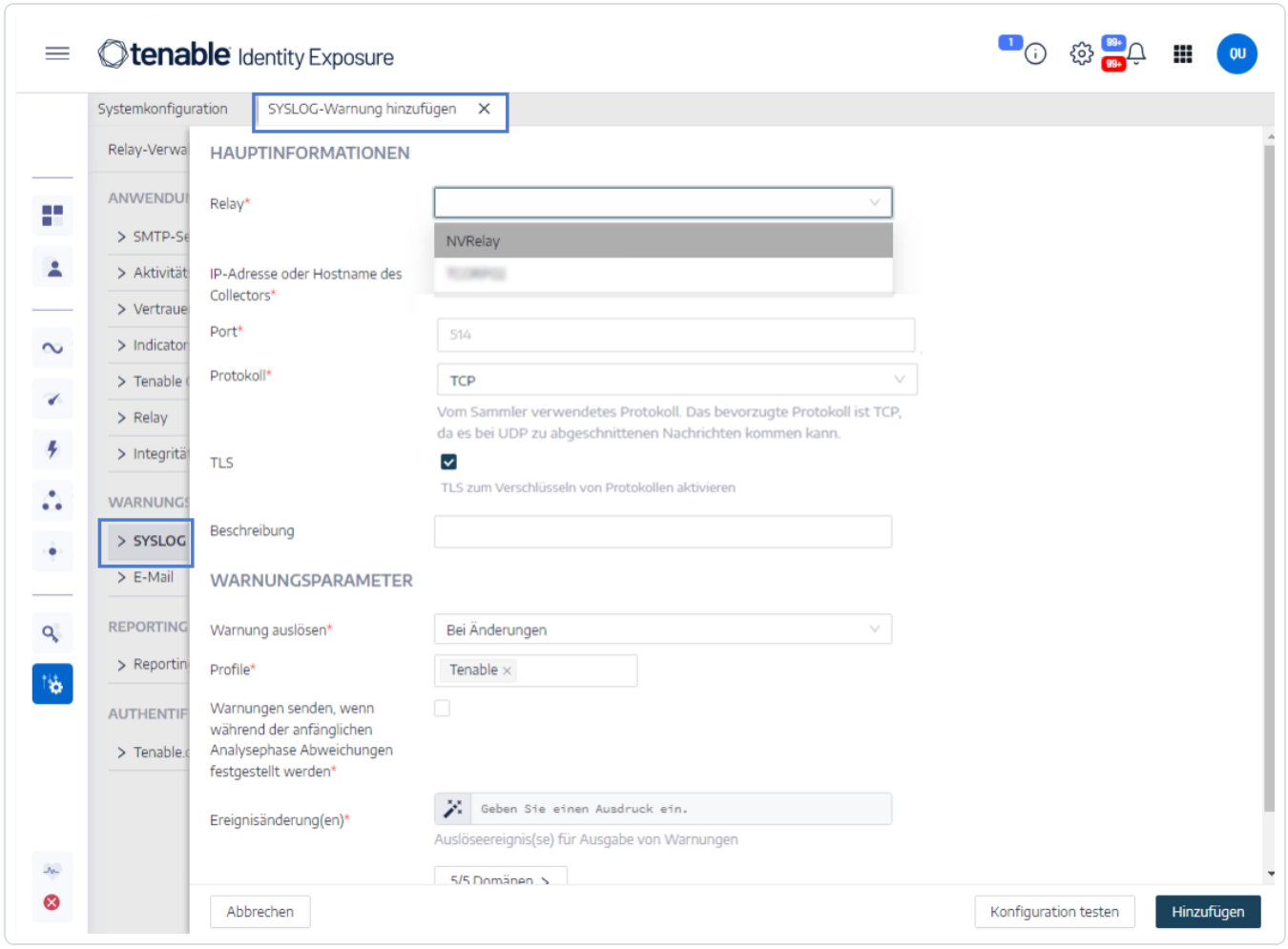
Syslog-Warnmeldungen

Einige Unternehmen verwenden SIEM (Security Information and Event Management), um Protokolle über potenzielle Bedrohungen und Sicherheitsvorfälle zu erfassen. Tenable Identity Exposure kann Sicherheitsinformationen, die sich auf Active Directory beziehen, an die SIEM-Syslog-Server weiterleiten, um deren Warnmechanismen zu verbessern.

So fügen Sie eine neue Syslog-Warnung hinzu:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration** > **Syslog**.
2. Klicken Sie auf der rechten Seite auf die Schaltfläche **SYSLOG-Warnung hinzufügen**.

   Daraufhin öffnet sich der Bereich **SYSLOG-Warnung hinzufügen**.



3. Geben Sie unter dem Abschnitt **Hauptinformationen** Folgendes an:

- **Wenn Ihr Netzwerk Secure Relay verwendet:** Klicken Sie im Feld **Relay** auf den Pfeil, um aus der Dropdown-Liste ein Relay auszuwählen, das mit Ihrem SIEM kommunizieren soll.
- Geben Sie im Feld **IP-Adresse oder Hostname des Collectors** die IP-Adresse oder den Hostnamen des Servers ein, der die Benachrichtigungen empfängt.
- Geben Sie in das Feld **Port** die Portnummer für den Collector ein.
- Klicken Sie im Feld **Protokoll** auf den Pfeil, um entweder UDP oder TCP auszuwählen.
  - Wenn Sie „TCP" wählen, aktivieren Sie das Kontrollkästchen der Option **TLS**, wenn Sie das TLS-Sicherheitsprotokoll zur Verschlüsselung der Protokolle aktivieren möchten.
- Geben Sie in das Feld **Beschreibung** eine kurze Beschreibung für den Collector ein.

4. Wählen Sie in der Dropdown-Liste **Warnung auslösen** eine der folgenden Optionen:
   - **Bei Änderungen**: Tenable Identity Exposure sendet eine Benachrichtigung, wenn ein von Ihnen angegebenes Ereignis eintritt.
   - **Bei jeder Abweichung**: Tenable Identity Exposure sendet eine Benachrichtigung bei jeder abweichenden IoA-Erkennung.
   - **Bei jedem Angriff**: Tenable Identity Exposure sendet eine Benachrichtigung bei jeder abweichenden IoA-Erkennung.
   - **Bei Integritätsprüfung-Statusänderung**: Tenable Identity Exposure sendet eine Benachrichtigung, wenn sich der Status für eine Integrationsprüfung ändert.
5. Klicken Sie in das Feld **Profile**, um das Profil auszuwählen, das für diese Syslog-Warnung verwendet werden soll (falls zutreffend).
6. **Warnungen senden, wenn während der anfänglichen Analysephase Abweichungen festgestellt werden**: Führen Sie eine der folgenden Aktionen aus (falls zutreffend):
   - Aktivieren Sie das Kontrollkästchen: Tenable Identity Exposure verschickt eine große Anzahl von E-Mail-Benachrichtigungen, wenn ein Systemneustart Warnungen auslöst.
   - Deaktivieren Sie das Kontrollkästchen: Tenable Identity Exposure verschickt keine E-Mail-Benachrichtigungen, wenn ein Systemneustart Warnungen auslöst.

7. **Schweregrad-Schwellenwert**: Klicken Sie auf den Pfeil des Dropdown-Feldes, um den Schwellenwert auszuwählen, bei dem Tenable Identity Exposure Warnungen sendet (falls zutreffend).
8. Abhängig von dem zuvor ausgewählten Warnungsauslöser:
    - **Ereignisänderungen**: Wenn Sie festlegen, dass Warnungen **bei Änderungen** ausgelöst werden, geben Sie einen Ausdruck ein, um die Ereignisbenachrichtigung auszulösen.

      Sie können entweder auf das Symbol klicken, um den Suchassistenten zu verwenden, oder eine Abfrage in das Suchfeld eingeben und auf **Validieren** klicken. Weitere Informationen finden Sie unter Trail Flow-Abfragen anpassen.
    - **Indicators of Exposure**: Wenn Sie festgelegt haben, dass Warnungen **bei jeder Abweichung** ausgelöst werden, klicken Sie auf den Pfeil neben den einzelnen Schweregradstufen, um die Liste der Indicators of Exposure zu erweitern und die Indikatoren auszuwählen, für die Warnungen gesendet werden sollen.
    - **Indicators of Attack**: Wenn Sie festgelegt haben, dass Warnungen **bei jedem Angriff** ausgelöst werden, klicken Sie auf den Pfeil neben jeder Schweregradstufe, um die Liste der Indicators of Attack zu erweitern und die Indikatoren auszuwählen, für die Warnungen gesendet werden sollen.
    - **Bei Integritätsprüfung-Statusänderung**: Klicken Sie auf **Integritätsprüfungen**, um den Typ der Integritätsprüfung auszuwählen, bei dem eine Warnung ausgelöst werden soll. Klicken Sie dann auf **Auswahlbasierter Filter**.
9. Klicken Sie auf das Feld **Domänen**, um die Domänen auszuwählen, für die Tenable Identity Exposure Warnungen versendet.

   Der Fensterbereich **Gesamtstrukturen und Domänen** wird angezeigt.

    a. Wählen Sie die Gesamtstruktur oder Domäne aus.

    b. Klicken Sie auf **Auswahlbasierter Filter**.
10. Klicken Sie auf **Konfiguration testen**.

    Eine Meldung bestätigt, dass Tenable Identity Exposure eine Syslog-Warnung an den Server gesendet hat.

11. Klicken Sie auf **Hinzufügen**.

    Eine Meldung bestätigt, dass Tenable Identity Exposure die Syslog-Warnung erstellt hat.

So bearbeiten Sie eine Syslog-Warnung:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration** > **Syslog**.
2. Fahren Sie mit dem Mauszeiger in der Liste der Syslog-Warnungen über die Warnung, die Sie ändern möchten, und klicken Sie auf das Symbol ✎ am Ende der Zeile.

   Daraufhin öffnet sich der Bereich **SYSLOG-Warnung bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen wie in der Vorgehensweise So fügen Sie eine neue Syslog-Warnung hinzu: beschrieben vor.
4. Klicken Sie auf **Bearbeiten**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Warnung aktualisiert hat.

So löschen Sie eine Syslog-Warnung:

1. Klicken Sie in Tenable Identity Exposure auf **System** > **Konfiguration** > **Syslog**.
2. Fahren Sie mit dem Mauszeiger in der Liste der Syslog-Warnungen über die Warnung, die Sie löschen möchten, und klicken Sie auf das Symbol 🗑 am Ende der Zeile.

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.
3. Klicken Sie auf **Löschen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Warnung gelöscht hat.

Siehe auch

- Details zu Syslog- und E-Mail-Warnungen

Details zu Syslog- und E-Mail-Warnungen

Wenn Sie Syslog- oder E-Mail-Warnungen aktivieren, sendet Tenable Identity Exposure Benachrichtigungen, wenn es eine Abweichung, einen Angriff oder eine Änderung erkennt.

Warnmeldungskopfzeile

Syslog-Warnmeldungskopfzeilen (RFC-3164) verwenden das Common Event Format (CEF), ein gängiges Format in Lösungen, die Security Information and Event Management (SIEM) integrieren.

Beispiel einer Warnmeldung für einen Indicator of Exposure (IoE)

IoE-Warnmeldungskopfzeile

```
<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"
```

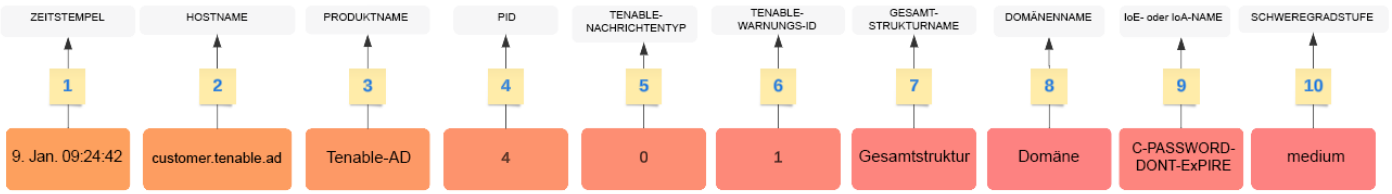
Beispiel einer Warnmeldung für einen Indicator of Attack (IoA)

IoA-Warnmeldungskopfzeile

```
<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"
```

Warnmeldungsinformationen

Generische Elemente

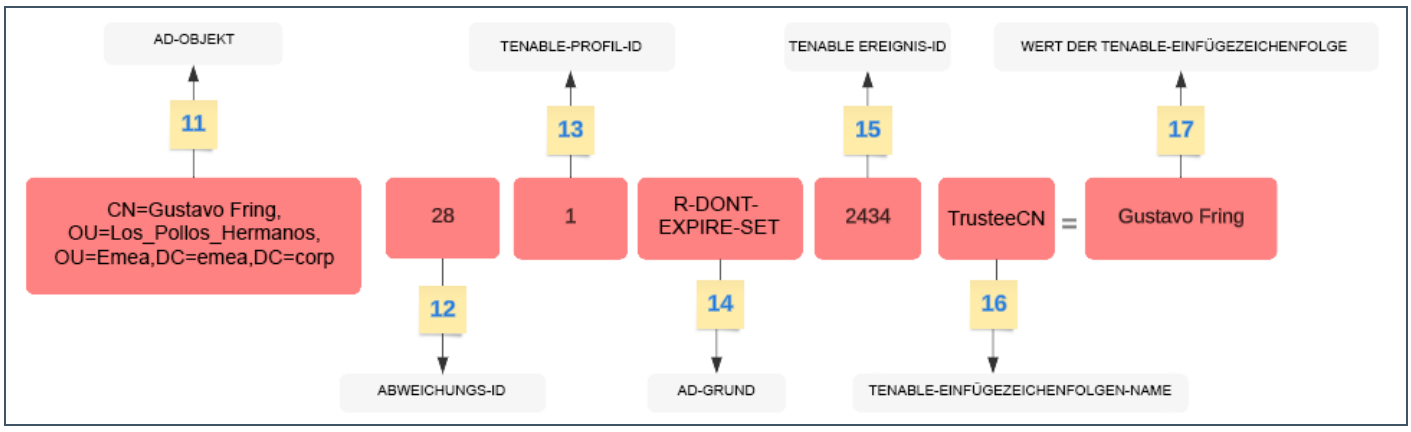


Die Kopfzeilenstruktur umfasst die folgenden Teile, wie in der Tabelle beschrieben.

Teil	Beschreibung
1	**Zeitstempel** – Das Datum der Erkennung. Beispiel: „7. Jun. 05:37:03“

2	**Hostname** – Der Hostname Ihrer Anwendung. Beispiel: „kunde.tenable.ad“
3	**Produktname** – Der Name des Produkts, das die Abweichung ausgelöst hat. Beispiel: „TenableAD“, „AnderesTenableADProdukt“
4	**PID** – Die Produkt(Tenable Identity Exposure)-ID. Beispiel: [4]
5	**Tenable-Nachrichtentyp** – Der Bezeichner von Ereignisquellen. Beispiel: „0“ (= bei jeder Abweichung), „1“ (= bei Änderungen), „2“ (= bei jedem Angriff)
6	**Tenable-Warnmeldungs-ID** – Die eindeutige ID der Warnung. Beispiel: „0“, „132“
7	**Name der Gesamtstruktur** – Der Name der Gesamtstruktur des betreffenden Ereignisses. Beispiel: „Unternehmensgesamtstruktur“
8	**Domänenname** – Der mit dem Ereignis verbundene Domänenname. Beispiel: „tenable.corp“, „zwx.com“
9	**Tenable-Codename** – Der Codename des Indicator of Exposure (IoE) oder Indicator of Attack (IoA). Beispiele: „C-PASSWORD-DONT-EXPIRE“, „DC Sync“.
10	**Tenable-Schweregradstufe** – Der Schweregrad der betreffenden Abweichung. Beispiel: „critical“, „high“, „medium“

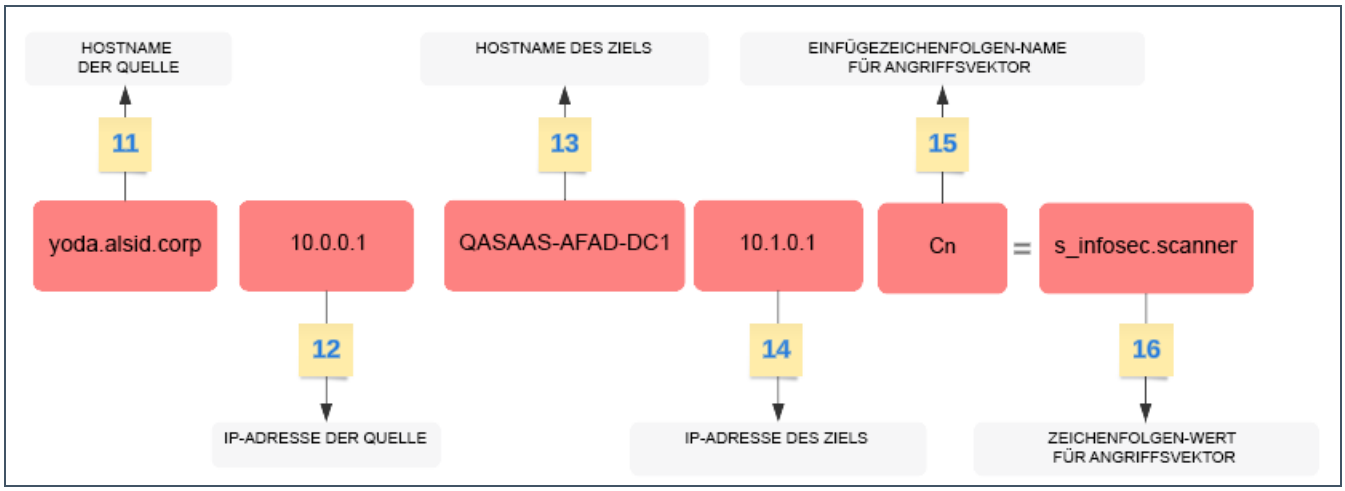
IoE-spezifische Elemente



Teil	Beschreibung
11	**AD-Objekt** – Der Distinguished Name des abweichenden Objekts. Beispiel: „CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local“

12	**Tenable-Abweichungs-ID** – Die ID der Abweichung. Beispiel: „24980“, „132“, „28“
13	**Tenable-Profil-ID** – Die ID des Profils, für das Tenable Identity Exposure die Abweichung ausgelöst hat. Beispiel: „1“ (Tenable), „2“ (sec_team)
14	**AD-Ursachen-Codename** – Der Codename des Abweichungsgrunds. Beispiel: „R-DONT-EXPIRE-SET“, „R-UNCONST-DELEG“
15	**Tenable-Ereignis-ID** – Die ID des Ereignisses, das durch die Abweichung ausgelöst wurde. Beispiel: „40667“, „28“
16	**Tenable-Einfügezeichenfolgen-Name** – Der Name des Attributs, das durch das abweichende Objekt ausgelöst wurde. Beispiel: „Cn“, „useraccountcontrol“, „member“, „pwdlastset“
17	**Tenable-Einfügezeichenfolgen-Wert** – Der Wert des Attributs, das durch das abweichende Objekt ausgelöst wurde. Beispiel: „s_infosec.scanner“, „CN=Backup Operators,CN=Builtin,DC=domain,DC=local“

IoA-spezifische Elemente



Teil	Beschreibung
11	**Hostname der Quelle** – Der Hostname des angreifenden Hosts. Der Wert kann auch „Unbekannt“ sein.
12	**IP-Adresse der Quelle** – Die IP-Adresse des angreifenden Hosts. Werte können IPv4 oder IPv6 sein.

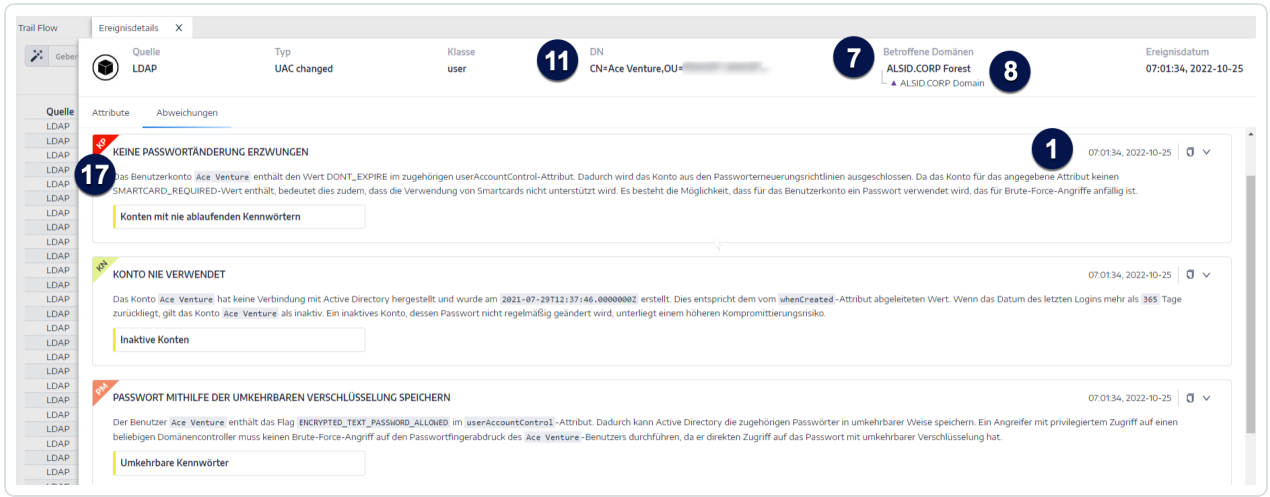
13	**Hostname des Ziels** – Der Hostname des angegriffenen Hosts.
14	**IP-Adresse des Ziels** – Die IP-Adresse des angegriffenen Hosts. Werte können IPv4 oder IPv6 sein.
15	**Angriffsvektor-Einfügezeichenfolgen-Name** – Der Name des Attributs, das durch das abweichende Objekt ausgelöst wurde.
16	**Angriffsvektor-Einfügezeichenfolgen-Wert** – Der Wert des Attributs, das durch das abweichende Objekt ausgelöst wurde.

Beispiele

Trail Flow-Ereignisdetails

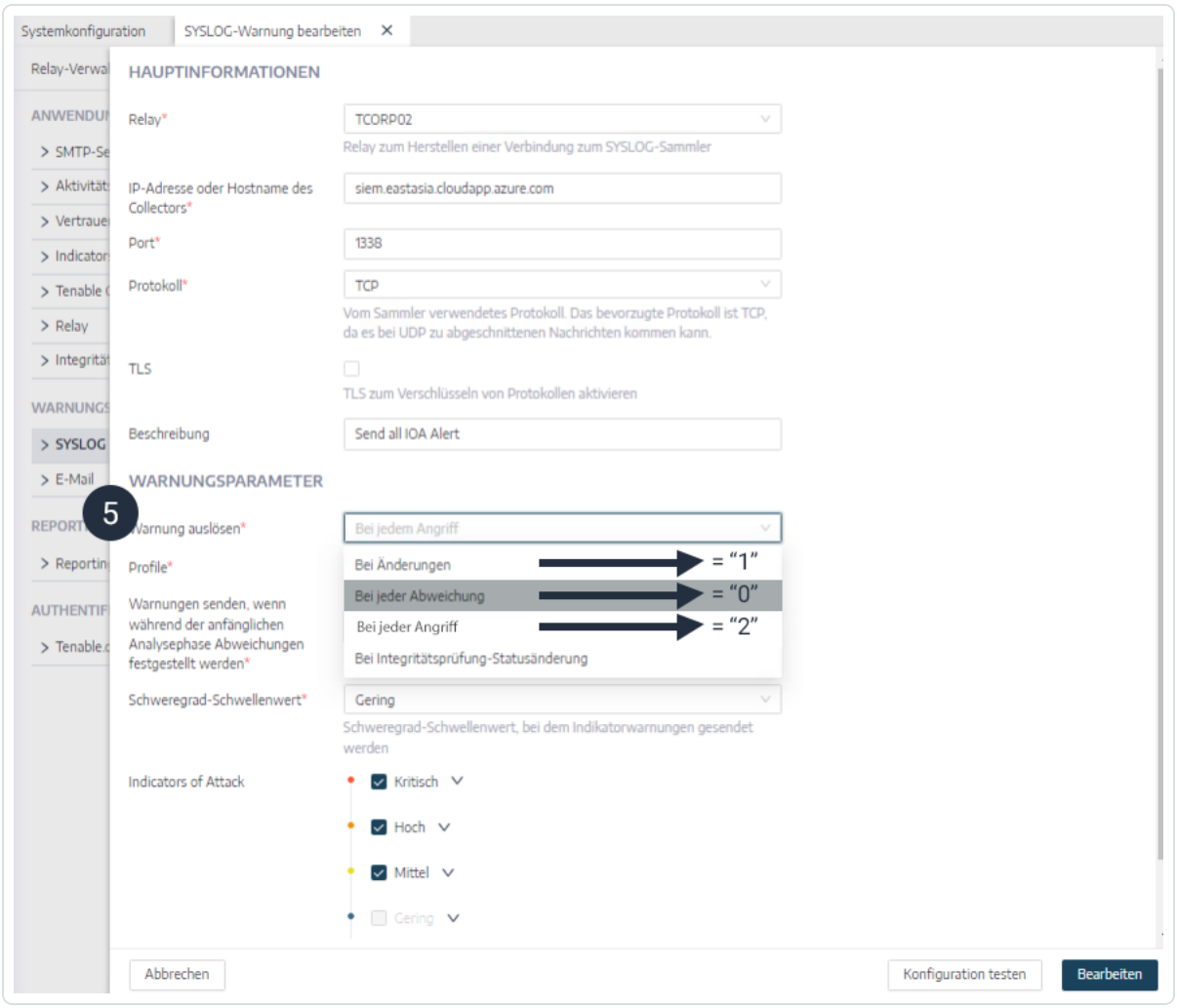
Das folgende Beispiel zeigt Details eines Ereignisses im Trail Flow, das Folgendes enthält:

- Den Zeitstempel (1)
- Den Namen des abweichenden Objekts (11)
- Den Namen der Gesamtstruktur (7) und den Domänennamen (8).
- Den Wert des Attributs, das durch das abweichende Objekt ausgelöst wurde (17).



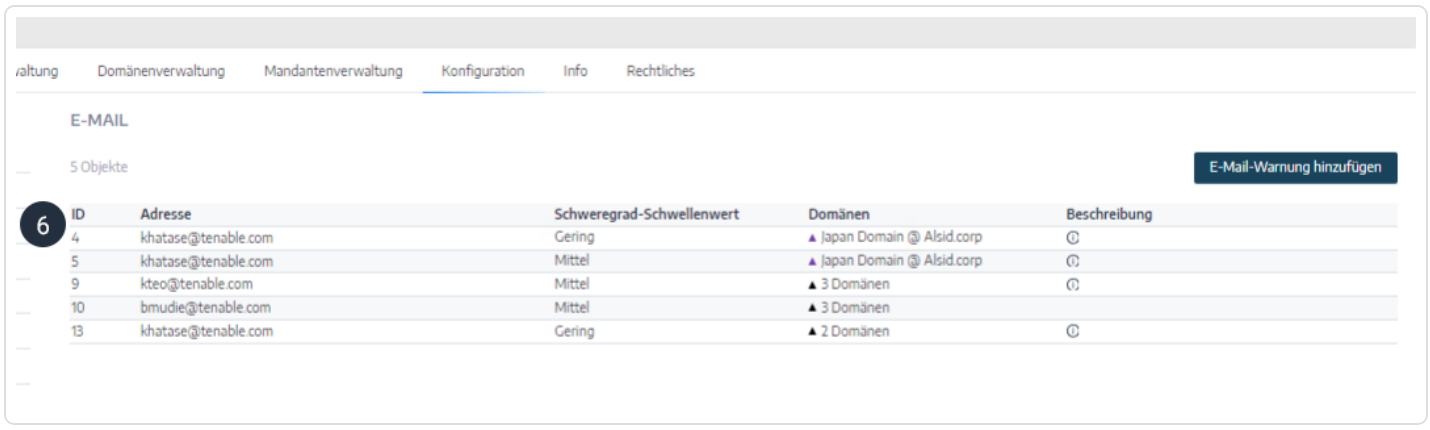
Ereignisquelle

Dieses Beispiel zeigt die Quelle für das Ereignis (5). Sie legen diesen Parameter auf der Syslog-Konfigurationsseite fest. Weitere Informationen finden Sie unter Syslog-Warnmeldungen.



Warnungs-ID

Dieses Beispiel zeigt die eindeutige ID der Warnung (6), die Sie in der Liste der konfigurierten E-Mail-Adressen in Tenable Identity Exposure unter **System** > **Konfiguration** > **E-Mail** finden.


altung
Domänenverwaltung
Mandantenverwaltung
Konfiguration
Info
Rechtliches
E-MAIL
5 Objekte
E-Mail-Warnung hinzufügen
6
ID
Adresse
Schweregrad-Schwellenwert
Domänen
Beschreibung
4
khatase@tenable.com
Gering
Japan Domain @ Alsid.corp
5
khatase@tenable.com
Mittel
Japan Domain @ Alsid.corp
9
kteo@tenable.com
Mittel
3 Domänen
10
bmudie@tenable.com
Mittel
3 Domänen
13
khatase@tenable.com
Gering
2 Domänen

Integritätsprüfungen

Die Funktion zur **Integritätsprüfung** in Tenable Identity Exposure bietet Ihnen Echtzeit-Einblick in die Konfiguration Ihrer Domänen und Dienstkonten in einer konsolidierten Ansicht. Von dieser aus können Sie einen Drilldown durchführen, um alle Konfigurationsanomalien zu untersuchen und zu beheben, die zu Problemen mit der Konnektivität oder anderen Problemen in Ihrer Infrastruktur führen. Es wird überprüft, ob alles ordnungsgemäß eingerichtet ist, um den reibungslosen Betrieb von Tenable Identity Exposure zu gewährleisten. Außerdem haben Sie die Möglichkeit, schnelle und präzise Maßnahmen zur Behebung von Problemen zu ergreifen. Sie können darauf vertrauen, dass Ihre Konfigurationseinstellungen optimal sind, um die effiziente Funktion von Tenable Identity Exposure zu ermöglichen.

Integritätsprüfungen sind standardmäßig für Administratorrollen und durch die Berechtigung für bestimmte Benutzerrollen sichtbar. Sie können außerdem Syslog- oder E-Mail-Warnungen für jede Änderung des Systemdiagnosestatus erstellen.

Integritätsprüfungen und DC Sync-Angriffserkennung

Integritätsprüfungen liefern wertvolle Informationen über den Status und die Benutzerfreundlichkeit von Tenable Identity Exposure-Diensten. Sie prüfen, ob das Dienstkonto in der Lage ist, sensible Informationen wie Passwort-Hashes und DPAPI-Sicherungsschlüssel zu erfassen, die für die privilegierte Analyse verwendet werden. Im Integritätsprüfungsbericht versucht Tenable, sensible Daten zu erfassen, um zu ermitteln, ob die Funktion „Privilegierte Analyse“ für das Dienstkonto ordnungsgemäß konfiguriert ist, ohne dabei tatsächlich Daten zu erfassen, wenn diese Funktion nicht verwendet wird. Um zu verhindern, dass während dieses Vorgangs ein DCSync-Angriff erkannt wird, setzt Tenable das bereitgestellte Dienstkonto automatisch für den DCSync-Indicator of Attack auf die Zulassungsliste.

Domänenstatus

Tenable Identity Exposure führt für jede Domäne die folgenden Prüfungen durch:

- Authentifizierung bei der AD-Domäne – LDAP-Einstellungen und -Status, Anmeldeinformationen und SMB-Zugriff
- Erreichbarkeit der Domäne – Funktionierende Verbindung zum dynamischen RPC-Port, ein erreichbarer SMB-Server, eine erreichbare IP-Adresse oder FQDN des Domänencontrollers,

eine funktionierende Verbindung zum RPC-Port, ein erreichbarer LDAP-Server und ein erreichbarer LDAP-Server des globalen Katalogs.

- Berechtigungen – Fähigkeit, auf AD-Domänendaten zuzugreifen und privilegierte Daten zu erfassen.
- Domäne mit Relay verknüpft – Die Domäne ist korrekt mit einem Relay-Dienst verknüpft.

Plattformstatus

Tenable Identity Exposure führt die folgenden Prüfungen Ihrer Plattformkonfiguration durch:

- Ausgeführter Relay-Dienst – Ermittelt, ob die Relay-Konfiguration korrekt ist und gibt Tipps zur Fehlerbehebung.
- Konsistenz der Relay-Version – Ermittelt, ob die Relay-Version mit der Tenable Identity Exposure-Version übereinstimmt.
- Ausführung von AD-Datensammlerdienst – Ermittelt, ob der Datensammlerdienst, der Broker und die Datensammler-Bridge in Betrieb sind und Daten an andere Dienste weiterleiten.

So greifen Sie auf Integritätsprüfungen zu:

1. Bewegen Sie mit den Mauszeiger auf der Seite Tenable Identity Exposure unten links über das Symbol  , um den globalen Status Ihrer Infrastruktur anzuzeigen.
2. Klicken Sie auf das Symbol, um die Seite **Integritätsprüfung** zu öffnen. Auf der Registerkarte **Domänenstatus** oder **Plattformstatus** wird eines der folgenden Elemente angezeigt:
    - Eine Meldung, dass alle Integritätsprüfungen bestanden wurden
    - Eine Liste mit Warnungen oder Problemen mit bestimmten Status:

	Die Prüfung war erfolgreich und zeigt ein normales Ergebnis.
	Die Prüfung ist fehlgeschlagen und hat ein Problem identifiziert.
	Die Prüfung ist fehlgeschlagen, aber das Problem verhindert nicht, dass Tenable Identity Exposure ordnungsgemäß funktioniert.

	Beispielsweise führt die Prüfung der Datensammlung zu einem Fehler, wenn Active Directory auf der Clientseite nicht ordnungsgemäß konfiguriert ist und das Dienstkonto keine privilegierten Daten erfassen kann. Dies ist jedoch kein schwerwiegendes Problem, da Sie die Funktion „Privilegierte Analyse“ für diese Domäne nicht in Tenable Identity Exposureaktiviert haben. Daher tritt diese Warnung auf. Wenn Sie die Funktion „Privilegierte Analyse“ jedoch aktivieren, schlägt die Prüfung sofort fehl.
	Die Prüfung zeigt ein unbekanntes Ergebnis, da eine abhängige Prüfung fehlgeschlagen ist. Beispielsweise kann die Prüfung auf Erreichbarkeit des Netzwerks nicht fortgesetzt werden, wenn die Prüfung auf Authentifizierung fehlgeschlagen ist.

So zeigen Sie alle Integritätsprüfungen an:

- Klicken Sie rechts über der Liste mit den Integritätsprüfungen auf den Umschalter **Erfolgreiche Prüfungen anzeigen**, um alle Prüfungen, die Tenable Identity Exposure durchgeführt hat, mit den folgenden Informationen aufzulisten:
  - Name der Integritätsprüfung
  - Status (Bestanden, Nicht bestanden, Nicht blockierender Fehler und Unbekannt)
  - Betroffene Domäne und die zugehörige Gesamtstruktur (nur bei Integritätsprüfungen für Domänen)
  - Zeitpunkt der zuletzt durchgeführten Prüfung
  - Dauer, wie lange sich die Prüfung in diesem Status befindet

So aktualisieren Sie die Seite für die Integritätsprüfung:

- Obwohl Tenable Identity Exposure regelmäßig Integritätsprüfungen durchführt, wird die Seite nicht in Echtzeit mit den Ergebnissen aktualisiert. Klicken Sie auf , um die Liste mit den Ergebnissen zu aktualisieren.

So filtern Sie Ergebnisse nach dem Typ der Integritätsprüfung oder nach Domäne:

1. Klicken Sie rechts über der Liste mit den Integritätsprüfungen auf **n/n Integritätsprüfungen** oder **n/n Domänen** (nur für Domänenstatus).

   Der Fensterbereich **Integritätsprüfungen** oder **Gesamtstrukturen und Domänen** wird geöffnet.

2. Wählen Sie die Typen von Integritätsprüfungen oder Gesamtstrukturen/Domänen (falls zutreffend) aus und klicken Sie auf **Auswahlbasierter Filter**.

So schlüsseln Sie die Informationen zu den einzelnen Integritätsprüfungen weiter auf:

1. Klicken Sie in der Liste mit den Integritätsprüfungen auf den Namen einer Integritätsprüfung oder auf den blauen Pfeil (→) am Ende der Zeile.

   Der Fensterbereich Details wird geöffnet und zeigt eine Beschreibung der Prüfung sowie eine Liste der relevanten Details an.

Name der Integritätsprüfung	Typ	Beschreibung der Prüfung	Ursachen
Erreichbarkeit der Domäne	Domäne	Fähigkeit, eine Verbindung zur AD-Domäne herzustellen	• `IP-UNREACHABLER-LDAP-GLOBAL-CATALOG-UNREACHABLE` • `LDAP-SERVER-UNREACHABLE` • `SMB-SERVER-UNREACHABLE` • `DYNAMIC-RPC-CONNECTION-NOT-WORKING` • `RPC-CONNECTION-NOT-WORKING`

Authentifizierung bei der AD-Domäne	Domäne	Fähigkeit, sich bei der AD-Domäne zu authentifizieren	• `INCORRECT-CREDENTIALS` • `LDAP-SERVER-BUSY` • `LDAP-SERVER-UNAVAILABLE` • `LDAP-SERVER-ACCESS-DENIED` • `SMB-SERVER-ACCESS-DENIED`
Berechtigungen zum Erfassen der AD-Domänendaten	Domäne	Fähigkeit, die AD-Domänendaten zu erfassen	• `MISSING-PERMISSIONS-PRIVILEGED-DATA`
Berechtigungen zum Zugriff auf die AD-Container	Domäne	Fähigkeit, auf die AD-Container zuzugreifen	• `MISSING-PERMISSIONS-DELETED-OBJECTS-ACCESS` • `MISSING-PERMISSIONS-PASSWORD-SETTINGS-ACCESS`
Domäne mit Relay verknüpft	Domäne	Die Domäne ist mit einem Relay verknüpft.	• `LINKED-TO-RELAY-DOWN`
Relay-Dienst aktiv	Plattform	Das Relay funktioniert wie	• `RELAY-DOWN`

		erwartet.	
Version des Relay-Diensts	Plattform	Die Relay-Version ist auf das Produkt abgestimmt.	• `VERSION-MISMATCH`
AD-Datensammler aktiv	Plattform	Der AD-Datensammler funktioniert wie erwartet.	• `DATA-COLLECTOR-SERVICE-DOWN` • `DATA-COLLECTOR-BRIDGE-DOWN` • `BROKER-DOWN`

2. Klicken Sie auf den Pfeil am Ende der Detailzeile, um sie zu erweitern und weitere Informationen über das Ergebnis anzuzeigen.

So blenden Sie das Symbol für den Status der Integritätsprüfung aus:

Standardmäßig zeigt Tenable Identity Exposure das Symbol für den Status der Integritätsprüfung unten links auf dem Bildschirm an.

1. Wechseln Sie in Tenable Identity Exposure in der linken Navigationsleiste zu **System** und wählen Sie die Registerkarte **Konfiguration** aus.

   Alternativ können Sie auch auf der Seite „Integritätsprüfung“ oben rechts auf ··· klicken und **Konfiguration** auswählen.

2. Wählen Sie unter **Anwendungsdienste** die Option **Integritätsprüfung**.

3. Klicken Sie auf den Umschalter **Globalen Status der Integritätsprüfung zeigen**, um die Option zu deaktivieren.

   Tenable Identity Exposure blendet das Symbol für den Status der Integritätsprüfung unten links auf dem Bildschirm aus.

So weisen Sie Benutzerrollen Berechtigungen für die Integritätsprüfung zu:

1. Wechseln Sie in Tenable Identity Exposure in der linken Navigationsleiste zu **Konten** und wählen Sie die Registerkarte **Rollenverwaltung** aus.
2. Wählen Sie in der Liste der Rollen eine Benutzerrolle aus und klicken Sie am Ende der Zeile auf ✎.

   Der Fensterbereich **Rolle bearbeiten** wird geöffnet.
3. Wählen Sie die Registerkarte **Systemkonfigurationsentitäten** aus.
4. Wählen Sie die Entität **Integrationsprüfung** aus und klicken Sie auf den Umschalter für die Berechtigung, um ihn von **Nicht autorisiert** auf **Erteilt** umzustellen.
5. Klicken Sie auf **Anwenden und schließen**.

Weitere Informationen zu Berechtigungen finden Sie unter Berechtigungen für eine Rolle festlegen.

So richten Sie Warnungen bei Änderung des Status für Integrationsprüfungen ein:

1. Wechseln Sie in Tenable Identity Exposure in der linken Navigationsleiste zu **System** und wählen Sie die Registerkarte **Konfiguration** aus.

   Alternativ können Sie auch auf der Seite „Integritätsprüfung“ oben rechts auf ⋯ klicken und **Warnungen** auswählen.
2. Wählen Sie unter **Warnungsmodul** die Option **Syslog** oder **E-Mail** aus.
3. Klicken Sie auf **SYSLOG-Warnung hinzufügen** oder **E-Mail-Warnung hinzufügen**.

   Ein neuer Fensterbereich wird geöffnet. Das vollständige Verfahren finden Sie unter Warnmeldungen.
4. Wählen Sie unter **Warnungsparameter** im Feld **Warnung auslösen** im Dropdown-Menü die Option **Bei Integritätsprüfung-Statusänderung** aus.
5. Klicken Sie auf den Pfeil im Feld **Integritätsprüfungen**, um den Typ der Integritätsprüfung auszuwählen, bei dem eine Warnung ausgelöst werden soll. Klicken Sie dann auf **Auswahlbasierter Filter**.
6. Klicken Sie auf **Hinzufügen**.

Reporting Center

Das **Reporting Center** in Tenable Identity Exposure bietet eine sehr nützliche Funktion, mit der Sie wichtige Daten als Berichte exportieren und an wichtige Interessengruppen innerhalb einer Organisation weitergeben können. Das Reporting Center bietet die Möglichkeit, Berichte aus einer vordefinierten Liste zu erstellen und so einen effizienten und optimierten Prozess zu gewährleisten.

Administratoren können verschiedene Arten von Berichten für verschiedene Benutzer mit einem flexiblen Berichtszeitraum von bis zu einem Quartal erstellen. Die Möglichkeit, kritische Identitätsdaten aus Tenable Identity Exposure gemeinsam zu nutzen, ermöglicht es dem Unternehmen, Risiken proaktiv zu mindern und potenzielle identitätsbasierte Angriffe zu identifizieren.

Um einen Bericht herunterzuladen, erhalten Benutzer eine E-Mail mit einer URL zu einer Seite, auf der sie einen Berichtszugriffsschlüssel eingeben, den sie von ihrem Administrator erhalten haben. Berichte stehen 30 Tage lang zum Herunterladen zur Verfügung. Danach sind sie veraltet und werden von Tenable Identity Exposure gelöscht. Benutzer müssen die Berichte herunterladen, bevor Tenable Identity Exposure einen neuen Bericht für den angegebenen Zeitrahmen generiert und den vorherigen überschreibt.

So greifen Sie auf das Reporting Center zu:

1. Wählen Sie in Tenable Identity Exposure **Systeme** > **Konfiguration**.
2. Klicken Sie unter **Berichterstellung** auf **Reporting Center**.

   Es wird ein Fensterbereich mit einer Liste der konfigurierten Berichte und der zugehörigen Informationen geöffnet, wie z. B. Berichtsname, Berichtstyp, Domäne, Profil, Zeitraum, Wiederholung und E-Mail-Adressen der Empfänger.

So erstellen Sie einen Bericht:

1. Klicken Sie im Fensterbereich **Reporting Center** auf **Bericht erstellen**.

   Der Fensterbereich **Berichtskonfiguration** wird geöffnet.
2. Geben Sie unter **Berichtstyp** die folgenden Informationen ein:

a. Wählen Sie als **Berichtstyp** entweder **Abweichungen** oder **Angriffe** aus.

b. Klicken Sie unter **Indikatoren** auf **n/n Indikatoren**, um entweder **Indicators of Exposure** (für Abweichungen) oder **Indicators of Attack** (für Angriffe) auszuwählen. Klicken Sie dann auf **Auswahlbasierter Filter**.

c. Klicken Sie unter **Domänen** auf **n/n Domänen**, um die Gesamtstrukturen oder Domänen für den Bericht auszuwählen. Klicken Sie dann auf **Auswahlbasierter Filter**.

d. Klicken Sie unter **Profile** auf den Pfeil, um ein Profil aus dem Dropdown-Menü auszuwählen.

3. Geben Sie unter **Berichtsname** einen Namen für den Bericht ein.
4. Wählen Sie unter **Generierungsparameter** die folgenden Einstellungen aus:

   a. **Datenzeitrahmen** – Der Bericht umfasst den Zeitrahmen, der dem aktuellen vorausgeht, z. B. den vorhergehenden Tag, Woche, Monat oder Quartal.

   b. **Wiederholung** – Tenable Identity Exposure generiert einen neuen Bericht für jeden von Ihnen definierten Zeitrahmen: Klicken Sie auf den Pfeil, um die entsprechenden Werte im Dropdown-Menü auszuwählen.

   c. **Zeitzone** – Die mit dem Bericht verknüpfte Zeitzone.

5. Klicken Sie unter **Empfänger** auf **E-Mail-Adressen hinzufügen** und geben Sie die E-Mail-Adresse des Empfängers ein. Sie können so viele Empfänger wie benötigt hinzufügen.

   Informationen zum Einrichten von E-Mails für Berichtsempfänger finden Sie unter SMTP-Serverkonfiguration.

6. Klicken Sie auf **Bericht erstellen**.

So gestatten Sie Benutzern das Herunterladen eines Berichts:

- Klicken Sie oben im Fensterbereich **Reporting Center** unter **Zugriffsschlüssel für Berichte** auf , um ihn zu kopieren. Dieser Zugriffsschlüssel ist erforderlich, um den Bericht über den Link herunterzuladen, der dem Empfänger per E-Mail gesendet wurde. Er ist für alle Benutzer und Berichte eindeutig.
- Klicken Sie gegebenenfalls auf , um einen neuen Zugriffsschlüssel zu generieren.

Vorsicht: Wenn Sie einen neuen Zugriffsschlüssel generieren, wird der vorherige Schlüssel unbrauchbar. Nur der neue Zugriffsschlüssel kann Zugriff auf die vorhandenen Berichte gewähren.

So bearbeiten Sie die Berichtskonfiguration:

1. Wählen Sie in der Liste der Berichte einen Bericht aus und klicken Sie am Ende der Zeile auf ✎, um den Fensterbereich **Berichtskonfiguration** zu öffnen.
2. Ändern Sie diese nach Bedarf.
3. Klicken Sie auf **Speichern**.

So löschen Sie einen Bericht:

1. Wählen Sie in der Liste der Berichte einen Bericht aus und klicken Sie am Ende der Zeile auf 🗑, um den Bericht zu löschen.

   In einer Meldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.
2. Klicken Sie auf **Löschen**.

   Der zuletzt generierte Bericht, der dieser Berichtskonfiguration zugeordnet ist, steht nicht mehr zum Herunterladen zur Verfügung.

So erteilen Sie Rollen Berechtigungen:

- Administratoren können in der **Berechtigungsverwaltung** unter **Datenentitäten** > **Berichte** Benutzerrollen Berechtigungen zum Erstellen, Lesen oder Bearbeiten aller oder bestimmter Berichtskonfigurationen erteilen.

  Weitere Informationen finden Sie unter Berechtigungen für eine Rolle festlegen.

Siehe auch

- Widgets

Microsoft Entra ID-Unterstützung

Zusätzlich zu Active Directory unterstützt Tenable Identity Exposure auch Microsoft Entra ID (früher Azure AD oder AAD), um den Geltungsbereich von Identitäten in einer Organisation zu erweitern. Diese Funktion nutzt neue Indicators of Exposure, die sich auf Microsoft Entra ID-spezifische Risiken konzentrieren.

Um Microsoft Entra ID in Tenable Identity Exposure zu integrieren, befolgen Sie diesen Onboarding-Prozess:

1. Voraussetzungen erfüllen
2. Berechtigungen prüfen
3. Microsoft Entra ID-Einstellungen konfigurieren
4. Microsoft Entra ID-Unterstützung aktivieren
5. Mandantenscans aktivieren

Voraussetzungen

Sie müssen über ein **Tenable Vulnerability Management-Konto** verfügen, um die Funktion für Microsoft Entra ID-Unterstützung nutzen zu können. Mit dem Konto können Sie Tenable-Scans für Microsoft Entra ID konfigurieren und die Ergebnisse dieser Scans erfassen.

Berechtigungen

Die Unterstützung von Microsoft Entra ID erfordert die Erfassung von Daten von Microsoft Entra ID, wie beispielsweise Benutzern, Gruppen, Anwendungen, Dienstprinzipalen, Rollen, Berechtigungen, Richtlinien, Protokollen usw. Diese Daten werden mithilfe der Microsoft Graph-API und Dienstprinzipal-Anmeldeinformationen gemäß den Empfehlungen von Microsoft erfasst.

- Sie müssen sich bei Microsoft Entra ID **als Benutzer mit der Berechtigung zum Erteilen einer mandantenweiten Administratoreinwilligung** für Microsoft Graph einloggen, das laut Microsoft über die Rolle „Globaler Administrator“ oder „Privilegierter Rollenadministrator“ (oder eine beliebige benutzerdefinierte Rolle mit entsprechenden Berechtigungen) verfügen muss.
- Um auf die Konfiguration und Datenvisualisierung für Microsoft Entra ID zuzugreifen, muss

Ihre **Tenable Identity Exposure-Benutzerrolle** über die entsprechenden Berechtigungen verfügen. Weitere Informationen finden Sie unter Berechtigungen für eine Rolle festlegen.

Microsoft Entra ID-Einstellungen konfigurieren

Verwenden Sie die folgenden Verfahren (übernommen aus dem Artikel Schnellstart: Registrieren einer Anwendung bei Microsoft Identity Platform der Microsoft-Dokumentation), um alle erforderlichen Einstellungen in Microsoft Entra ID zu konfigurieren.

1. **Erstellen Sie eine Anwendung:**

   a. Öffnen Sie im Azure-Administratorportal die Seite **App-Registrierungen**.

   b. Klicken Sie auf **+ Neue Registrierung**.

   c. Geben Sie der Anwendung einen Namen (Beispiel: „Tenable Identity Collector“). Für die anderen Optionen können Sie die Standardwerte unverändert lassen.

   d. Klicken Sie auf **Registrieren**.

   e. Notieren Sie sich auf der Übersichtsseite dieser neu erstellten App die „Anwendungs-ID (Client)“ und die „Verzeichnis-ID (Mandant)“.

2. **Fügen Sie Anmeldeinformationen zur Anwendung hinzu:**

   a. Öffnen Sie im Azure-Administratorportal die Seite **App-Registrierungen**.

   b. Klicken Sie auf die von Ihnen erstellte Anwendung.

   c. Klicken Sie im linken Menü auf **Zertifikate und Geheimnisse**.

   d. Klicken Sie auf **+ Neuer geheimer Clientschlüssel**.

   e. Geben Sie im Feld **Beschreibung** einen praktischen Namen für dieses Geheimnis und einen **Ablaufwert** ein, der Ihren Richtlinien entspricht. Denken Sie daran, dieses Geheimnis kurz vor Ablauf seines Ablaufdatums zu erneuern.

   f. Speichern Sie den Wert des geheimen Schlüssels an einem sicheren Ort, da Azure ihn nur einmal anzeigt und Sie ihn neu erstellen müssen, wenn Sie ihn verlieren.

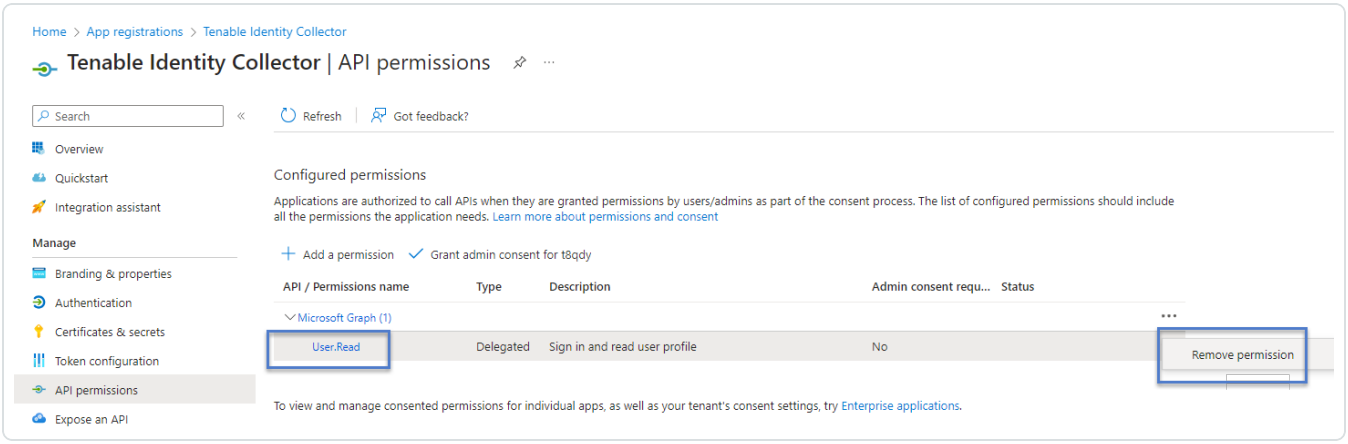
3. **Weisen Sie der Anwendung Berechtigungen zu:**

a. Öffnen Sie im Azure-Administratorportal die Seite **App-Registrierungen**.

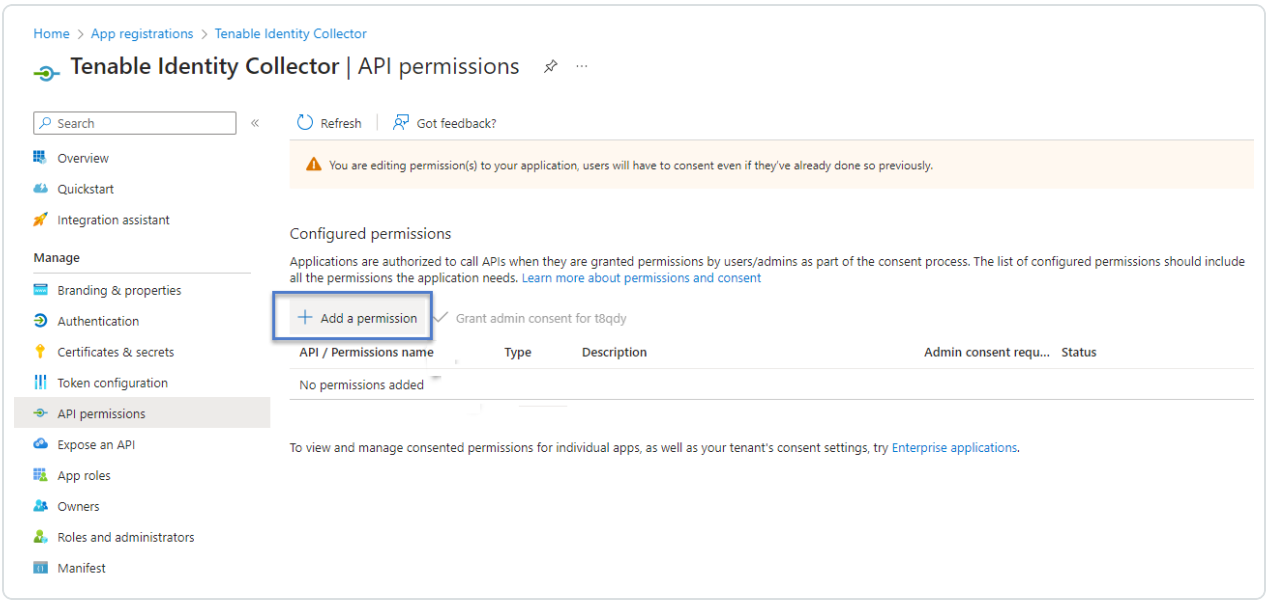
b. Klicken Sie auf die von Ihnen erstellte Anwendung.

c. Klicken Sie im linken Menü auf **API-Berechtigungen**.

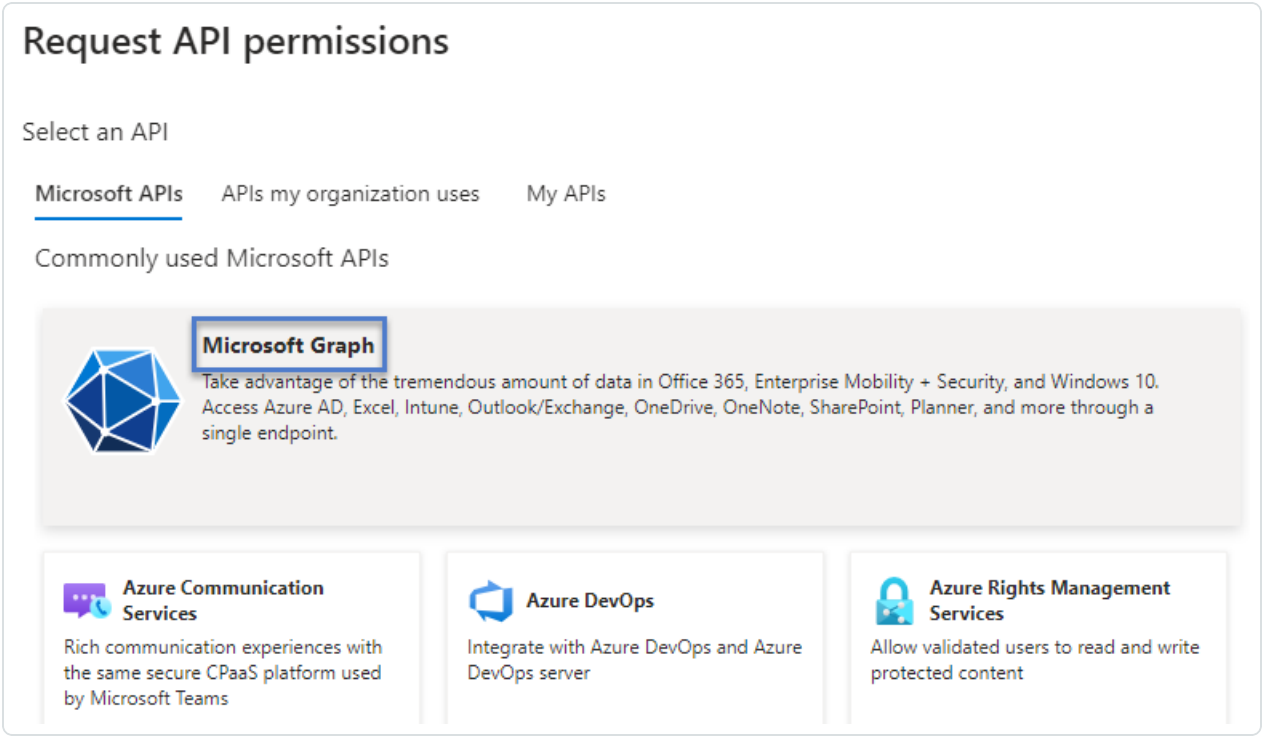
d. Entfernen Sie die vorhandene Berechtigung `User.Read`:



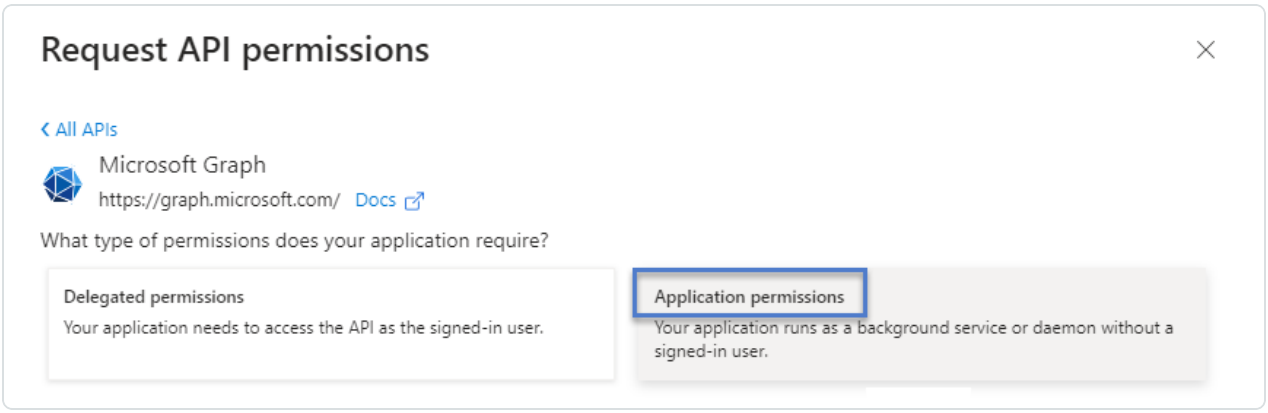
e. Klicken Sie auf **+ Berechtigung hinzufügen**:



f. Wählen Sie **Microsoft Graph** aus:



g. Wählen Sie **Anwendungsberechtigungen** aus (nicht „Delegierte Berechtigungen“).



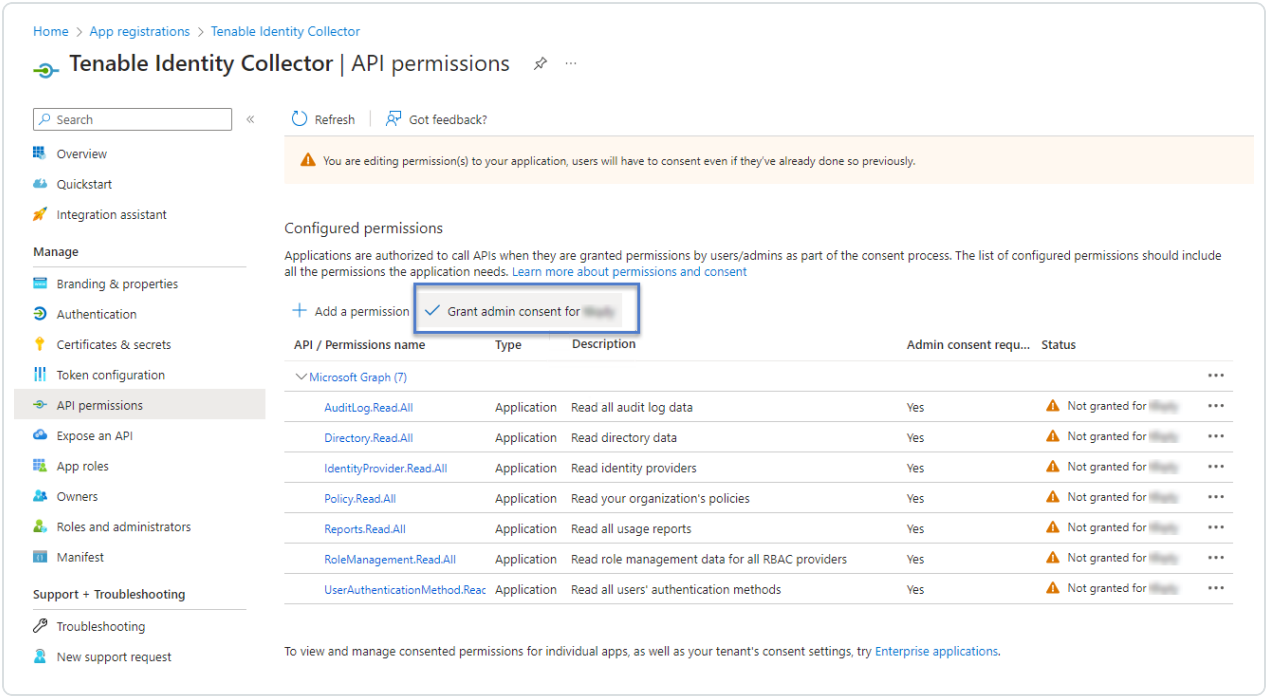
h. Verwenden Sie die Liste oder die Suchleiste, um alle folgenden Berechtigungen zu suchen und auszuwählen:

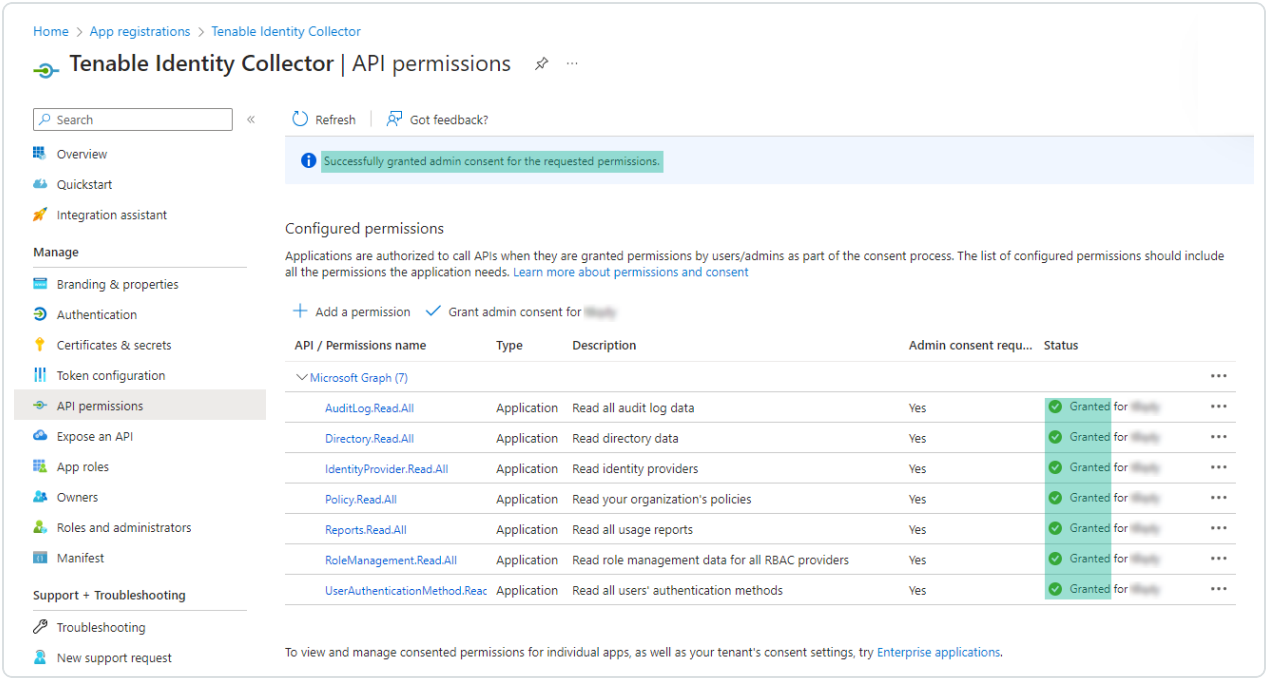
   - `AuditLog.Read.All`
   - `Directory.Read.All`
   - `IdentityProvider.Read.All`
   - `Policy.Read.All`

- `Reports.Read.All`
- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. Klicken Sie auf **Berechtigungen hinzufügen**.

j. Klicken Sie auf **Administratoreinwilligung erteilen für <Mandantenname>** und klicken Sie zur Bestätigung auf **Ja**:





4. Nachdem Sie alle erforderlichen Einstellungen in Microsoft Entra ID konfiguriert haben, führen Sie die folgenden Schritte aus:

    a. Erstellen Sie in Tenable Vulnerability Management neue Anmeldeinformationen des Typs „Microsoft Azure“.

b. Wählen Sie die Authentifizierungsmethode „Schlüssel“ und geben Sie die Werte ein, die Sie im vorherigen Verfahren abgerufen haben: Mandanten-ID, Anwendungs-ID und Client-Geheimnis.

Microsoft Entra ID-Unterstützung aktivieren

So aktivieren Sie -Unterstützung:

Hinweis: Um diese Funktion erfolgreich zu aktivieren, muss der Tenable Cloud-Benutzer, der den Zugriffsschlüssel und die geheimen Schlüssel erstellt hat, Administratorrechte für den Tenable Cloud-Container haben, auf den von der Tenable Identity Exposure-Lizenz verwiesen wird. Weitere Informationen finden Sie unter Lizenzierung von Tenable Identity Exposure.

1. Klicken Sie in Tenable Identity Exposure auf das Systeme-Symbol  in der linken Navigationsleiste.
2. Klicken Sie auf die Registerkarte **Konfiguration**.

   Die Seite **Konfiguration** wird geöffnet.
3. Klicken Sie unter „Anwendungsdienste“ auf **Tenable Cloud**.
4. Klicken Sie unter **Microsoft Entra ID-Unterstützung aktivieren** auf den Schalter, um ihn zu aktivieren.
5. Wenn Sie sich zuvor noch nicht bei Tenable Cloud eingeloggt haben, klicken Sie auf den Link, um zur Login-Seite zu gelangen:
   a. Klicken Sie auf **Passwort vergessen?** , um ein Passwort-Reset anzufordern.
   b. Geben Sie die mit Ihrer Tenable Identity Exposure-Lizenz verknüpfte E-Mail-Adresse ein und klicken Sie auf **Passwort-Reset anfordern**.

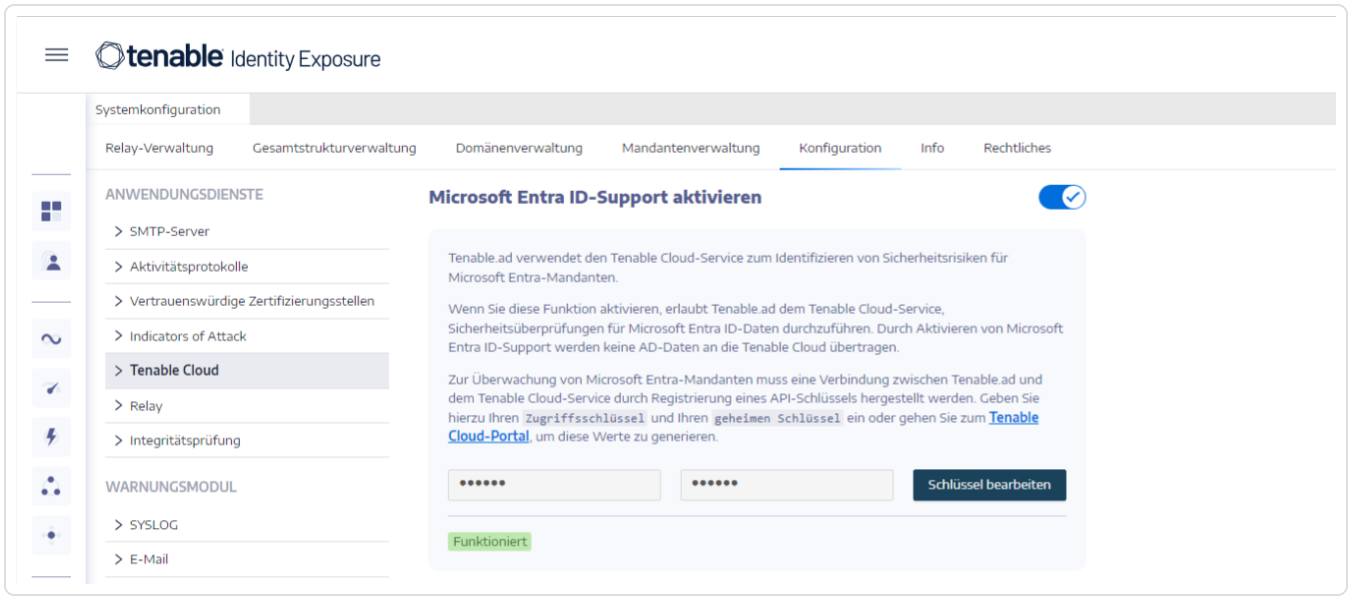
      Tenable sendet eine E-Mail mit einem Link zum Zurücksetzen Ihres Passworts an diese Adresse.

      Hinweis: Wenn Ihre E-Mail-Adresse nicht mit der mit der Tenable Identity Exposure-Lizenz verknüpften übereinstimmt, wenden Sie sich für Unterstützung an Ihren Kundensupport.
6. Loggen Sie sich bei Tenable Vulnerability Management ein.

7. Um API-Schlüssel in Tenable Vulnerability Managementzu generieren, gehen Sie zu Tenable Vulnerability Management > **Settings** (Einstellungen) > **My Account** (Mein Konto) > **API Keys** (API-Schlüssel).

8. Geben Sie Ihren Tenable Vulnerability Management-Admin-Benutzer `AccessKey` und `SecretKey` ein, um eine Verbindung zwischen Tenable Identity Exposure und dem Tenable-Cloud-Service einzurichten.

9. Klicken Sie auf **Schlüssel bearbeiten**, um die API-Schlüssel zu übermitteln.



Tenable Identity Exposure zeigt eine Meldung an, um zu bestätigen, dass die API-Schlüssel aktualisiert wurden.

Mandantenscans aktivieren

So fügen Sie einen neuen -Mandanten hinzu:

Durch das Hinzufügen eines Mandanten wird Tenable Identity Exposure mit dem Microsoft Entra ID-Mandanten verknüpft, um Scans für diesen Mandanten durchzuführen.

1. Klicken Sie auf der Seite „Konfiguration“ auf die Registerkarte **Mandantenverwaltung**.

   Die Seite **Mandantenverwaltung** wird geöffnet.

2. Klicken Sie auf **Mandanten hinzufügen**.

Die Seite **Mandanten hinzufügen** wird geöffnet.

3. Geben Sie im Feld **Name des Mandanten** einen Namen ein.
4. Klicken Sie im Feld **Anmeldeinformationen** auf die Dropdown-Liste, um Anmeldeinformationen auszuwählen.
5. Wenn Ihre Anmeldeinformationen nicht in der Liste angezeigt werden, haben Sie diese beiden Möglichkeiten:
    - Erstellen Sie Anmeldeinformationen in Tenable Vulnerability Management (Tenable Vulnerability Management > **Settings** (Einstellungen) > **Credentials** (Anmeldeinformationen)). Weitere Informationen finden Sie im Verfahren zum Erstellen von Azure-Anmeldeinformationen in Tenable Vulnerability Management.

- Überprüfen Sie, ob Sie über die Berechtigung „Can use“ (Verwendung erlaubt) oder „Can edit“ (Bearbeitung erlaubt) für die Anmeldeinformationen in Tenable Vulnerability Management verfügen. Sofern Sie nicht über diese Berechtigungen verfügen, zeigt Tenable Identity Exposure die Anmeldeinformationen nicht in der Dropdown-Liste an.

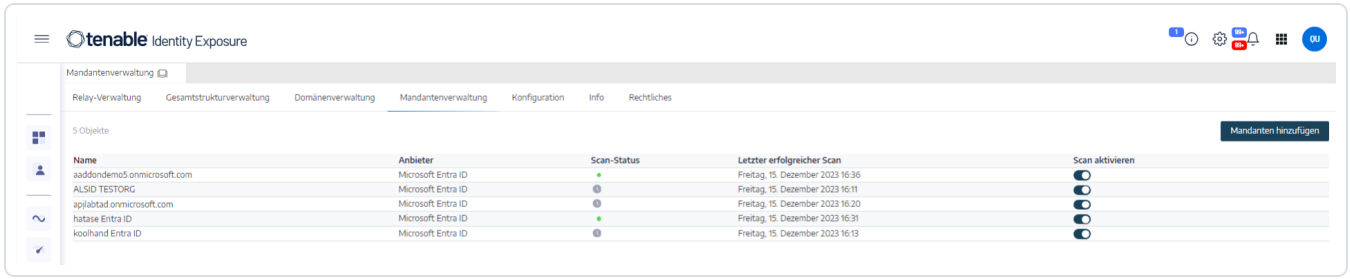
6. Klicken Sie auf **Aktualisieren**, um die Dropdown-Liste der Anmeldeinformationen zu aktualisieren.
7. Wählen Sie die von Ihnen erstellten Anmeldeinformationen aus.
8. Klicken Sie auf **Hinzufügen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure den Mandanten hinzugefügt hat, der nun in der Liste auf der Seite „Mandantenverwaltung“ angezeigt wird.

So aktivieren Sie Scans für den Mandanten:

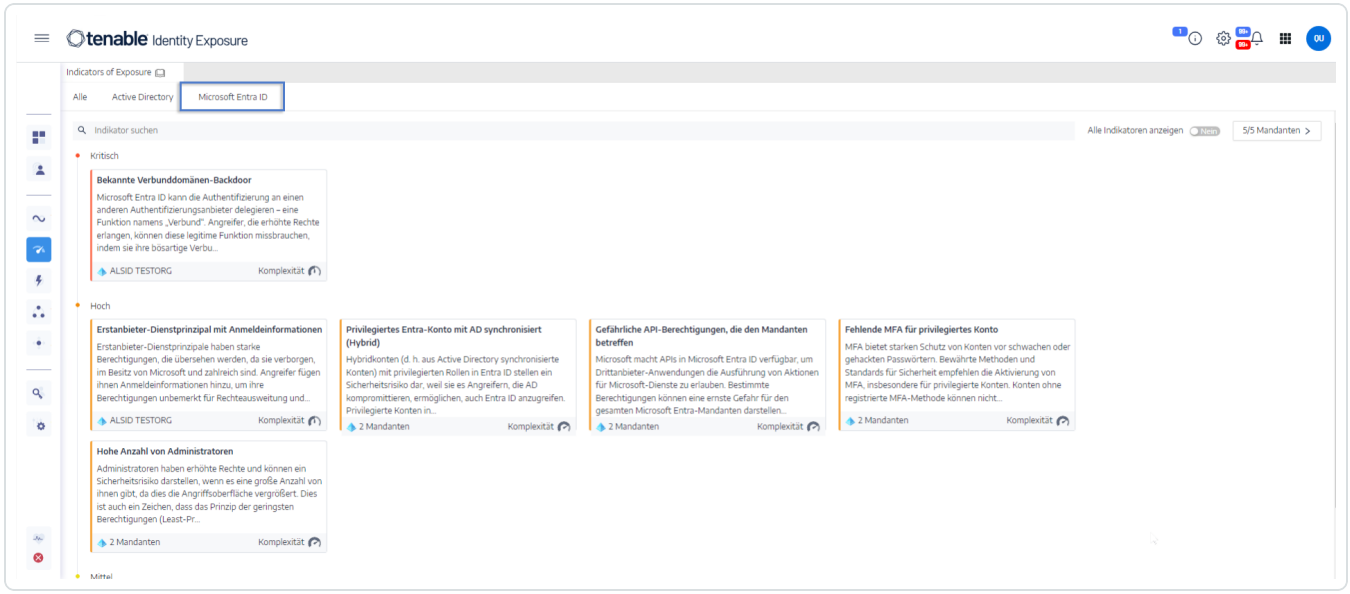
Hinweis: Mandantenscans erfolgen nicht in Echtzeit und erfordern mindestens 45 Minuten, bis Microsoft Entra ID-Daten im Identitäts-Explorer sichtbar sind.

- Wählen Sie einen Mandanten in der Liste aus und stellen Sie den Schalter auf **Scan aktiviert**.



Tenable Identity Exposure fordert einen Scan des Mandanten an und die Ergebnisse werden auf der Indicator of Exposure-Seite angezeigt.

Hinweis: Die obligatorische Mindestzeitspanne zwischen zwei Scans beträgt **30 Minuten**.



Tenable Cloud-Datensammlung

Tenable Cloud – die Datensammelfunktion in Tenable Identity Exposure – überträgt Ihre Informationen in die private Cloud, um Sicherheitsanalysen und -dienste bereitzustellen. Weitere Informationen zur Datenerfassung finden Sie in der Erklärung zu Vertrauen und Sicherheit von Tenable.

So verwenden Sie Tenable Cloud:

1. Klicken Sie in Tenable Identity Exposure in der seitlichen Navigationsleiste auf **System**.

   Der Fensterbereich **Systemkonfiguration** wird geöffnet.

2. Wählen Sie die Registerkarte **Konfiguration** aus.

3. Klicken Sie unter dem Abschnitt **Anwendungsdienste** auf **Tenable Cloud**.

   Der Fensterbereich **Tenable Cloud** wird geöffnet.

4. **Aktivieren** Sie den Umschalter „Tenable Cloud-Dienst verwenden“.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Konfiguration der Datenübertragung aktualisiert hat.

Privilegierte Analyse

„Privilegierte Analyse“ ist eine optionale Tenable Identity Exposure-Funktion, die – im Gegensatz zu den anderen Funktionen – mehr Rechte erfordert, um ansonsten geschützte Daten abzurufen und eine umfassendere Sicherheitsanalyse durchzuführen.

Datenabruf

> Hinweis: Die Funktion „Privilegierte Analyse“ erfordert erhöhte Rechte. Siehe Zugriff auf „Privilegierte Analyse“.

Wenn die Funktion „Privilegierte Analyse“ aktiviert ist, ruft sie die folgenden zusätzlichen Daten ab:

- **Passwort-Hashes** – Tenable Identity Exposure ruft LM- und NT-Hashes zur Passwortanalyse ab. Tenable Identity Exposure ruft LM-Hashes lediglich ab, um vor ihrem Vorhandensein zu warnen, da sie einen veralteten und schwachen Algorithmus verwenden. Diese Hashes werden jedoch nicht gespeichert. Die Hash-Erfassung umfasst Folgendes:
    - Alle aktivierten Benutzerkonten
    - Alle aktivierten Domänencontroller-Computerkonten

Datenschutz

Das Active Directory (AD) selbst speichert Benutzerkennwörter nicht direkt, sondern nur deren Hashes. Der hierzu verwendete LM- oder NT-Hashing-Algorithmus lässt keine Wiederherstellung des ursprünglichen Passworts zu. Tenable Identity Exposure speichert keine LM-Hashes.

Mit Ausnahme von Clients, die ihr Relay auf einer SAAS-VPN-Plattform hosten, verlassen Passwörter nie die Infrastruktur des Clients, da sie nur vom Relay verarbeitet werden. Das Relay speichert keine Passwörter, sondern ruft das Passwort des Benutzers jedes Mal ab, wenn es für Analysen benötigt wird. Es wird nur vorübergehend in seinem Cache gespeichert, in der Regel nur für einige Millisekunden. Tenable Identity Exposure bewahrt jedoch eine minimale Anzahl von Passwort-Hash-Datenbits auf, die sicher im RAM des Relay gespeichert werden. Diese dienen ausschließlich zur Durchführung einer K-Anonymitätsanalyse, um nach Benutzern mit identischen Passwörtern zu suchen.

> **Hinweis**: Für SaaS-VPN-Plattform-Clients ist das Verhalten identisch, allerdings wird das Relay von Tenable gehostet.

Aktivitätsprotokolle

Die Aktivitätsprotokolle in Tenable Identity Exposure enthalten die Spuren aller Aktivitäten, die auf der Tenable Identity Exposure-Plattform im Zusammenhang mit bestimmten IP-Adressen, Benutzern oder Aktionen stattgefunden haben.

So konfigurieren Sie die Aktivitätsprotokolle:

1. Klicken Sie in der seitlichen Navigationsleiste von Tenable Identity Exposure unter **Verwaltung** auf **System**.

   Der Fensterbereich **Systemkonfiguration** wird geöffnet.

2. Klicken Sie unter dem Abschnitt **Anwendungsdienste** auf **Aktivitätsprotokolle**.

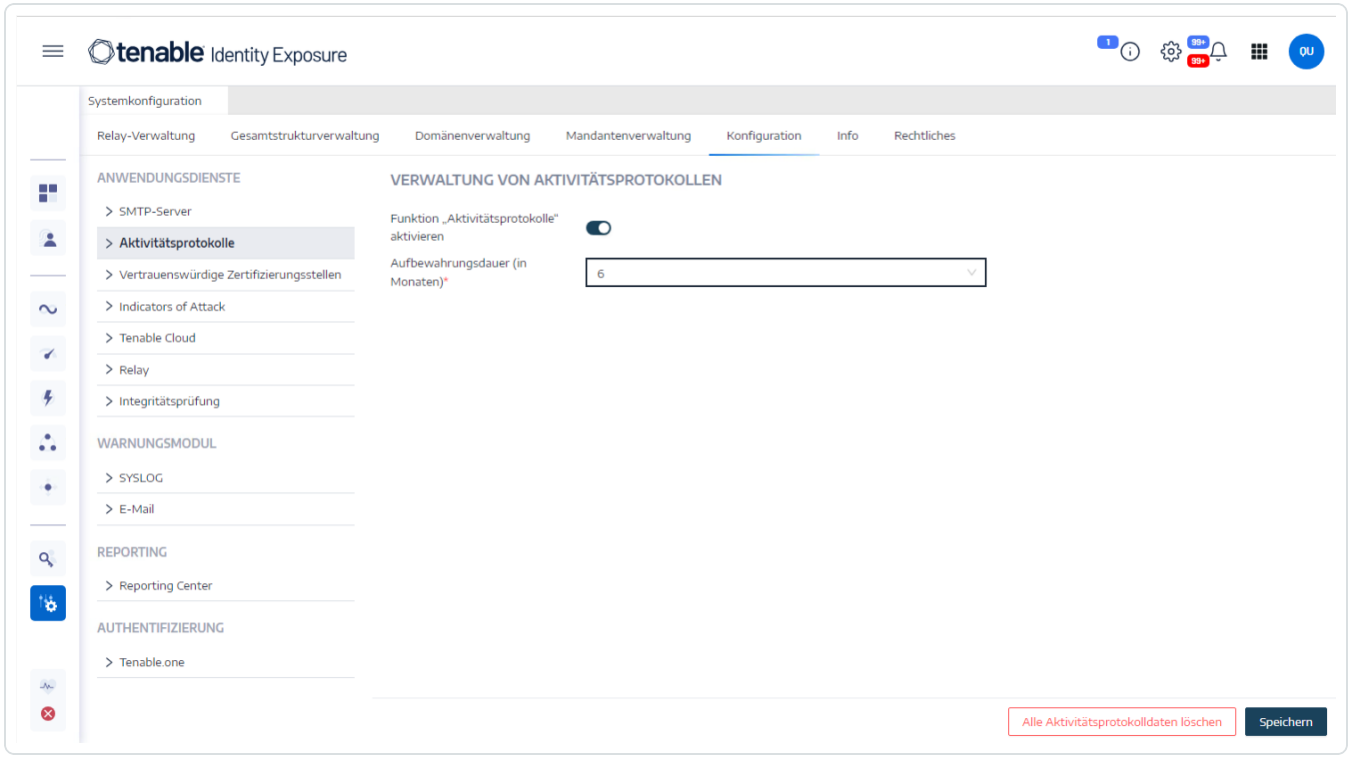
   Der Fensterbereich **Verwaltung von Aktivitätsprotokollen** wird geöffnet.

3. Um die Funktion „Aktivitätsprotokolle“ zu aktivieren, **aktivieren** Sie den Umschalter.

4. Klicken Sie im Feld „Aufbewahrungsdauer (in Monaten)“ auf **>**, um die Anzahl der Monate auszuwählen, für die Aktivitäten protokolliert werden sollen.

5. Klicken Sie auf **Speichern**.

Eine Meldung bestätigt, dass Tenable Identity Exposure die Einstellungen aktualisiert hat.



So löschen Sie die Aktivitätsprotokolldaten:

1. Klicken Sie in der seitlichen Navigationsleiste von Tenable Identity Exposure unter **Verwaltung** auf **System**.

   Der Fensterbereich **Systemkonfiguration** wird geöffnet.

2. Klicken Sie unter dem Abschnitt **Anwendungsdienste** auf **Aktivitätsprotokolle**.

   Der Fensterbereich **Verwaltung von Aktivitätsprotokollen** wird geöffnet.

3. Klicken Sie unter **Alle Aktivitätsprotokolldaten löschen** auf **Löschen**.

   In einer Meldung werden Sie aufgefordert, den Vorgang zu bestätigen.

4. Klicken Sie auf **Bestätigen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Einstellungen aktualisiert hat.

So legen Sie Berechtigungen für die eigenen Aktivitätsprotokolle eines Benutzers fest:

1. Klicken Sie in der seitlichen Navigationsleiste von Tenable Identity Exposure unter **Verwaltung** auf **Konten**.

   Der Fensterbereich **Benutzerkontenverwaltung** wird geöffnet.

2. Wählen Sie die Registerkarte **Rollenverwaltung** aus.

3. Fahren Sie in der Liste der Rollen mit dem Mauszeiger über die Benutzerrolle, die diese Berechtigung benötigt, und klicken auf das Symbol ✎ am Ende der Zeile.

   Der Fensterbereich **Rolle bearbeiten** wird geöffnet.

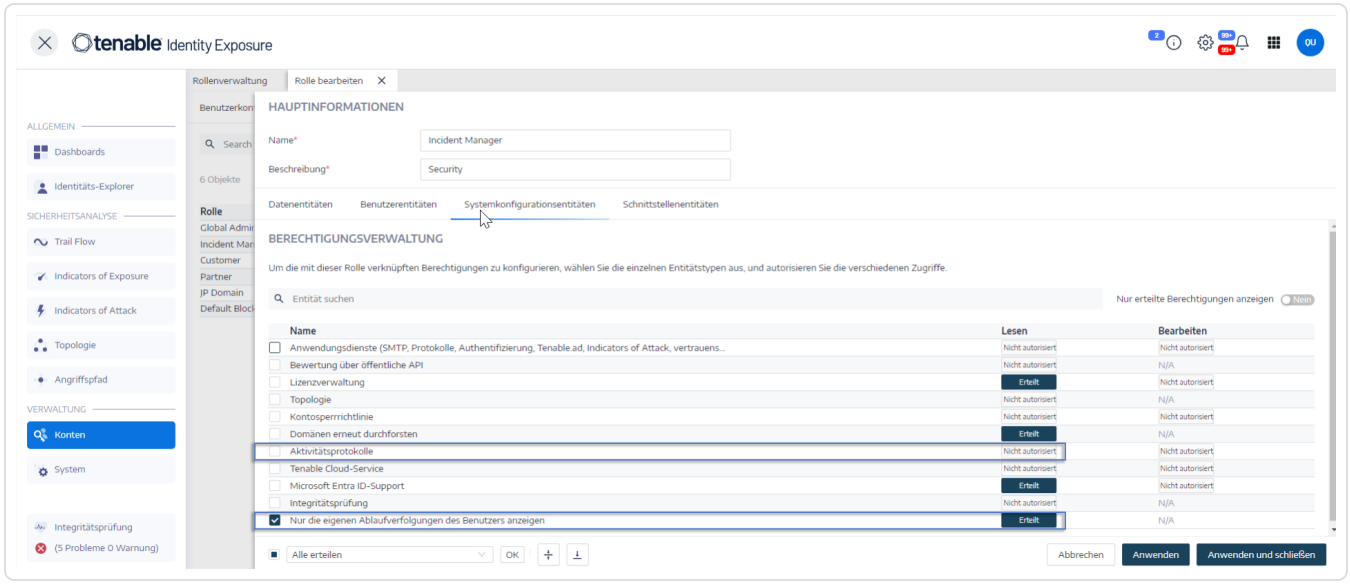
4. Wählen Sie unter dem Abschnitt **Hauptinformationen** die Registerkarte **Systemkonfigurationsentitäten** aus.

5. Gehen Sie im Abschnitt **Berechtigungsverwaltung** wie folgt vor:

   - Deaktivieren Sie die Berechtigung **Aktivitätsprotokolle**, sodass die Einstellung *Nicht autorisiert* lautet.
   - Aktivieren Sie die Berechtigung **Nur die Spuren der Benutzer anzeigen**, sodass die Einstellung *Erteilt* lautet.

6. Klicken Sie auf **Anwenden und schließen**.

   Eine Meldung bestätigt, dass Tenable Identity Exposure die Benutzerrolle aktualisiert hat.



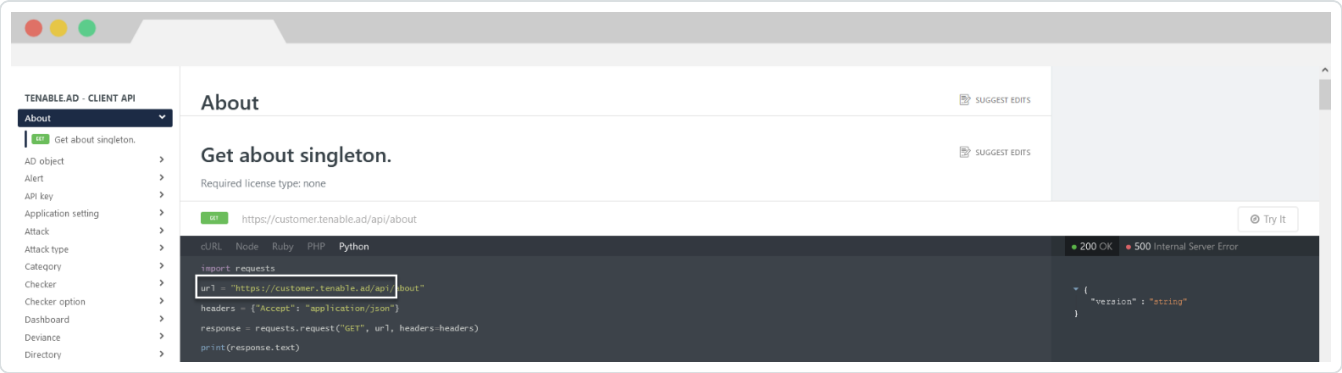
Öffentliche API von Tenable Identity Exposure

Die Tenable Identity Exposure-API ermöglicht es Ihnen, mit den Datenbankdiensten des Produkts zu kommunizieren.

Die OpenAPI-Datei mit der Struktur und den Ressourcen der Tenable Identity Exposure-API ist hier verfügbar.

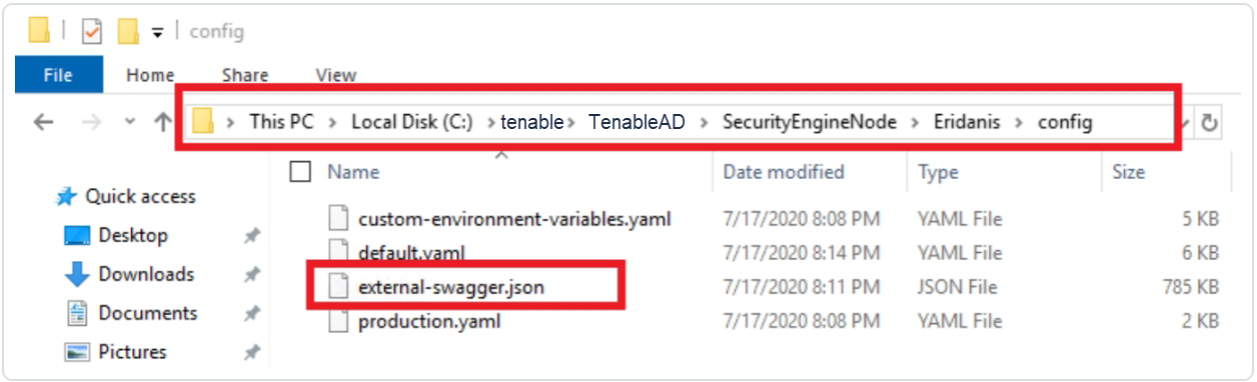
So greifen Sie auf die API für Ihre Tenable Identity Exposure-Instanz zu:

- Öffnen Sie in Ihrem Browser diese URL:



So laden Sie die OpenAPI-Datei herunter:

- Folgen Sie bei On-Premises-Installationen diesem Pfad zum Security Engine Node:



- Für SaaS-Installationen gehen Sie zum Tenable Identity Exposure API-Explorer.

So rufen Sie einen API-Schlüssel ab:

1. Klicken Sie in Tenable Identity Exposure auf das Symbol für Ihr Benutzerprofil und wählen Sie **Voreinstellungen** aus.

   Daraufhin wird der Fensterbereich „Voreinstellungen“ geöffnet.

2. Wählen Sie im Menü die Option **API-Schlüssel** aus.

   Tenable Identity Exposure zeigt Ihren aktuellen API-Schlüssel.

3. Um den API-Schlüssel in die Zwischenablage zu kopieren, klicken Sie auf das Symbol .

So aktualisieren Sie einen API-Schlüssel:

Zugriffstoken verfallen, wenn Sie auf **API-Schlüssel aktualisieren** klicken oder wenn Sie das Recht verlieren, einen API-Schlüssel oder ein Zugriffstoken zu generieren. Der Ablauf hängt nicht von der Zeit oder der Anzahl der API-Anfragen ab. Das Generieren oder Aktualisieren eines API-Schlüssels ist für den aktuellen Benutzer spezifisch und hat keine Auswirkungen auf API-Schlüssel anderer Konten. Zusammen mit einem API-Schlüssel erhalten Sie auch ein Aktualisierungstoken. Sie können dieses Aktualisierungstoken verwenden, um einen neuen API-Schlüssel abzurufen.

Achtung: Wenn Sie Ihren API-Schlüssel aktualisieren, deaktiviert Tenable Identity Exposure den aktuellen API-Schlüssel. Sie erhalten außerdem ein Aktualisierungstoken.

1. Klicken Sie auf **API-Schlüssel aktualisieren**.

   In einer Meldung werden Sie aufgefordert, den Vorgang zu bestätigen.

2. Klicken Sie auf **Bestätigen**.

Datenverwaltung

Tenable Identity Exposure bewahrt Daten sechs Monate lang auf. Dieser Datenverwaltungszeitraum ist nicht konfigurierbar.

Bereitstellungsregionen

Tenable Identity Exposure SaaS wird derzeit in den folgenden Azure-Regionen bereitgestellt:

Land	Azure-Region
Nord-, Mittel- und Südamerika	
Brasilien – São Paulo	Brasilien, Süden
Kanada – Québec (Stadt)	Kanada, Osten
Kanada – Toronto	Kanada, Mitte
USA – Kalifornien	USA, Westen
USA – Iowa	USA, Mitte
USA – Virginia	USA, Osten 2
Europa, Naher Osten, Afrika	
Frankreich – Paris	Frankreich, Mitte
Irland	Nordeuropa
Niederlande	Westeuropa
Südafrika – Johannesburg	Südafrika, Norden
Schweiz – Zürich	Schweiz, Norden
Vereinigte Arabische Emirate – Dubai	VAE, Norden
Vereinigtes Königreich – London	Vereinigtes Königreich, Süden
Asien-Pazifik	
Australia – New South Wales	Australien, Osten
Australien – Victoria	Australien, Südosten
Hongkong	Asien, Osten
Indien – Pune	Indien, Mitte

Japan – Osaka	Japan, Westen
Singapur	Asien, Südosten

Lizenzierung von Tenable Identity Exposure

In diesem Thema wird das Verfahren zur Lizenzierung von Tenable Identity Exposure als eigenständiges Produkt beschrieben. Außerdem wird erläutert, wie Assets gezählt werden und was bei Überschreitung oder Ablauf von Lizenzen geschieht. Informationen zur Verwendung von Tenable Identity Exposure finden Sie im Tenable Identity Exposure-Benutzerhandbuch.

Tenable Identity Exposure lizenzieren

Tenable Identity Exposure ist in zwei Versionen erhältlich: als Cloud-Version und als On-Premises-Version. Tenable bietet in einigen Fällen auch ein Subscription-Preismodell an.

Um Tenable Identity Exposure nutzen zu können, erwerben Sie Lizenzen, die auf den Anforderungen Ihres Unternehmens und den Umgebungsdetails basieren. Tenable Identity Exposure weist diese Lizenzen dann Ihren *Assets* zu – dies sind aktivierte Benutzer in Ihren Verzeichnisdiensten.

Wenn Ihre Umgebung größer wird, steigt auch die Anzahl Ihrer Assets. Um dieser Änderung Rechnung zu tragen, erwerben Sie zusätzliche Lizenzen. Für Tenable-Lizenzen gilt eine progressive Preisgestaltung: Je mehr Lizenzen Sie erwerben, desto geringer ist der Preis pro Einheit. Informationen zu Preisen erhalten Sie von dem für Sie zuständigen Tenable-Mitarbeiter.

Tipp: Um Ihre aktuelle Lizenzanzahl und die verfügbaren Assets anzuzeigen, klicken Sie in der oberen Navigationsleiste von Tenable auf  und dann auf **Lizenzinformationen**. Weitere Informationen finden Sie auf der Seite mit Lizenzinformationen.

Hinweis: Tenable bietet für Managed Security Service Providers (MSSPs) eine vereinfachte Preisgestaltung an. Weitere Informationen erhalten Sie von dem für Sie zuständigen Tenable-Mitarbeiter.

Zählung von Assets

Jede Tenable Identity Exposure-Lizenz, die Sie erwerben, berechtigt Sie zum Scannen einer eindeutigen Identität oder digitalen Darstellung eines Benutzers. Identitäten werden in Tenable nicht doppelt gezählt. Beispielsweise zählen Benutzerkonten, die für dieselbe Identität sowohl in Microsoft Active Directory als auch in Microsoft Entra ID aktiviert sind, als eine einzige Tenable-Lizenz.

Komponenten von Tenable Identity Exposure

Beide Versionen von Tenable Identity Exposure werden mit den folgenden Komponenten geliefert:

- Trail Flow-Ansicht
- Topologieansicht
- Indicators of Exposure
- Indicators of Attack
- Angriffspfade
- Identitäts-Explorer
- Microsoft Entra ID-Support

Lizenzen zurückfordern

Wenn Sie Lizenzen erwerben, bleibt die Gesamtanzahl Ihrer Lizenzen für die Dauer Ihres Vertrags unverändert, es sei denn, Sie erwerben weitere Lizenzen. Tenable Identity Exposure fordert jedoch Lizenzen in Echtzeit zurück, wenn Sie aktivierte Benutzer aus dem Verzeichnisdienst Ihrer Umgebung löschen.

Überschreitung der maximalen Lizenzanzahl

Um Nutzungsspitzen aufgrund von Hardware-Aktualisierungen, plötzlicher Expansion der Umgebung oder unerwarteten Bedrohungen auszugleichen, sind Tenable-Lizenzen elastisch. Wenn Sie jedoch mehr Assets scannen, als Lizenzen vorhanden sind, weist Tenable Sie deutlich auf die Überschreitung hin und schränkt dann die Funktionalität in drei Stufen ein.

Szenario	Ergebnis
Sie haben an drei aufeinanderfolgenden Tagen mehr aktivierte Identitäten als Lizenzen.	Eine Meldung wird in Tenable Identity Exposure angezeigt.
Sie haben an mehr als 15 Tagen mehr aktivierte Identitäten als Lizenzen.	Eine Meldung und eine Warnung zu eingeschränkter Funktionalität werden in Tenable Identity Exposure angezeigt.
Sie haben an mehr als 45 Tagen mehr	Eine Meldung wird in Tenable Identity Exposure

aktivierte Identitäten als Lizenzen.	angezeigt. Exportfunktionen werden deaktiviert.

Abgelaufene Lizenzen

Die von Ihnen erworbenen Tenable Identity Exposure-Lizenzen sind für die Dauer Ihres Vertrags gültig. 30 Tage vor Ablauf Ihrer Lizenz wird eine Warnung in der Benutzeroberfläche angezeigt. Setzen Sie sich während dieses Verlängerungszeitraums mit dem für Sie zuständigen Tenable-Mitarbeiter in Verbindung, um Produkte hinzuzufügen oder zu entfernen oder die Anzahl Ihrer Lizenzen zu ändern.

Wenn Ihre Lizenz abgelaufen ist, können Sie sich nicht mehr bei der Tenable-Plattform einloggen.

Lizenz verwalten

Die für Tenable Identity Exposure erforderliche Lizenzdatei erhalten Sie von Tenable oder über autorisierte Unternehmenspartner. Die Anzahl der Lizenzbenutzer umfasst alle aktivierten Benutzer und Dienstkonten.

Sie müssen die Lizenzdatei hochladen, um Tenable Identity Exposure zu konfigurieren und zu nutzen.

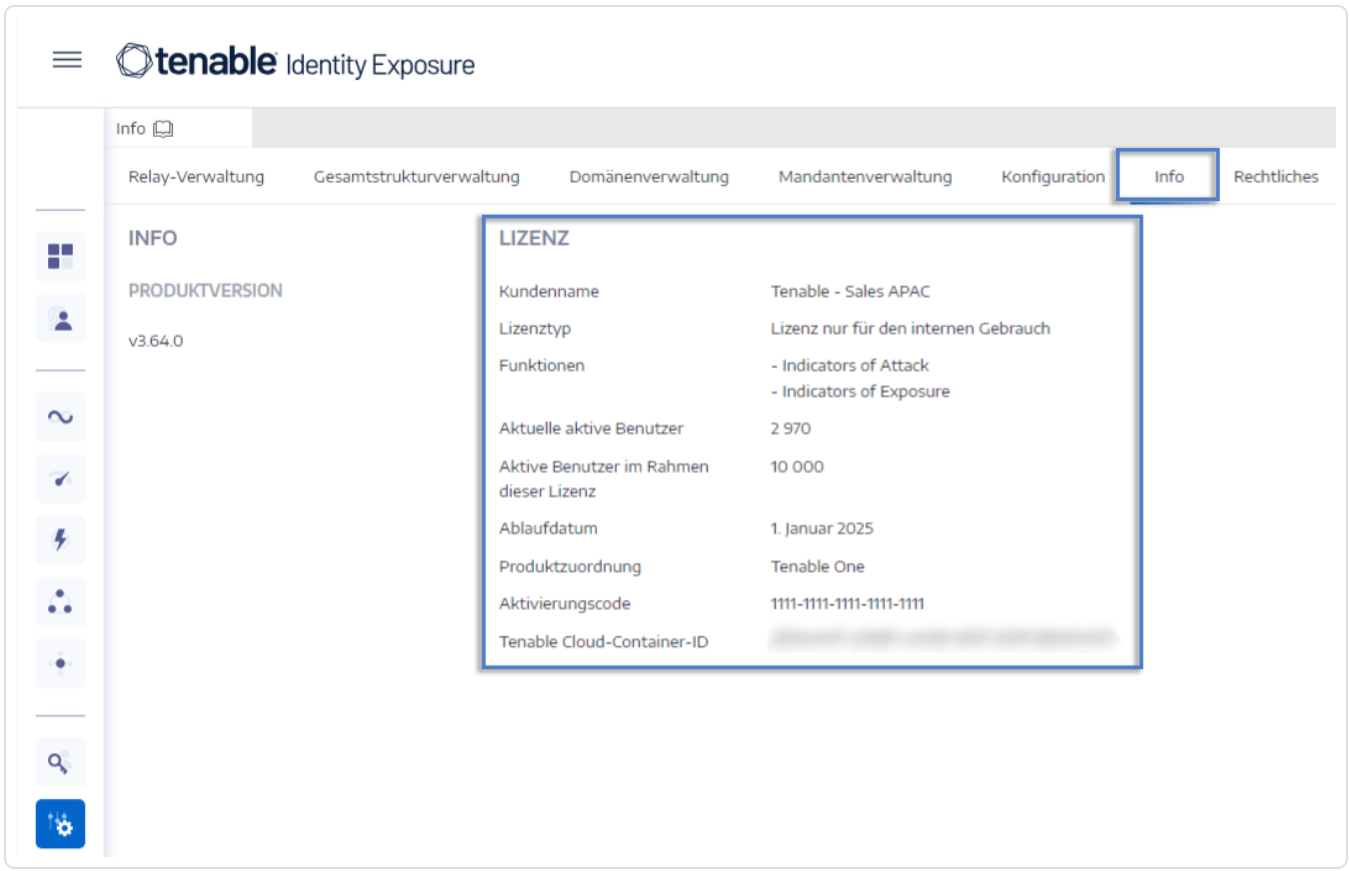
Die Tenable Identity Exposure-Lizenzen können Folgendes umfassen:

- Indicators of Attack
- Indicators of Exposure
- Beide der oben genannten

So zeigen Sie Ihre Lizenz an:

- Klicken Sie in Tenable Identity Exposure auf **Systeme**  > Registerkarte **Info**.

  Die Lizenz wird angezeigt.



Lizenzverbrauch

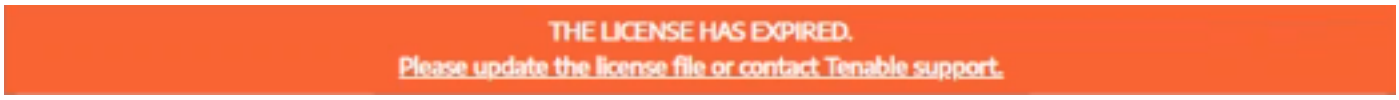
Bei On-Premises-Installationen verfolgt Tenable Identity Exposure den Lizenzverbrauch, wenn eine Internetverbindung verfügbar ist.

Gültigkeit der Lizenz

Die Tenable Identity Exposure-Lizenz bleibt gültig, solange Sie die folgenden Kriterien erfüllen:

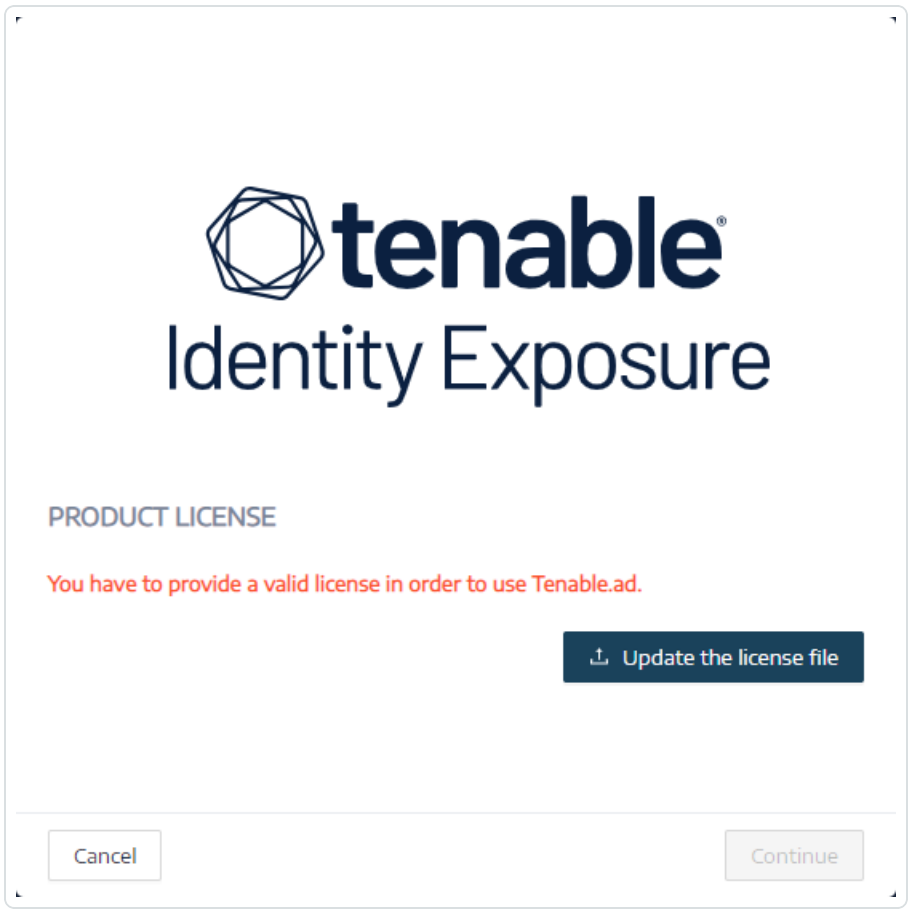
- Die Anzahl der Benutzer überschreitet nicht die von der Lizenz abgedeckte Anzahl.
- Das Ablaufdatum ist noch nicht überschritten.

Wenn Sie eines der oben genannten Kriterien nicht erfüllen, zeigt Tenable Identity Exposure eine Warnung an und fordert Sie auf, Ihre Lizenz zu aktualisieren:



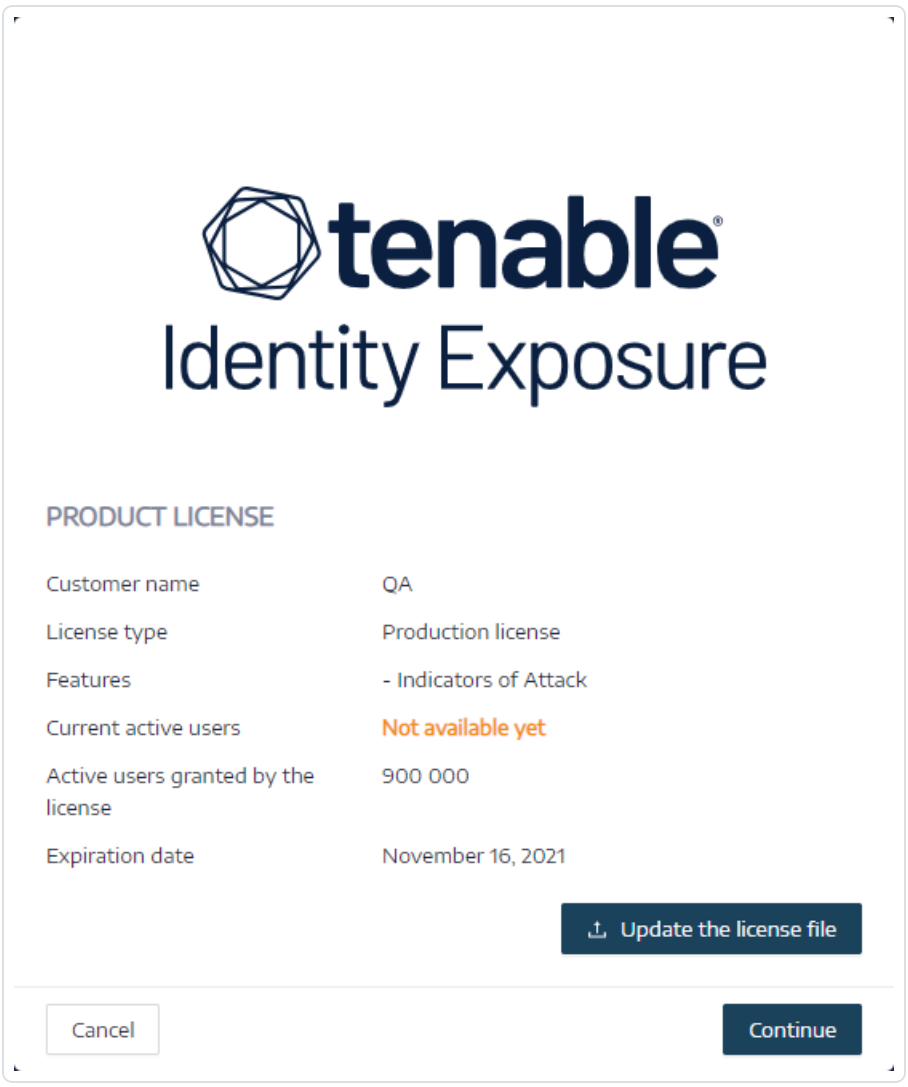
So laden Sie eine Lizenzdatei hoch:

1. Klicken Sie im Login-Fenster auf **Lizenzdatei aktualisieren**.



2. Navigieren Sie zum Speicherort Ihrer Lizenzdatei und klicken Sie auf **Öffnen**.

   Das folgende Beispiel zeigt eine erfolgreich angewandte Lizenzdatei:



3. Klicken Sie auf **Weiter**, um Tenable Identity Exposure zu öffnen.

So aktualisieren Sie eine Lizenzdatei:

1. Klicken Sie in Tenable Identity Exposure auf **System** und **Info**.
2. Klicken Sie auf **Lizenzdatei aktualisieren**.
3. Navigieren Sie zum Speicherort Ihrer Lizenzdatei und klicken Sie auf **Öffnen**.

   Ihre Lizenz wird von Tenable Identity Exposure aktualisiert. Wenden Sie sich im Falle einer ungültigen Lizenzdatei an den Kundensupport.

Tenable Identity Exposure-Fehlerbehebung

Die folgenden Themen unterstützen Sie bei Problemen, die bei der Arbeit mit Tenable Identity Exposure (ehemals Tenable.ad) auftreten können:

- Tenable Identity Exposure-Diagnosetool
- Störung des Tenable Identity Exposure-Betriebs durch SYSVOL-Härtung

Tenable Identity Exposure-Diagnosetool

Tenable Identity Exposure stellt ein Diagnosetool bereit, mit dem Sie Protokollinformationen im Zusammenhang mit Ihrer Tenable Identity Exposure-Installation abrufen können, damit der Kundensupport jedes Problem analysieren und Ihnen helfen kann.

Sie laden dieses Diagnosetool aus dem Tenable Download-Portal herunter.

> **Hinweis**: Dieses Diagnosetool funktioniert nur für **On-Premises-Installationen** von Tenable Identity Exposure.

Das Diagnosetool kann die folgenden Aufgaben ausführen:

- Identifizieren, ob der aktuelle Computer (auf dem Sie die ausführbare Datei gestartet haben) den Storage Manager (SM), den Security Engine Node (SEN) oder den Directory Listener (DL) hostet
- Die Umgebung überprüfen, um nach anderen in Ihrem Netzwerk verfügbaren Tenable Identity Exposure-Installationen zu suchen
- Eine Liste von Protokollquellen im Zusammenhang mit Ihren Tenable Identity Exposure-Installationen erkennen, um diese zu testen und Informationen darüber abzurufen
- MSI-Protokolle zu fehlgeschlagenen Tenable Identity Exposure-Installationsversuchen abrufen

Einige Tipps für beste Ergebnisse

- Führen Sie das Diagnosetool auf dem SEN aus.
- Führen Sie das Diagnosetool mit einem Benutzer mit erhöhten Rechten aus, um die meisten oder alle Protokollquellen zu aktivieren.
- Um den SM oder eine andere Installation zu erkennen, überprüfen Sie, ob die folgenden Bedingungen erfüllt sind:
    - Die Konfiguration ermöglicht die Ausführung von Remotebefehlen auf dem Remote-Computer (Invoke-Command-Cmdlet).
    - Die Konfiguration ermöglicht den Remote-Zugriff auf Festplatten.
    - WMI ist aktiviert und für das aktuelle Benutzerkonto zulässig.

So führen Sie das Diagnosetool aus:

1. Laden Sie die Datei `TenableAdDiagnosticTool.OnPrem.Console.exe` aus dem Tenable Download-Portal herunter.
2. Führen Sie die ausführbare Datei als Administrator auf einem Tenable Identity Exposure-Computer aus, vorzugsweise demjenigen, der den SEN hostet.
3. Geben Sie an der Eingabeaufforderung eine der folgenden Optionen ein:
   - `E` – Alle Protokolle (Standardoption)
   - `Msi` – Protokolle im Zusammenhang mit Tenable Identity Exposure-Installationen
   - `Tenable` – Protokolle im Zusammenhang mit Tenable Identity Exposure
4. Drücken Sie die Eingabetaste.

   Das Diagnosetool überprüft Ihre Installation. Nach Abschluss der Überprüfung erhalten Sie eine gezippte Datei, die sich in Ihrem aktuellen Verzeichnis befindet.
5. Senden Sie diese ZIP-Datei an den Tenable Identity Exposure-Kundensupport. Achten Sie darauf, den Dateiinhalt in keiner Weise zu verändern.

So führen Sie das Diagnosetool über die Befehlszeile aus:

1. Führen Sie in der Befehlszeile die ausführbare Datei `TenableAdDiagnosticTool.OnPrem.Console.exe` als Administrator auf dem Tenable Identity Exposure-Computer aus, vorzugsweise demjenigen, auf dem der SEN gehostet wird.

   Das Diagnosetool überprüft Ihre Installation. Nach Abschluss der Überprüfung erhalten Sie eine ZIP-Datei, die sich in Ihrem aktuellen Verzeichnis befindet.
2. Senden Sie diese ZIP-Datei an den Tenable Identity Exposure-Kundensupport. Achten Sie darauf, den Dateiinhalt in keiner Weise zu verändern.

Andere Optionen

Bei Ausführung des Diagnosetools über die Befehlszeile stehen außerdem die folgenden Optionen zur Verfügung:

- `--help` – Eine kurze Beschreibung der Verwendung des Diagnosetools.
- `--commands` – Eine Liste von PowerShell-/WMI-Abfragen, mit denen die Computerfunktionen getestet und andere Installationen überprüft werden können.

Störung des Tenable Identity Exposure-Betriebs durch SYSVOL-Härtung

SYSVOL ist ein freigegebener Ordner, der sich auf jedem Domänencontroller (DC) in einer Active Directory-Domäne befindet. In ihm werden die Ordner und Dateien für Gruppenrichtlinienobjekte (GPOs) gespeichert. Der Inhalt des SYSVOL-Ordners wird über alle DCs repliziert und der Zugriff erfolgt über UNC-Pfade (Universal Naming Convention) wie `\\<beispiel.com>\SYSVOL` oder `\\<DC_IP_oder_FQDN>\SYSVOL`.

SYSVOL-Härtung bezieht sich auf die Verwendung des Parameters „UNC Hardened Paths“, auch bekannt als „Gehärteter UNC-Zugriff“, „UNC-Pfad-Härtung“ oder „Gehärtete Pfade“ usw. Diese Funktion wurde als Reaktion auf die Schwachstelle MS15-011 (KB 3000483) in Gruppenrichtlinien entwickelt. Viele Cybersicherheitsstandards wie CIS-Benchmarks schreiben die Durchsetzung dieser Funktion vor.

Wenn Sie diesen Härtungsparameter auf SMB-Clients (Server Message Block) anwenden, erhöht er tatsächlich die Sicherheit der in die Domäne eingebundenen Computer, um sicherzustellen, dass der GPO-Inhalt, den die Computer von SYSVOL abrufen, nicht von einem Angreifer im Netzwerk manipuliert wird. In bestimmten Situationen kann dieser Parameter jedoch auch die Funktion von Tenable Identity Exposure stören.

Befolgen Sie die Anleitung in diesem Fehlerbehebungsabschnitt, wenn Sie feststellen, dass gehärtete UNC-Pfade die Konnektivität zwischen Tenable Identity Exposure und der SYSVOL-Freigabe unterbrechen.

Betroffene Umgebungen

Dieses Problem kann bei den folgenden Tenable Identity Exposure-Bereitstellungsoptionen auftreten:

- On-Premises
- SaaS mit Secure Relay

Diese Bereitstellungsoption ist nicht betroffen:

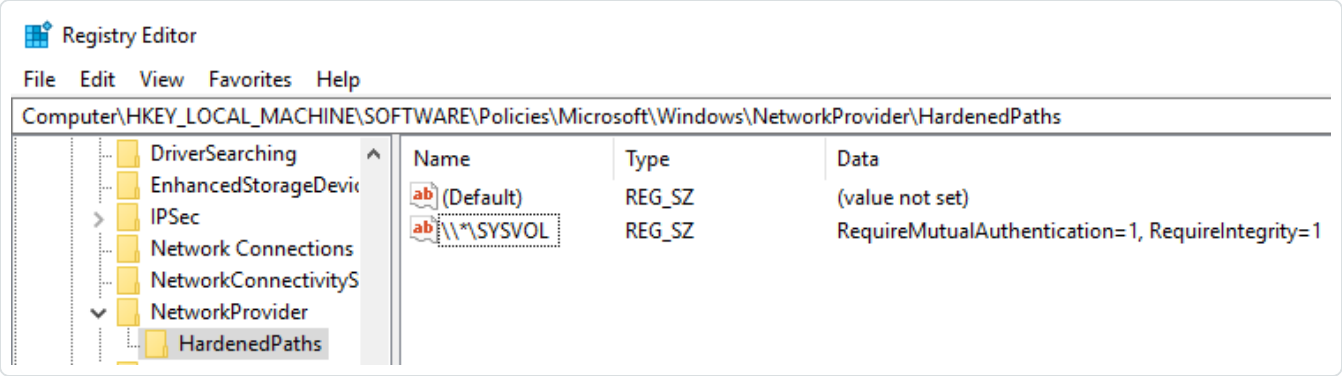
- SaaS mit VPN

Die SYSVOL-Härtung ist ein clientseitiger Parameter und wird daher auf den Computern angewendet, die eine Verbindung zur SYSVOL-Freigabe herstellen, und nicht auf den Domänencontrollern.

Dieser Parameter wird von Windows standardmäßig aktiviert und kann die Funktion von Tenable Identity Exposure stören.

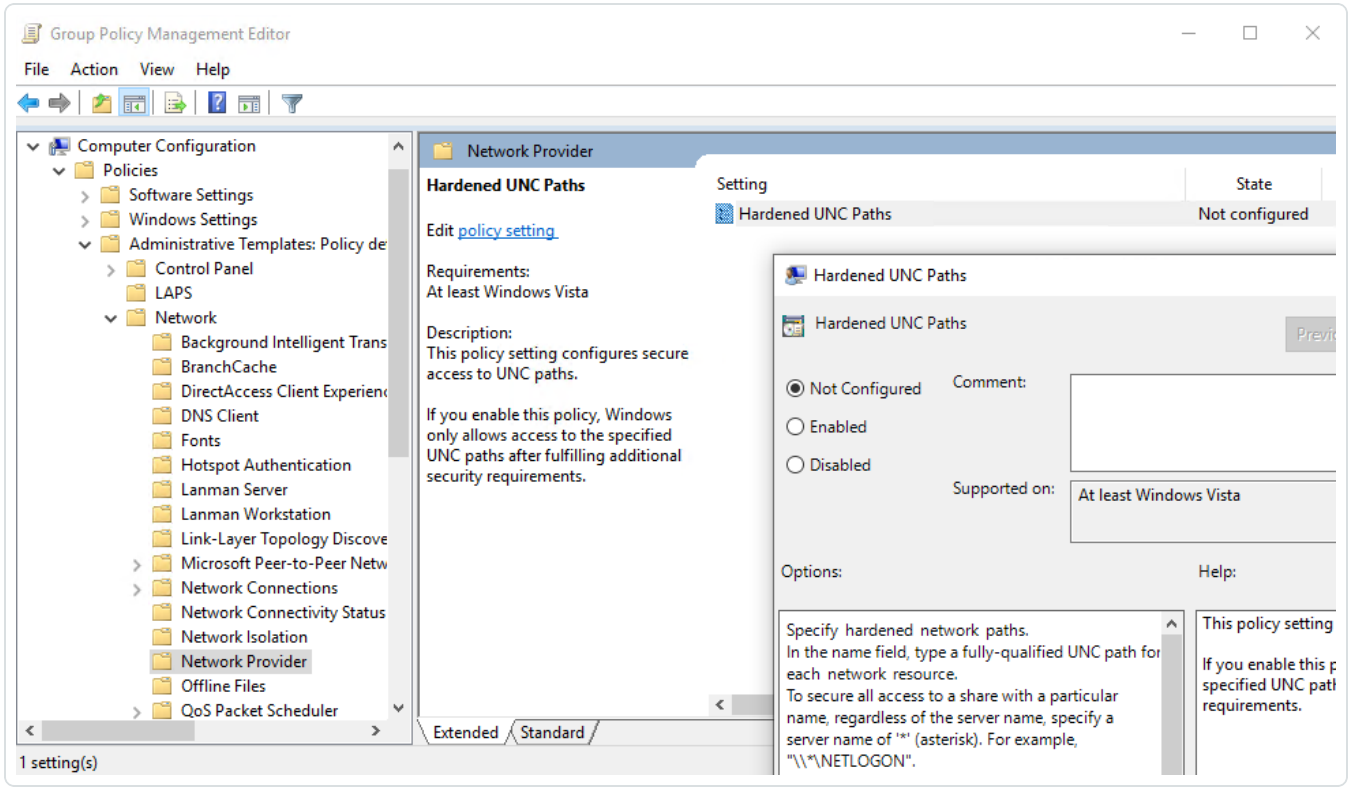
Einige Organisationen möchten die Aktivierung dieses Parameters sicherstellen und erzwingen seine Nutzung, indem sie die zugehörige GPO-Einstellung verwenden oder den entsprechenden Registrierungsschlüssel direkt festlegen.

- Sie finden die Registrierungsschlüssel zu gehärteten UNC-Pfaden unter „`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`“:



- Die entsprechende GPO-Einstellung finden Sie unter „`Computerkonfiguration/Administrative`

`Vorlagen/Netzwerk/Netzwerkanbieter/Gehärtete UNC-Pfade`“:



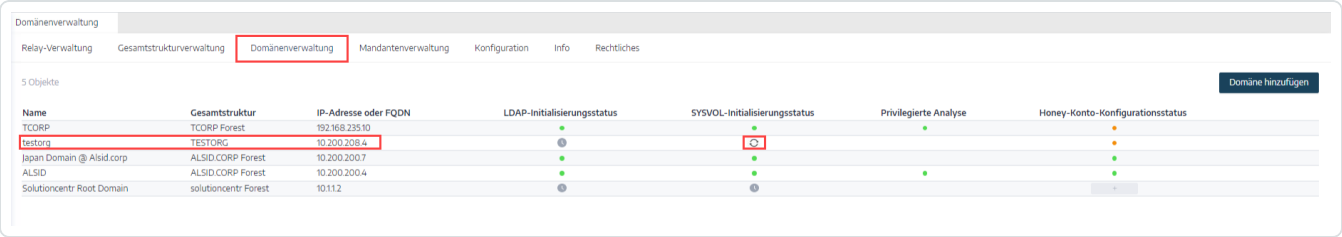
Die SYSVOL-Härtung wird erzwungen, wenn in einem UNC-Pfad, der auf SYSVOL verweist – zum Beispiel „`\\*\SYSVOL`“ – die Parameter „`RequireMutualAuthentication`“ und „`RequireIntegrity`“ auf den Wert „`1`“ festgelegt sind.

Anzeichen für durch SYSVOL-Härtung verursachte Probleme

Wenn Sie vermuten, dass die SYSVOL-Härtung die Funktion von Tenable Identity Exposure stört, überprüfen Sie Folgendes:

1. Gehen Sie in Tenable Identity Exposure zu **System** > **Domänenverwaltung**, um den LDAP- und SYSVOL-Initialisierungsstatus für jede Domäne anzuzeigen.

   Für eine Domäne mit normaler Konnektivität wird ein grüner Indikator angezeigt, während für eine Domäne mit Konnektivitätsproblemen ein Durchforstungsindikator angezeigt werden kann, der endlos weiterläuft.



2. Öffnen Sie auf dem Directory Listener- oder Relay-Computer den Protokollordner: `<Installationsordner>\DirectoryListener\logs`.

3. Öffnen Sie die Ceti-Protokolldatei und suchen Sie nach der Zeichenfolge „SMB mapping creation failed“ oder „Access is denied“. Fehlerprotokolle, die diesen Ausdruck enthalten, weisen darauf hin, dass wahrscheinlich eine UNC-Härtung auf dem Directory Listener- oder Relay-Computer stattfindet.

Mögliche Behebungsmaßnahmen

Es gibt zwei mögliche Behebungsmaßnahmen: Wechsel zur Kerberos-Authentifizierung oder Deaktivierung der SYSVOL-Härtung.

Wechsel zur Kerberos-Authentifizierung

Dies ist die bevorzugte Option, da hierbei die Härtungsfunktion nicht deaktiviert werden muss.

Eine Störung von Tenable Identity Exposure durch die SYSVOL-Härtung tritt nur dann auf, wenn die Verbindung zu den überwachten Domänencontrollern mithilfe von NTLM-Authentifizierung hergestellt wird. Dies liegt daran, dass NTLM nicht mit dem Parameter „`RequireMutualAuthentication=1`“ kompatibel ist. Tenable Identity Exposure unterstützt auch Kerberos. Die SYSVOL-Härtung muss nicht deaktiviert werden, wenn Sie Kerberos ordnungsgemäß konfigurieren und verwenden. Weitere Informationen finden Sie unter Kerberos-Authentifizierung.

Deaktivierung der SYSVOL-Härtung

Wenn Sie nicht zur Kerberos-Authentifizierung wechseln können, haben Sie auch die Möglichkeit, die SYSVOL-Härtung zu deaktivieren.

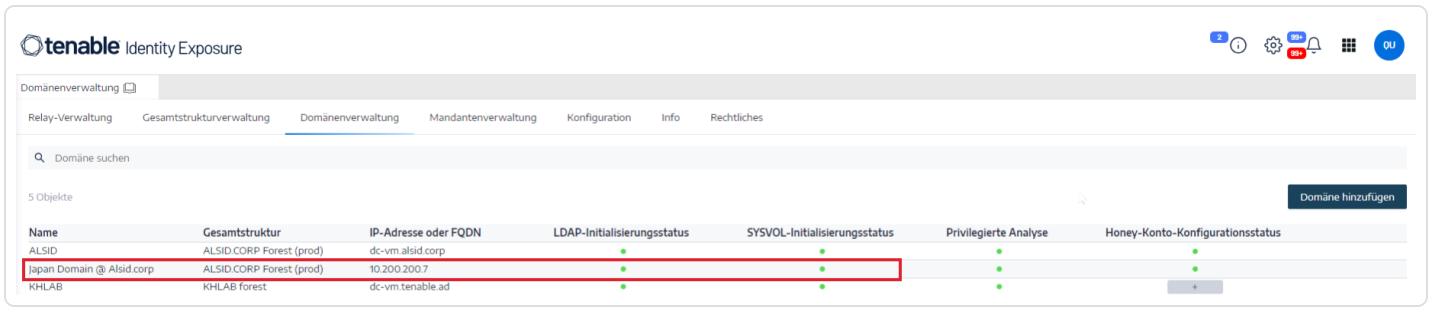
Die SYSVOL-Härtung wird von Windows standardmäßig aktiviert, sodass es nicht ausreicht, lediglich den Registrierungsschlüssel oder die GPO-Einstellung zu entfernen. Sie müssen die Funktion explizit deaktivieren und diese Änderung nur auf den Computer anwenden, der den Directory Listener (On-Premises) oder das Relay (SaaS mit Secure Relay) hostet. Andere Computer sind davon nicht betroffen, und Sie müssen die SYSVOL-Härtung nie auf den Domänencontrollern selbst deaktivieren.

Die Tenable Identity Exposure-Installationsprogramme, die auf dem Computer verwendet werden, auf dem der Directory Listener (On-Premises) oder das Relay (SaaS mit Secure Relay) gehostet wird, deaktivieren die SYSVOL-Härtung bereits lokal. Der Registrierungsschlüssel kann jedoch durch ein GPO oder ein Skript in Ihrer Umgebung entfernt oder überschrieben werden.

Es gibt zwei mögliche Fälle:

- Der Directory Listener- oder Relay-Computer **ist nicht in die Domäne eingebunden**: Sie können kein GPO verwenden, um den Computer zu konfigurieren. Sie müssen die SYSVOL-Härtung in der Registrierung deaktivieren (siehe Registrierung – GUI oder Registrierung – PowerShell).
- Der Directory Listener- oder Relay-Computer **ist in eine Domäne eingebunden** (wird von Tenable Identity Exposure nicht empfohlen): Sie können die Einstellung entweder direkt in der Registrierung anwenden (siehe Registrierung – GUI oder Registrierung – PowerShell) oder ein GPO verwenden. Wenn Sie eine dieser Methoden verwenden, müssen Sie sicherstellen, dass ein GPO oder Skript den Registrierungsschlüssel nicht überschreibt. Hierzu haben Sie zwei Möglichkeiten:
    - Überprüfen Sie sorgfältig alle GPOs, die auf diesem Computer gelten.
    - Wenden Sie die Änderung an und warten Sie ein wenig, oder erzwingen Sie die Anwendung der GPOs mit „`gpupdate /force`“ und überprüfen Sie, ob der Wert des Registrierungsschlüssels beibehalten wurde.

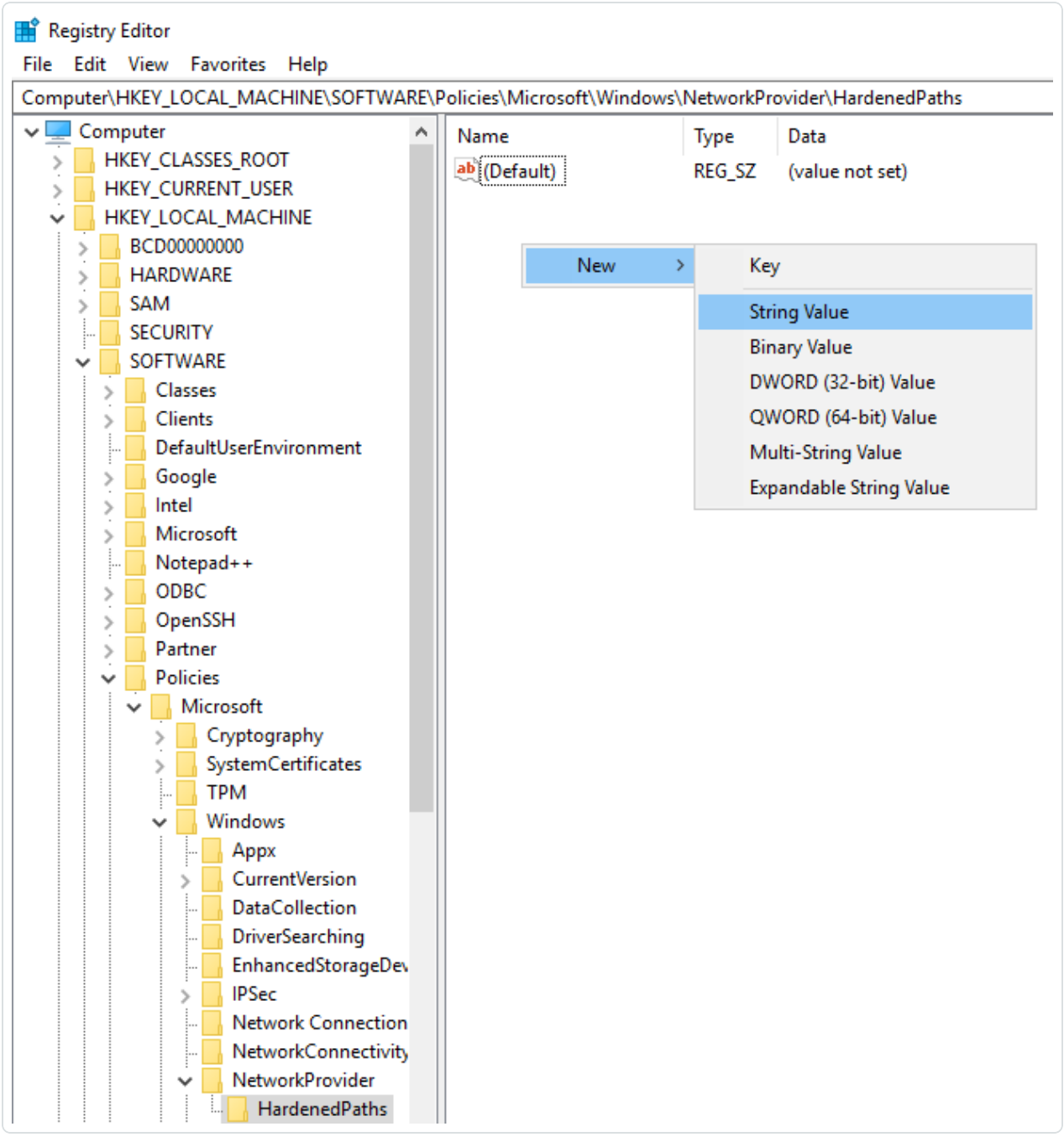
Nachdem Sie den Directory Listener- oder Relay-Computer neu gestartet haben, sollte der Durchforstungsindikator in der geänderten Domäne sich in einen grünen Indikator ändern:



Registrierung – GUI

So deaktivieren Sie die SYSVOL-Härtung in der Registrierung unter Verwendung der GUI:

1. Stellen Sie mit Administratorrechten eine Verbindung zum Directory Listener- oder Relay-Computer her.
2. Öffnen Sie den Registrierungs-Editor und navigieren Sie zu: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`.
3. Erstellen Sie wie folgt einen Schlüssel mit dem Namen „`\\*\SYSVOL`“, falls er noch nicht vorhanden ist:
    a. Klicken Sie mit der rechten Maustaste in den rechten Bereich und wählen Sie **Neu** > **Zeichenfolge** aus.



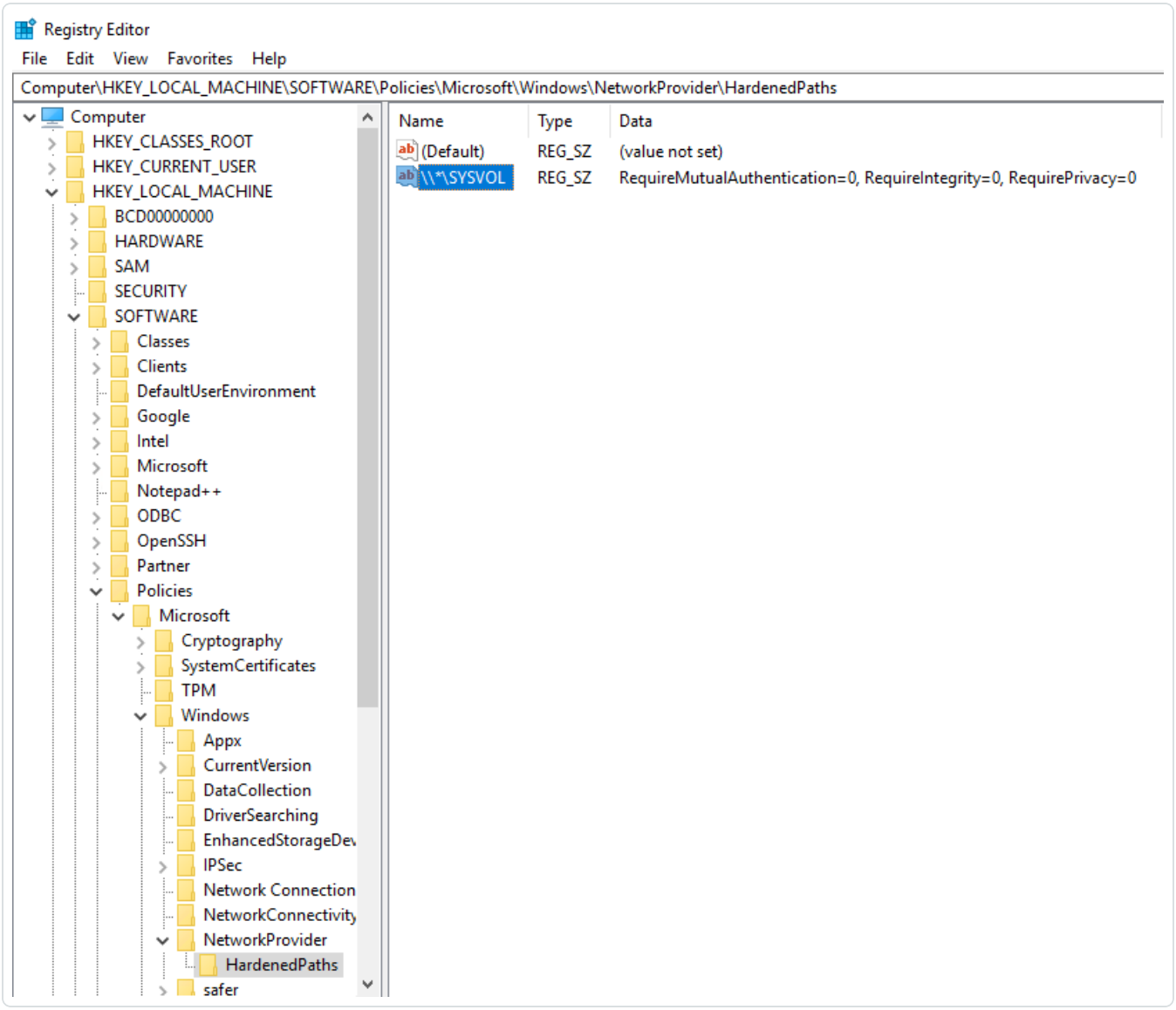
b. Geben Sie im Namensfeld `\\*\SYSVOL` ein.

4. Doppelklicken Sie auf den Schlüssel „`\\*\SYSVOL`“ (neu erstellt oder bereits vorhanden), um das Fenster **Zeichenfolge bearbeiten** zu öffnen.

5. Geben Sie im Datenfeld **Wert** den folgenden Wert ein: `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

6. Klicken Sie auf **Speichern**.

   Das Ergebnis sollte wie folgt aussehen:



7. Starten Sie den Computer neu.

Registrierung – PowerShell

So deaktivieren Sie die SYSVOL-Härtung in der Registrierung unter Verwendung von PowerShell:

1. Erfassen Sie zu Referenzzwecken die aktuellen Werte der Registrierungsschlüssel für gehärtete UNC-Pfade mit diesem PowerShell-Befehl:

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. Legen Sie den empfohlenen Wert fest:

```
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. Starten Sie den Computer neu.

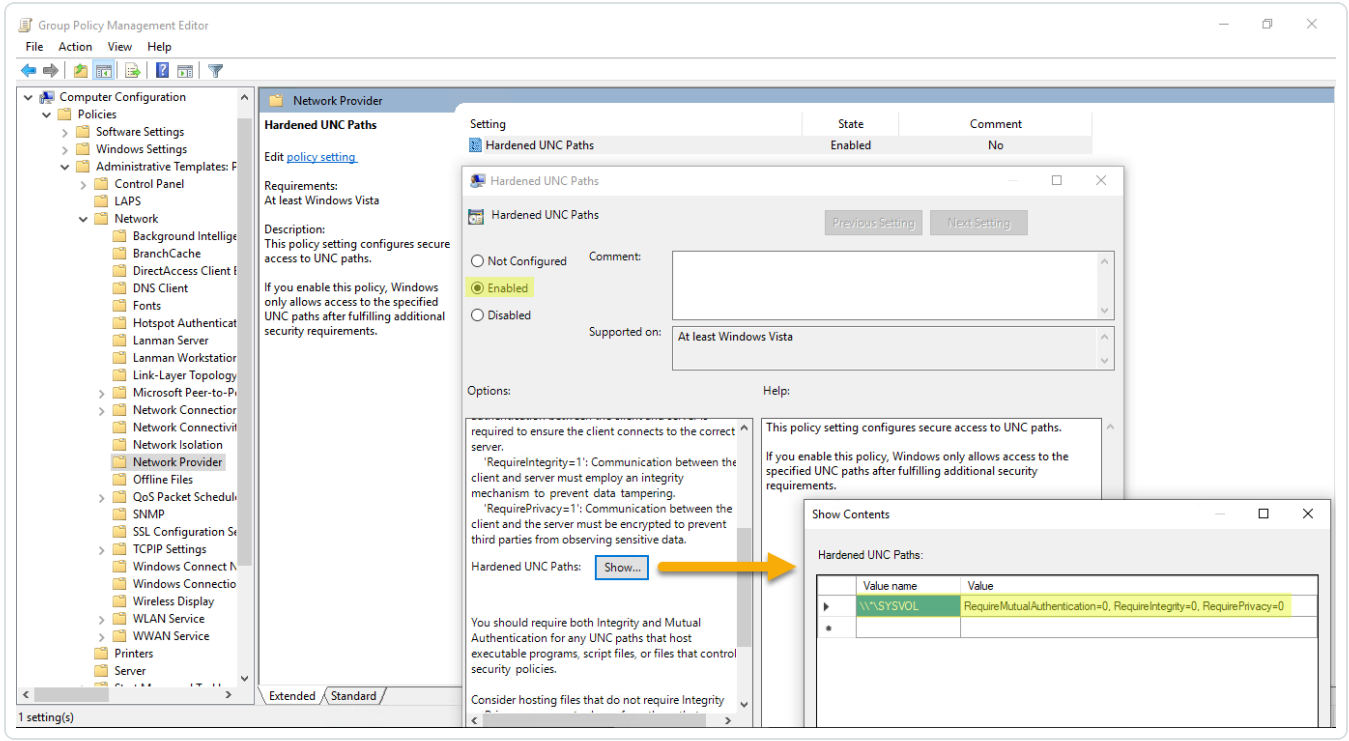
GPO

Voraussetzung: Sie müssen sich als Active Directory-Benutzer verbinden, der über die Rechte zum Erstellen von GPOs in der Domäne und zum Verknüpfen der GPOs mit der Organisationseinheit verfügt, die den Tenable Identity Exposure Directory Listener- oder Relay-Computer enthält.

So deaktivieren Sie die SYSVOL-Härtung unter Verwendung eines GPO:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Erstellen Sie ein neues GPO.
3. Bearbeiten Sie das GPO und navigieren Sie zum folgenden Ort: `Computerkonfiguration/Administrative Vorlagen/Netzwerk/Netzwerkanbieter/Gehärtete UNC-Pfade`.
4. Aktivieren Sie diese Einstellung und erstellen Sie einen neuen gehärteten UNC-Pfad mit folgenden Angaben:
   - Wertname = `\\*\SYSVOL`
   - Wert = `RequireMutualAuthentication=0`, `RequireIntegrity=0`, `RequirePrivacy=0`

   Das Ergebnis sollte wie folgt aussehen:

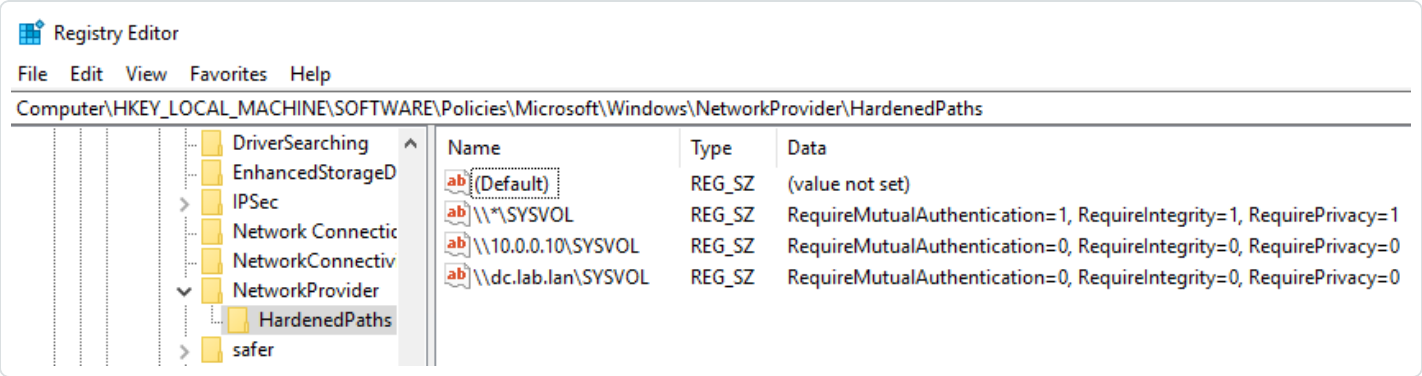


5. Klicken Sie zur Bestätigung auf **OK**.
6. Verknüpfen Sie dieses GPO mit der Organisationseinheit, die den Tenable Identity Exposure Directory Listener- oder Relay-Computer enthält. Sie können auch die GPO-Funktion für Sicherheitsgruppenfilter verwenden, um sicherzustellen, dass dieses GPO nur für diesen Computer gilt.

Ausnahmen für bestimmte UNC-Pfade

In den vorherigen Verfahren wird die SYSVOL-Härtung mit einem Platzhalter-UNC-Pfad deaktiviert: „`\\*\SYSVOL`“. Sie können die Funktion auch nur für eine bestimmte IP-Adresse oder einen FQDN deaktivieren. Das bedeutet, dass Sie die Einstellungen für gehärtete UNC-Pfade für „`\\*\SYSVOL`“ aktiviert lassen (mit Wert „`1`“) und eine Ausnahme für jede IP-Adresse oder jeden FQDN eines in Tenable Identity Exposure konfigurierten Domänencontrollers festlegen können.

Die folgende Abbildung zeigt ein Beispiel für die Aktivierung der SYSVOL-Härtung für alle Server („*“), mit Ausnahme von „`10.0.0.10`“ und „`dc.lab.lan`“, bei denen es sich um Domänencontroller handelt, die in Tenable Identity Exposure konfiguriert wurden:



Sie können diese zusätzlichen Einstellungen mithilfe der oben beschriebenen Registrierungs- oder GPO-Methoden hinzufügen.

Hinweis: Sie müssen den genauen Wert angeben, der in Tenable Identity Exposure konfiguriert ist (z. B. können Sie keine IP-Adresse angeben, wenn die Tenable Identity Exposure-Konfiguration einen FQDN verwendet). Denken Sie auch daran, diese Schlüssel jedes Mal zu aktualisieren, wenn Sie eine IP-Adresse oder einen FQDN auf der Domänenverwaltungsseite von Tenable Identity Exposure ändern.

Risiken bei der Deaktivierung der SYSVOL-Härtung

Die SYSVOL-Härtung ist eine Sicherheitsfunktion, deren Deaktivierung berechtigte Bedenken aufwerfen kann.

- Nicht in die Domäne eingebundene Computer: Es besteht kein Risiko beim Deaktivieren der SYSVOL-Härtung. Da diese Computer keine GPOs anwenden, erhalten sie keine Inhalte von der SYSVOL-Freigabe, um sie auszuführen.
- In Domänen eingebundene Computer (Directory Listener- oder Relay-Computer) (wird von Tenable Identity Exposure nicht empfohlen): Wenn das potenzielle Risiko besteht, dass sich ein Angreifer in einer „Man-in-the-Middle"-Situation zwischen dem Directory Listener- oder Relay-Computer und den Domänencontrollern befindet, ist die Deaktivierung der SYSVOL-Härtung nicht sicher. In diesem Fall empfiehlt Tenable Identity Exposure, stattdessen zur Kerberos-Authentifizierung zu wechseln.

Diese Deaktivierung wird nur auf den Directory Listener- oder Relay-Computer angewendet, nicht auf andere Domänencomputer und niemals auf die Domänencontroller.