TENABLE.OT

BENUTZERHANDBUCH

VERSION 3.15

REVISIONSVERLAUF

Produktversion: Tenable.ot 3.15

Revisionsverlauf des Dokuments:

Dokumentrevision	Datum	Beschreibung
1.0	8. Oktober 2018	Erste Version des Benutzerhandbuchs für Version 2.5 erstellt
1.1	28. Januar 2019	Aktualisiert für Version 2.7
1.2	20. August 2019	Aktualisiert für Version 3.1
1.3	10. Oktober 2019	Überarbeitet für aktuell unterstützte Funktionen
1.4	12. Januar 2019	Aktualisiert für Version 3.3
1.5	24. März 2020	Aktualisiert für Version 3.4
1.6	6. April 2020	Aktualisiert für Version 3.5
1.7	27. April 2020	Dokumentation von Sensoren hinzugefügt
1.8	3. Juni 2020	Aktualisiert für Version 3.6
1.9	8. August 2020	Aktualisiert für Version 3.7
2.0	11. Oktober 2020	Aktualisiert für Version 3.8
2.1	2. Dezember 2020	Aktualisiert für Version 3.9
2.2	6. April 2021	Aktualisiert für Version 3.10
2.3	30. Juni 2021	Aktualisiert für Version 3.11
2.4	12. Dezember 2021	Aktualisiert für Version 3.12
2.5	25. März 2022	Aktualisiert für Version 3.13
2.6	22. August 2022	Aktualisiert für Version 3.14
2.7	25. September 2022	SAML-Integration hinzugefügt (SP1)
2.8	31. Januar 2023	Aktualisiert für Version 3.15

INHALT

EINFÜHRUNG

Tenable.ot schützt industrielle Netzwerke vor Cyberbedrohungen, böswilligen Insidern und menschlichen Fehlern. Von der Bedrohungserkennung und -entschärfung bis hin zu Asset-Verfolgung, Schwachstellen-Management, Konfigurationskontrolle und Active Querying-Überprüfungen – die ICS-Sicherheitsfunktionen von Tenable.ot maximieren die Transparenz, Sicherheit und Kontrolle Ihrer Betriebsumgebungen.

Tenable.ot bietet umfassende Sicherheitstools und Berichte für IT-Sicherheitspersonal und OT-Ingenieure. Es bietet einen beispiellosen Einblick in konvergente IT/OT-Segmente und ICS-Aktivitäten und liefert ein klares Lagebild für alle Standorte und ihre jeweiligen OT-Assets – von Windows-Servern bis hin zu SPS-Backplanes – in einer zentralen, einheitlichen Ansicht.

Tenable.ot bietet die folgenden wichtigen Leistungsmerkmale:

- **360-Grad-Sichtbarkeit –** Angriffe können sich in einer IT/OT-Infrastruktur leicht ausbreiten. Mit einer einzigen Plattform zur Verwaltung und Messung des Cyberrisikos für Ihre OT- und IT-Systeme erhalten Sie einen vollständigen Einblick in Ihre konvergente Angriffsoberfläche. Tenable.ot lässt sich auch nativ in führende IT-Sicherheits- und Betriebstools integrieren, wie z. B. Ihre Security Information and Event Management(SIEM)-Lösung, Protokollverwaltungstools, Next-Generation-Firewalls und Ticketing-Systeme. Zusammen entsteht dadurch ein Ökosystem des Vertrauens, in dem all Ihre Sicherheitsprodukte als Einheit zusammenarbeiten können, um Ihre Umgebung zu schützen.
- **Bedrohungserkennung und -entschärfung** – Tenable.ot nutzt eine Multi-Detection Engine, um hochriskante Ereignisse und Verhaltensweisen zu finden, die sich auf den OT-Betrieb auswirken können. Diese Engines umfassen richtlinien-, verhaltens- und signaturbasierte Erkennung.
- **Asset-Inventarisierung und aktive Erkennung** – Tenable.ot nutzt bahnbrechende patentierte Technologie und bietet einen beispiellosen Einblick in Ihre Infrastruktur – nicht nur auf Netzwerkebene, sondern bis hinunter auf die Geräteebene. Es verwendet native Kommunikationsprotokolle, um sowohl IT- als auch OT-Geräte in Ihrer ICS-Umgebung aktiv abzufragen und alle Aktivitäten und Aktionen zu identifizieren, die in Ihrem Netzwerk ausgeführt werden.
- **Risikobasiertes Schwachstellen-Management** – Auf der Grundlage umfassender und detaillierter Funktionen zur Verfolgung von IT- und OT-Assets generiert Tenable.ot Schwachstellen- und Risikostufen mithilfe von Predictive Prioritization für jedes Asset in Ihrem ICS-Netzwerk. Diese Berichte enthalten Risikobewertungen und detaillierte Einblicke sowie Vorschläge zur Risikominderung.
- **Konfigurationskontrolle** – Tenable.ot stellt einen vollständigen granularen Verlauf der Gerätekonfigurationsänderungen im Laufe der Zeit, einschließlich spezifischer Kontaktplan-Segmente, Diagnosepuffer, Tag-Tabellen und mehr. Auf diese Weise können Administratoren einen Backup-Snapshot mit dem „letzten bekannten guten Zustand" für eine schnellere Wiederherstellung und Einhaltung von Branchenvorschriften erstellen.

Tenable.ot-Technologien

Die umfassende Lösung Tenable.ot umfasst zwei zentrale Erfassungstechnologien:

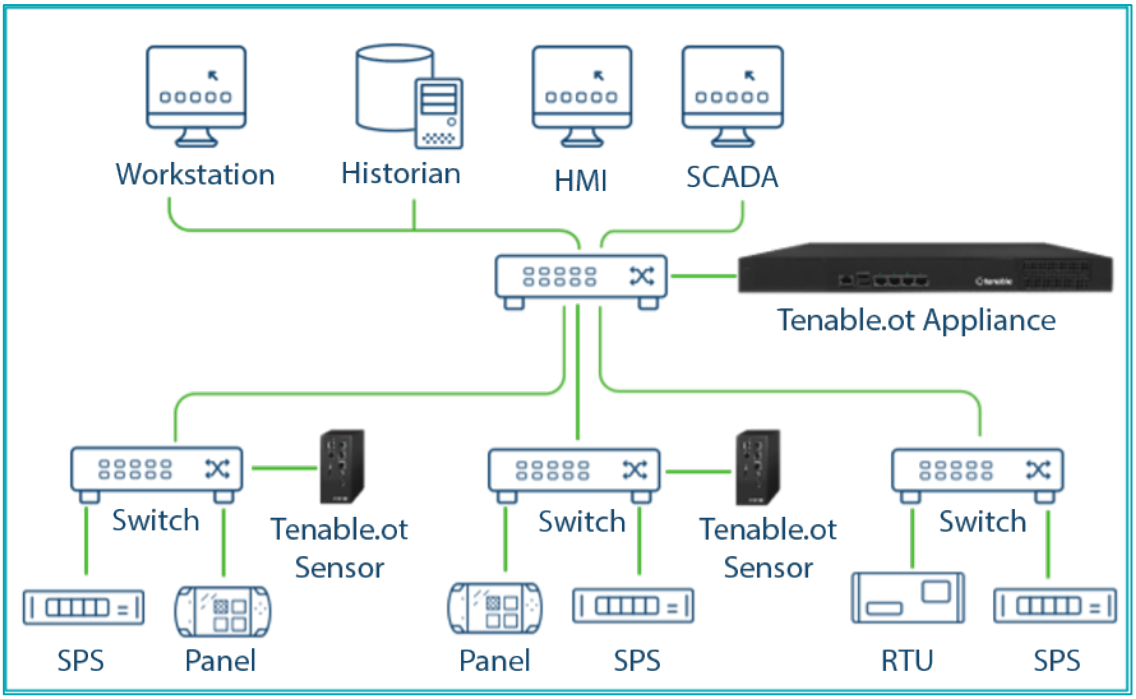
- **Netzwerkerkennung** – Die Netzwerkerkennungstechnologie von Tenable.ot ist eine passive Deep-Packet Inspection Engine, die speziell für die einzigartigen Eigenschaften und Anforderungen industrieller Steuerungssysteme entwickelt wurde. Die Netzwerkerkennung bietet detaillierte Echtzeit-Einblicke in alle Aktivitäten, die über das Betriebsnetzwerk durchgeführt werden, mit einem einzigartigen Fokus auf Engineering-Aktivitäten. Dazu gehören Firmware-Downloads/-Uploads, Code-Updates und Konfigurationsänderungen, die über proprietäre, anbieterspezifische Kommunikationsprotokolle stattfinden. Die Netzwerkerkennung warnt in Echtzeit vor verdächtigen/nicht autorisierten Aktivitäten und erstellt ein umfassendes Ereignisprotokoll mit forensischen Daten. Die Netzwerkerkennung generiert drei Arten von Warnungen:
    - **Richtlinienbasiert** – Sie können vordefinierte Richtlinien aktivieren oder benutzerdefinierte Richtlinien erstellen, die bestimmte granulare Aktivitäten, die auf Cyberbedrohungen oder Betriebsfehler hinweisen, auf die Zulassungsliste und/oder Sperrliste setzen, um Warnungen auszulösen. Es können auch Richtlinien festgelegt werden, um Prüfungen aktiver Abfragen für vordefinierte Situationen auszulösen.
    - **Verhaltensanomalien** – Das System erkennt Abweichungen von einer Baseline für den Netzwerk-Traffic, die basierend auf Traffic-Mustern während eines bestimmten Zeitraums festgelegt wurde. Außerdem erkennt es verdächtige Scans, die auf Malware und Auskundschaftsverhalten hinweisen.
    - **Signaturerkennungsrichtlinien** – Diese Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert wurden.
- **Aktive Abfrage** – Die patentierte Abfragetechnologie von Tenable.ot überwacht Geräte, die sich im Netzwerk befinden, indem sie regelmäßig die Metadaten von Kontrollgeräten im ICS-Netzwerk abfragt. Diese Funktionalität verbessert die Fähigkeit von Tenable.ot, alle ICS-Ressourcen, einschließlich untergeordneter Geräte wie SPS und RTUs, automatisch zu erkennen und zu klassifizieren, selbst wenn sie nicht im Netzwerk aktiv sind. Sie identifiziert außerdem lokal implementierte Änderungen in den Metadaten des Geräts (z. B. Firmware-Version, Konfigurationsdetails und Status) sowie Änderungen in jedem Code-/Funktionsblock der Gerätelogik. Da sie schreibgeschützte Abfragen in den nativen Controller-Kommunikationsprotokollen verwendet, ist sie absolut sicher und hat keine Auswirkungen auf die Geräte. Abfragen können regelmäßig nach einem vordefinierten Zeitplan oder nach Bedarf durch den Benutzer ausgeführt werden.

Lösungsarchitektur

Tenable.ot-Plattformkomponenten

Die Tenable.ot-Lösung besteht aus zwei Komponenten:

- **Tenable.ot Appliance** – Diese Komponente erfasst und analysiert den Netzwerk-Traffic direkt aus dem Netzwerk (über einen Span-Port oder Netzwerk-Tap) und/oder mithilfe eines Datenfeeds von den Tenable.ot Sensoren. Die Tenable.ot Appliance führt sowohl die Netzwerkerkennung als auch die aktive Abfrage aus.
- **Tenable.ot Sensoren** – Kleine Geräte, die in Netzwerksegmenten von Interesse bereitgestellt werden können, bis zu einem Sensor pro Managed Switch. Die Sensoren sind in zwei Formfaktoren erhältlich: kompakte Rack-Montage oder DIN-Schienenmontage. Tenable.ot Sensoren bieten einen vollständigen Einblick in diese Netzwerksegmente, indem sie den gesamten Traffic erfassen, ihn analysieren und die Informationen dann an die Tenable.ot Appliance übermitteln. Sensoren der Version 3.14 und höher können auch so konfiguriert werden, dass sie aktive Abfragen an die Netzwerksegmente senden, in denen sie bereitgestellt werden.



Netzwerkbereitstellung der Tenable.ot Appliance und Sensoren

Netzwerkkomponenten

Tenable.ot unterstützt die Interaktion mit den folgenden Netzwerkkomponenten:

- **Tenable.ot-Benutzer (Verwaltung)** – Benutzerkonten werden erstellt, um den Zugriff auf die Tenable.ot-Verwaltungskonsole zu steuern. Der Zugriff auf die Verwaltungskonsole erfolgt mit einem Webbrowser (Google Chrome) über Secure Socket-Layer-Authentifizierung (HTTPS).

> Auf die Benutzeroberfläche kann nur über einen Chrome-Browser zugegriffen werden. Zudem muss die neueste Version von Chrome verwendet werden.

- **Active Directory-Server** – Benutzerzugangsdaten können optional über einen LDAP-Server wie beispielsweise Active Directory zugewiesen werden. In diesem Fall werden die Benutzerrechte in Active Directory verwaltet.
- **SIEM** – Tenable.ot-Ereignisprotokolle können mithilfe des Syslog-Protokolls an SIEM gesendet werden.
- **SMTP-Server** – Tenable.ot-Ereignisbenachrichtigungen können per E-Mail über einen SMTP-Server an bestimmte Mitarbeitergruppen gesendet werden.
- **DNS-Server** – DNS-Server können in Tenable.ot integriert werden, um bei der Auflösung von Asset-Namen zu helfen.
- **Anwendungen von Drittanbietern** – Externe Anwendungen können mit Tenable.ot über dessen REST-API interagieren oder über andere spezifische Integrationen auf Daten zugreifen[1].

Systemelemente

Assets

Assets sind die Hardwarekomponenten in Ihrem Netzwerk, wie beispielsweise Controller, Engineering-Stationen, Server usw. Die automatisierte Asset-Erfassung, -Klassifizierung und -Verwaltung von Tenable.ot ermöglicht eine präzise Asset-Inventarisierung, indem alle Änderungen an Geräten kontinuierlich verfolgt werden. Dies vereinfacht die Aufrechterhaltung der betrieblichen Kontinuität, Zuverlässigkeit und Sicherheit. Es spielt außerdem eine wichtige Rolle bei der Planung von Wartungsprojekten, der Priorisierung von Upgrades, der Bereitstellung von Patches sowie bei der Vorfallsreaktion und Risikominderungsmaßnahmen.

Risikobewertung

Tenable.ot wendet ausgefeilte Algorithmen an, um den Grad des Risikos zu bewerten, dem jedes Asset im Netzwerk ausgesetzt ist. Für jedes Asset im Netzwerk wird ein *Risikowert* (von 0 bis 100) vergeben. Der Risikowert basiert auf den folgenden Faktoren:

- **Ereignisse** – Ereignisse, die im Netzwerk aufgetreten sind und sich auf das Gerät ausgewirkt haben (gewichtet basierend auf dem Schweregrad des Ereignisses und dem Zeitpunkt, zu dem das Ereignis aufgetreten ist).

Ereignisse werden nach Aktualität gewichtet, sodass neuere Ereignisse einen größeren Einfluss auf den Risikowert haben als ältere Ereignisse.

- **Schwachstellen** – CVEs, die Assets in Ihrem Netzwerk betreffen, sowie andere in Ihrem Netzwerk identifizierte Bedrohungen (z. B. veraltete Betriebssysteme, Verwendung anfälliger Protokolle, anfällige offene Ports usw.). In Tenable.ot werden diese als Plugin-Treffer auf Ihren Assets erkannt.
- **Asset-Kritikalität** – ein Messwert, der die Wichtigkeit des Geräts für das ordnungsgemäße Funktionieren des Systems angibt.

Bei SPS, die an eine Backplane angeschlossen sind, wirkt sich der Risikowert anderer Module, die die Backplane gemeinsam nutzen, auf den Risikowert der SPS aus.

Richtlinien und Ereignisse

Richtlinien werden verwendet, um bestimmte Arten von Ereignissen zu definieren, die verdächtig, nicht autorisiert, anormal oder anderweitig auffällig sind und im Netzwerk stattfinden. Wenn ein Ereignis eintritt, das alle Bedingungen der

[1] Beispielsweise unterstützt Tenable.ot die Integration mit Palo Alto Networks Next Generation Firewall (NGFW) und Aruba ClearPass, wodurch Tenable.ot Asset-Inventarisierungsdaten mit diesen Systemen austauschen kann. Tenable.ot kann auch mit anderen Tenable-Plattformen wie Tenable.io und Tenable.sc integriert werden. Integrationen werden unter **Lokale Einstellungen** > **Integrationen** konfiguriert, siehe **Lokale Einstellungen.**

Richtliniendefinition für eine bestimmte Richtlinie erfüllt, wird im System ein Ereignis generiert. Das Ereignis wird im System protokolliert und Benachrichtigungen werden gemäß den für die Richtlinien konfigurierten *Richtlinienaktionen* versendet.

Es gibt zwei Arten von Richtlinienereignissen:

- **Richtlinienbasierte Erkennung** – Löst Ereignisse aus, wenn die genauen Bedingungen der Richtlinie, wie durch eine Reihe von Ereignisdeskriptoren definiert, erfüllt sind.
- **Anomalie-Erkennung** – Löst Ereignisse aus, wenn anomale oder verdächtige Aktivitäten im Netzwerk identifiziert werden.

Das System verfügt über eine Reihe vordefinierter (sofort einsetzbarer) Richtlinien. Darüber hinaus bietet das System die Möglichkeit, die vordefinierten Richtlinien zu bearbeiten oder neue benutzerdefinierte Richtlinien zu definieren.

Richtlinienbasierte Erkennung

Für die richtlinienbasierte Erkennung konfigurieren Sie die spezifischen Bedingungen dafür, welche Ereignisse im System Ereignisbenachrichtigungen auslösen. Richtlinienbasierte Ereignisse werden nur ausgelöst, wenn die genauen Bedingungen der Richtlinie erfüllt sind. Dies stellt sicher, dass keine Fehlalarme auftreten, da das System bei tatsächlichen Ereignissen warnt, die im ICS-Netzwerk stattfinden, und gleichzeitig aussagekräftige detaillierte Informationen über das „Wer", „Was", „Wann", „Wo" und „Wie" liefert. Die Richtlinien können auf verschiedenen Ereignistypen und -deskriptoren basieren. Im Folgenden finden Sie einige Beispiele für mögliche Richtlinienkonfigurationen:

- **Anomale oder nicht autorisierte ICS-Steuerungsebenenaktivität (Engineering):** Beispielsweise sollte eine HMI die Firmwareversion eines Controllers nicht abfragen (kann auf Auskundschaftung hinweisen) und ein Controller sollte nicht während der Betriebszeiten programmiert werden (kann auf nicht autorisierte, potenziell böswillige Aktivität hinweisen).
- **Änderung am Code des Controllers:** Es wurde eine Änderung an der Controller-Logik festgestellt („Snapshot-Konflikt").
- **Anomale oder nicht autorisierte Netzwerkkommunikation:** Beispielsweise wurde ein unzulässiges Kommunikationsprotokoll zwischen zwei Netzwerk-Assets verwendet oder es fand eine Kommunikation zwischen zwei Assets statt, die noch nie zuvor kommuniziert haben.
- **Anomale oder nicht autorisierte Änderungen an der Asset-Inventarisierung:** Beispielsweise wurde ein neues Asset entdeckt oder ein Asset kommuniziert nicht mehr im Netzwerk.
- **Anomale oder nicht autorisierte Änderungen an Asset-Eigenschaften:** Beispielsweise hat sich die Asset-Firmware oder der Status geändert.
- **Abnormales Schreiben von Sollwerten:** Ereignisse werden für Änderungen an bestimmten Parametern generiert. Der Benutzer kann die zulässigen Bereiche für einen Parameter definieren und Ereignisse für Abweichungen von diesem Bereich generieren.

Anomalie-Erkennung

Richtlinien zur Anomalie-Erkennung erkennen verdächtiges Verhalten im Netzwerk basierend auf den integrierten Funktionen des Systems zur Erkennung von Abweichungen von „normalen" Aktivitäten. Die folgenden Richtlinien für die Anomalie-Erkennung sind verfügbar.

- **Abweichungen von einer Basislinie für den Netzwerkverkehr:** Der Benutzer definiert eine Basislinie für „normalen" Netzwerkverkehr basierend auf der Verkehrskarte während eines bestimmten Zeitraums und generiert Warnungen für Abweichungen von der Basislinie. Die Baseline kann jederzeit aktualisiert werden.
- **Spitze im Netzwerk-Traffic:** Es wird ein drastischer Anstieg des Netzwerk-Traffic-Volumens oder der Anzahl von Konversationen festgestellt.
- **Potenzielle Netzwerkaufklärungs-/Cyberangriffsaktivität:** Ereignisse werden für Aktivitäten generiert, die auf Aktivitäten in Zusammenhang mit Auskundschaftung oder Cyberangriffen im Netzwerk hinweisen, wie z. B. IP-Konflikte, TCP-Port-Scans und ARP-Scans.

Richtlinienkategorien

Die Richtlinien sind nach folgenden Kategorien geordnet:

  - **Richtlinien für Konfigurationsereignisse** – Diese Richtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Es gibt zwei Unterkategorien von Konfigurationsereignisrichtlinien:
  - **Controller-Validierung** – Diese Richtlinien beziehen sich auf Änderungen, die in den Controllern im Netzwerk stattfinden. Dabei kann es sich um Statusänderungen eines Controllers, aber auch um Änderungen an Firmware, Asset-Eigenschaften oder Codeblöcken handeln. Die Richtlinien können auf bestimmte Zeitpläne (z. B. Firmware-Upgrade während eines Arbeitstages) und/oder bestimmte Controller beschränkt werden.
  - **Controller-Aktivitäten** – Diese Richtlinien beziehen sich auf bestimmte Engineering-Befehle, die sich auf den Status und die Konfiguration von Controllern auswirken. Es ist möglich, bestimmte Aktivitäten zu definieren, die immer Ereignisse generieren, oder eine Reihe von Kriterien zum Generieren von Ereignissen festzulegen. Zum Beispiel, wenn bestimmte Aktivitäten zu bestimmten Zeiten und/oder auf bestimmten Controllern ausgeführt werden. Assets, Aktivitäten und Zeitpläne können sowohl auf Sperrlisten als auch auf Zulassungslisten gesetzt werden.

- **Richtlinien für Netzwerkereignisse** – Diese Richtlinien beziehen sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets. Dies schließt Assets ein, die dem Netzwerk hinzugefügt oder daraus entfernt wurden. Es enthält auch Traffic-Muster, die für das Netzwerk ungewöhnlich sind oder die als besonders besorgniserregend gekennzeichnet wurden. Wenn beispielsweise eine Engineering-Station mit einem Controller über ein Protokoll kommuniziert, das nicht Teil eines vorkonfigurierten Satzes von Protokollen ist (z. B. Protokolle, die von Controllern verwendet werden, die von einem bestimmten Anbieter hergestellt werden), wird ein Ereignis ausgelöst. Diese Richtlinien können auf bestimmte Zeitpläne und/oder bestimmte Assets beschränkt werden. Anbieterspezifische Protokolle werden der Einfachheit halber nach Anbieter organisiert, während jedes Protokoll in einer Richtliniendefinition verwendet werden kann.
- **SCADA-Ereignisrichtlinien** – Diese Richtlinien erkennen Änderungen der Sollwerte, die den industriellen Prozess beeinträchtigen können. Diese Änderungen können aus einem Cyberangriff oder menschlichem Fehlverhalten resultieren.
- **Netzwerkbedrohungsrichtlinien** – Diese Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert wurden.

Gruppen

Eine wesentliche Komponente bei der Definition von Richtlinien in Tenable.ot ist die Verwendung von *Gruppen*. Bei der Konfiguration einer Richtlinie wird jeder der Parameter durch eine Gruppe und nicht durch einzelne Entitäten bestimmt. Dadurch wird der Prozess für die Richtlinienkonfiguration erheblich optimiert.

Ereignisse

Wenn ein Ereignis eintritt, das die Bedingungen einer Richtlinie erfüllt, wird im System ein Ereignis generiert. Alle Ereignisse werden im Bildschirm „Ereignisse“ angezeigt und können auch über die entsprechenden Bildschirme „Inventar“ und „Richtlinie“ aufgerufen werden. Jedes Ereignis ist mit einem Schweregrad gekennzeichnet, der den Grad des Risikos angibt, das von dem Ereignis ausgeht. Benachrichtigungen können automatisch an E-Mail-Empfänger und SIEMs gesendet werden, wie in den Richtlinienaktionen der Richtlinie angegeben, die das Ereignis generiert hat.

Ein Ereignis kann von einem autorisierten Benutzer als gelöst markiert und mit einem Kommentar versehen werden.

TENABLE.OT-HARDWAREKOMPONENTEN

Tenable.ot Appliance

Frontblende

Komponente	Beschreibung
Betriebsanzeige	Zeigt an, ob die Tenable.ot Appliance ein- (grün) oder ausgeschaltet ist.
Konsolenanschluss	Nicht in Gebrauch
USB-Ports	Nicht in Gebrauch
Ethernet-Ports	Vier GbE-Ports werden wie folgt für die Verbindung mit Verwaltungs- und Betriebsnetzwerken verwendet: Port 1 – Standardmäßig wird dieser Port sowohl für die Verwaltung (UI) als auch als Port für aktive Abfragen (der mit den Netzwerk-Assets kommuniziert) verwendet. Diese Portkonfiguration kann (sowohl während der Einrichtung als auch später auf der Seite „Einstellungen“) so geändert werden, dass sie nur die Abfragen enthält. Dies geschieht, um die Verwaltungsschnittstelle vom Netzwerk der Controller zu trennen. Port 2 – Spiegelport: Wird als Ziel der Spiegelungssitzung (SPAN) verwendet. Dieser Port empfängt eine Kopie des Netzwerk-Traffic. Dieser Port hat keine IP-Adresse. Port 3 – Wenn die Option für Port-Trennung aktiviert ist, wird dieser Port nur für die Verwaltung (UI) verwendet und kann mit einem Netzwerk verbunden werden, das nicht Teil des Controller-Netzwerks ist. Port 4 – Reservierter Port, der von den Professional Services von Tenable.ot für Remote- oder lokalen Support verwendet wird.

Rückwand

Komponente	Beschreibung
Lüfter	Zwei Lüfter. Stellen Sie sicher, dass die Lüfter nicht blockiert sind.
Netzschalter	Ein-/Aus-Schalter. (Einige Sekunden lang gedrückt halten, um das Gerät auszuschalten.)
Stromversorgungsanschluss	AC-Netzanschluss; 100 – 240 VAC.

Packungsinhalt

Komponente	Beschreibung
Zwei Ethernet-Kabel	Zwei standardmäßige RJ45-Ethernet-Kabel. Verwenden Sie diese Kabel, um die Tenable.ot Appliance mit dem Netzwerk-Switch zu verbinden.
Stromversorgungsanschluss	AC-Netzanschluss; 100 – 240 VAC.
Montagehalterungen	2 x 1-HE-Rack-Montagehalterungen.

Tenable.ot Sensor

Rack-Montage-Sensor

Der Rack-Montage-Sensor wird eingestellt. Stattdessen bieten wir jetzt ein Adapterkit an, mit dem Sie das konfigurierbare Sensormodell an einer Rack-Halterung befestigen können.

Frontblende

Komponente	Beschreibung
Konsolenanschluss	Nicht in Gebrauch
USB-Ports	Nicht in Gebrauch
Ethernet-Ports	Vier 1-GbE-Ports werden wie folgt für die Verbindung mit Verwaltungs- und Betriebsnetzwerken verwendet: Port 1 – Verwaltungsport: Wird zur Verwaltung des Geräts verwendet. Port 2 – Spiegelport: Wird als Ziel der Spiegelungssitzung (SPAN) verwendet. Dieser Port empfängt eine Kopie des Netzwerk-Traffic. Dieser Port hat keine IP-Adresse. Port 3 – Nicht verwendet. Port 4 – Nicht verwendet.

Rückwand

Komponente	Beschreibung
Power-Taste	Stand-by-Modus in Rot; Einschaltmodus in Grün.
Reset-Taste	Startet das System neu, ohne es auszuschalten.
Netzschalter	Ein-/Aus-Schalter. (Einige Sekunden lang gedrückt halten, um das Gerät auszuschalten.)
Stromversorgungsanschluss	AC-Netzanschluss; 100 – 240 VAC.

Packungsinhalt

Komponente	Beschreibung
Ethernet-Kabel	Ein standardmäßiges RJ45-Ethernet-Kabel. Verwenden Sie dieses Kabel, um den Sensor mit dem Netzwerk-Switch zu verbinden.
Netzkabel	Ein landesübliches Standard-AC-Netzkabel.
Stromversorgung	60-W-AC-Netzadapter; 100 – 240 VAC.
Montagehalterungen	2 x L-förmige 1-HE-Rack-Montagehalterungen.
Schraubenpaket	

Konfigurierbarer Sensor

Dieses Modell kann entweder auf einer DIN-Schiene oder auf einem Montage-Rack (unter Verwendung des Adaptersatzes) montiert werden. In der Vergangenheit wurde dieses Modell als DIN-Schienensensor bezeichnet.

Frontblende

Komponente	Beschreibung
Betriebsanzeige	Zeigt an, ob der Sensor ein- (grün) oder ausgeschaltet ist.
Konsolenanschluss	Nicht in Gebrauch
USB-Ports	Nicht in Gebrauch

Komponente	Beschreibung
Ethernet-Ports	Fünf GbE-Ports werden wie folgt für die Verbindung mit Verwaltungs- und Betriebsnetzwerken verwendet: Port 1 – Verwaltungsport: Wird zur Verwaltung des Geräts verwendet. Port 2 – Nicht verwendet. Port 3 – Spiegelport: Wird als Ziel der Spiegelungssitzung (SPAN) verwendet. Dieser Port empfängt eine Kopie des Netzwerk-Traffic. Dieser Port hat keine IP-Adresse. Port 4 – Nicht verwendet. Port 5 – Nicht verwendet.

Packungsinhalt

Komponente	Beschreibung
Netzkabel	Ein landesübliches Standard-AC-Netzkabel.
Stromversorgung	60-W-AC-Netzadapter; 100 – 240 VAC.
Ethernet-Kabel	Ein standardmäßiges RJ45-Ethernet-Kabel. Verwenden Sie dieses Kabel, um den Sensor mit dem Netzwerk-Switch zu verbinden.
Montagelaschen	2 x L-förmige 1-HE-Rack-Montagehalterungen (Laschen).
Schraubenpaket	

ÜBERLEGUNGEN ZUR FIREWALL

Beim Einrichten Ihres Tenable.ot-Systems ist es wichtig festzulegen, welche Ports offen bleiben sollen, damit das Tenable-System ordnungsgemäß funktionieren kann. Die folgenden Tabellen geben an, welche Ports für die Verwendung mit der Tenable.ot Core-Plattform und Tenable.ot Sensoren offen gelassen werden sollten. Außerdem gibt es Tabellen mit den Ports, die für die Ausführung von aktiven Abfragen und für die Integration mit Tenable.io und Tenable.sc benötigt werden.

Tenable.ot Core-Plattform

Die folgenden Ports sollten für die Kommunikation mit der Tenable.ot Core-Plattform offen bleiben.

Flussrichtung	Port	Kommuniziert mit	Zweck
Eingehend	TCP 443	Weboberfläche für Tenable.ot	Browserzugriff auf Tenable.ot
Eingehend	TCP 8000	Weboberfläche für Tenable Core	Browserzugriff auf Tenable Core
Eingehend	TCP 22	Sensoren	Sensorkommunikation
Eingehend	TCP 22	Appliance für SSH-Zugriff	Befehlszeilenzugriff auf Betriebssystem oder Appliance
Ausgehend*	TCP 443	Tenable.sc	Sendet Daten zur Integration
Ausgehend*	TCP	cloud.tenable.com	Sendet Daten zur Integration
Ausgehend*	Verschiedene Industrieprotokolle	SPS/Steuerungen	Aktive Abfrage
Ausgehend*	TCP 25	E-Mail-Server für Warnmeldungen	SMTP (Warn-E-Mails, Berichte)
Ausgehend*	UDP 514	Syslog-Server	Syslog-Server
Ausgehend*	UDP 53	DNS-Server	Namensauflösung
Ausgehend*	UDP 123	NTP-Server	Zeitdienst
Ausgehend*	TCP 636	AD-Server	AD-LDAP-Authentifizierung
Ausgehend*	TCP 443	SAML-Anbieter	Single Sign-On (SSO)
Ausgehend*	UDP 161	SNMP-Server	SNMP-Überwachung an Tenable Core
Ausgehend*	TCP\443	*.tenable.com	Automatische Plugin-, Anwendungs- und Betriebssystem-Updates**

* Optionale Dienste

** Offline-Verfahren verfügbar

Tenable.ot Sensoren

Die folgenden Ports sollten für die Kommunikation mit Tenable.ot Sensoren offen bleiben.

Flussrichtung	Port	Kommuniziert mit	Zweck
Eingehend	TCP 8000	Weboberfläche	Browserzugriff auf Benutzer-GUI
Ausgehend	TCP 22	Tenable.ot Appliance	Sensorkommunikation
Eingehend	TCP 22	Appliance für SSH-Zugriff	Befehlszeilenzugriff auf Betriebssystem oder Appliance
Ausgehend*	TCP 25	E-Mail-Server für Warnmeldungen	SMTP (Warn-E-Mails, Berichte)
Ausgehend*	UDP 53	DNS-Server	Namensauflösung
Ausgehend*	UDP 123	NTP-Server	Zeitdienst
Ausgehend*	UDP 161	SNMP-Server	SNMP-Überwachung an Tenable Core

* Optionale Dienste

Aktive Abfrage

Die folgenden Ports sollten offen bleiben, um die Funktion für aktive Abfragen nutzen zu können.

Flussrichtung	Port	Kommuniziert mit	Zweck
Ausgehend	TCP 80	OT-Geräte	HTTP-Fingerprinting
Ausgehend	TCP 102	OT-Geräte	S7/S7+-Protokoll
Ausgehend	TCP 443	OT-Geräte	HTTPS-Fingerprinting
Ausgehend	TCP 445	OT-Geräte	WMI-Abfragen
Ausgehend	TCP 502	OT-Geräte	Modbus-Protokoll
Ausgehend	TCP 5432	OT-Geräte	PostgreSQL-Abfragen
Ausgehend	TCP 44818	OT-Geräte	CIP-Protokoll*
Ausgehend	TCP/UDP 53	OT-Geräte	DNS
Ausgehend	ICMP	OT-Geräte	Asset-Erfassung
Ausgehend	UDP 161	OT-Geräte	SNMP-Abfragen
Ausgehend	UDP 137	OT-Geräte	NBNS-Abfragen
Ausgehend	UDP 138	OT-Geräte	NetBIOS-Abfragen

* Wird ausschließlich für den Anbieter verwendet.

** Je nach Marke und Modell der Geräte können andere Ports und Protokolle erforderlich sein.

Tenable.ot-Integrationen

Die folgenden Ports sollten für die Kommunikation mit den Tenable.io- und Tenable.sc-Integrationen offen bleiben.

Flussrichtung	Port	Kommuniziert mit	Zweck
Ausgehend	TCP 443	cloud.tenable.com	Tenable.sc-Integration
Ausgehend	TCP 443	Tenable.sc	Tenable.io-Integration

INSTALLIEREN DER TENABLE.OT APPLIANCE

Schritt 1 – Einrichten der Tenable.ot Appliance

Die Tenable.ot Appliance kann entweder in einem Rack montiert oder einfach auf einer ebenen Oberfläche (z. B. einem Schreibtisch) aufgestellt werden.

Rack-Montage

➡ **So montieren Sie die Tenable.ot Appliance in einem Standard-Rack (19 Zoll):**

1. Setzen Sie die Servereinheit in einen freien 1-HE-Steckplatz im Rack ein.

Stellen Sie sicher, dass das Rack geerdet ist. Stellen Sie sicher, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

2. Sichern Sie das Gerät am Rack, indem Sie die Rack-Montage-Halterungen (mitgeliefert) am Rack-Rahmen befestigen. Verwenden Sie dabei geeignete Schrauben für die Rack-Montage (nicht mitgeliefert).
3. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss an der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Ebene Oberfläche

➡ **So installieren Sie die Tenable.ot Appliance auf einer ebenen Oberfläche:**

1. Stellen Sie die Geräteeinheit auf eine trockene, ebene Oberfläche (z. B. einen Schreibtisch).

Stellen Sie sicher, dass die Tischplatte eben und trocken ist.
Vergewissern Sie sich, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

2. Wenn das Gerät zusammen mit anderen Elektrogeräten aufgestellt wird, vergewissern Sie sich, dass hinter dem Lüfter (in der Rückwand) genügend Platz ist, um eine ausreichende Belüftung und Kühlung zu gewährleisten.
3. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss an der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Schritt 2 – Verbinden von Tenable.ot mit dem Netzwerk

Tenable.ot wird sowohl für die Netzwerküberwachung als auch für aktive Abfragen verwendet.

- **Um eine Netzwerküberwachung durchzuführen**, müssen Sie das Gerät an einen Spiegelport am Netzwerk-Switch anschließen, der mit den relevanten Controllern/SPS verbunden ist.
- **Um aktive Abfragen auszuführen**, müssen Sie das Gerät an einen regulären Port mit einer IP-Adresse am Netzwerk-Switch anschließen, der mit den relevanten Controllern/SPS verbunden ist.

Standardmäßig sind aktive Abfragen und die Verwaltungskonsole so konfiguriert, dass sie denselben Port am Gerät verwenden (Port 1). Nach der Ersteinrichtung ist es jedoch möglich, den Verwaltungsport vom Port für aktive Abfragen zu trennen, indem die Verwaltung an Port 3 konfiguriert wird. Nach dieser Konfiguration müssen Sie Port 3 am Gerät mit einem regulären Port am Switch verbinden, um die Verwaltung durchzuführen, wie in **Schritt 7 – Anschließen des separaten Verwaltungsports (für Option zur Port-Trennung)** beschrieben.

Für die Ersteinrichtung verbinden Sie Port 1 mit einem regulären Port am Netzwerk-Switch und Port 2 mit einem Spiegelport.

➡ So verbinden Sie die Tenable.ot Appliance mit dem Netzwerk:

1. Schließen Sie in der Tenable.ot Appliance das Ethernet-Kabel (mitgeliefert) an **Port 1** an.
2. Schließen Sie das Kabel an einen regulären Anschluss am Netzwerk-Switch an.
3. Schließen Sie am Gerät ein weiteres Ethernet-Kabel (mitgeliefert) an **Port 2** an.
4. Schließen Sie das Kabel an einen Spiegelport am Netzwerk-Switch an.

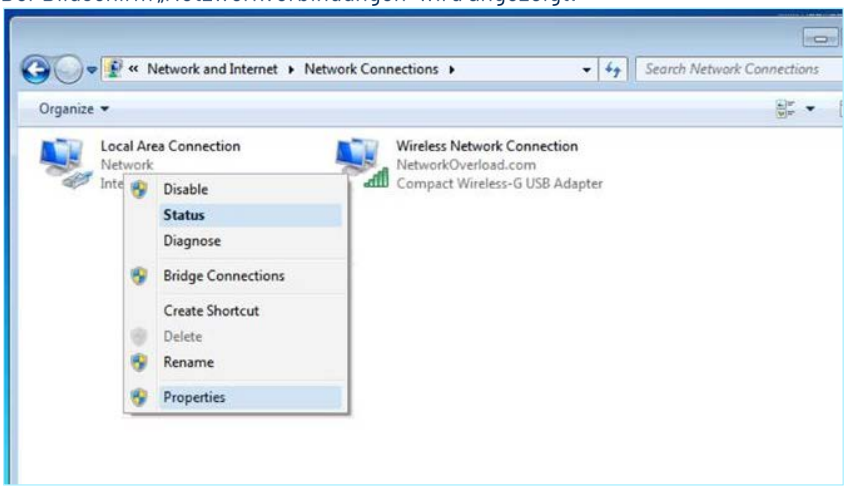
Schritt 3 – Einloggen bei der Verwaltungskonsole

➡ So loggen Sie sich bei der Verwaltungskonsole ein:

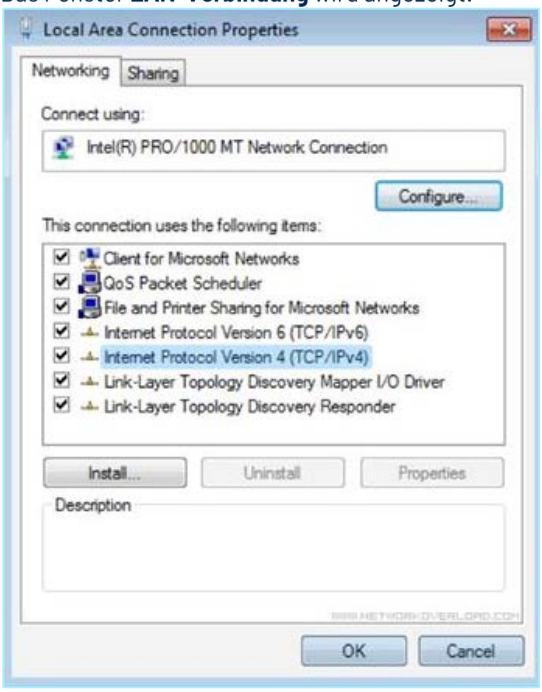
1. Führen Sie einen der folgenden Schritte aus:
   - Verbinden Sie die Workstation der Verwaltungskonsole (z. B. PC, Laptop usw.) über das Ethernet-Kabel direkt mit Port 1 der Tenable.ot Appliance ODER
   - Verbinden Sie die Workstation der Verwaltungskonsole mit dem Netzwerk-Switch.
2. Stellen Sie sicher, dass die Workstation der Verwaltungskonsole Teil desselben Subnetzes ist wie die Tenable.ot Appliance (d. h. 192.168.1.0/24) oder an das Gerät umgeleitet werden kann.
3. Verwenden Sie das folgende Verfahren, um eine statische IP-Adresse einzurichten (Sie müssen eine statische IP einrichten, um eine Verbindung zur Tenable.ot Appliance herzustellen):
   a. Gehen Sie zu **Netzwerk und Internet** > **Netzwerk- und Freigabecenter** > **Adaptereinstellungen ändern**.

Die Navigation kann bei den verschiedenen Windows-Versionen leicht variieren.

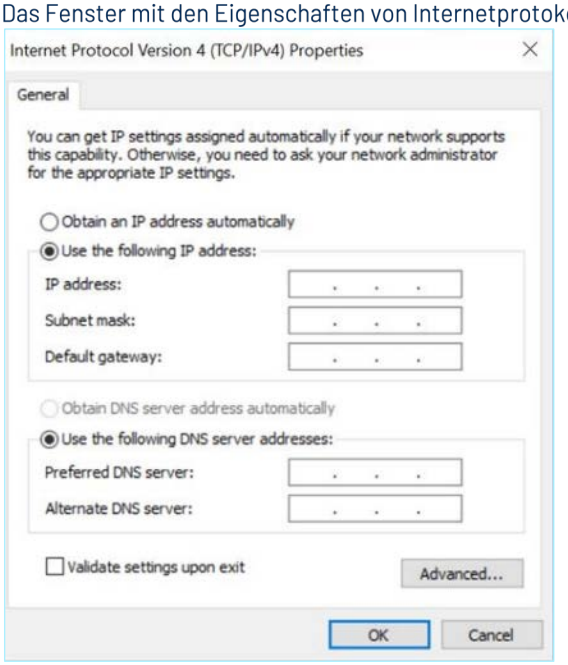
b. Der Bildschirm „Netzwerkverbindungen“ wird angezeigt.



c. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung** und wählen Sie **Eigenschaften**. Das Fenster **LAN-Verbindung** wird angezeigt.



d. Wählen Sie **Internetprotokoll, Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.
Das Fenster mit den Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) wird angezeigt.



e. Wählen Sie „Folgende IP-Adresse verwenden" aus.
f. Geben Sie im Feld „IP-Adresse" *192.168.1.10* ein.
g. Geben Sie im Feld „Subnetzmaske" *255.255.255.0* ein.
h. Klicken Sie auf **OK**.
Die neuen Einstellungen werden übernommen.

4. Navigieren Sie im Chrome-Webbrowser zu https://192.168.1.5.
Der Begrüßungsbildschirm des Setup-Assistenten wird geöffnet.

Auf die Benutzeroberfläche kann nur über einen Chrome-Browser zugegriffen werden. Zudem muss die neueste Version von Chrome verwendet werden.

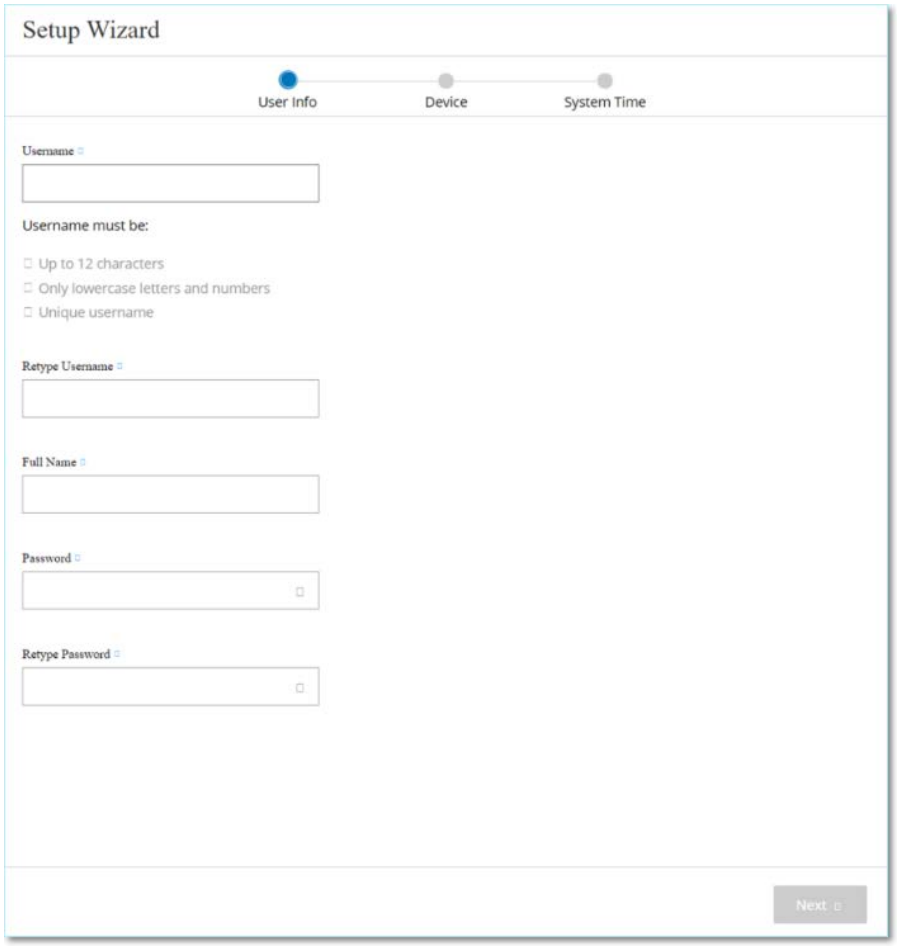
5. Klicken Sie auf **Setup-Assistenten starten**.
Der Setup-Assistent wird geöffnet und zeigt die Seite **Benutzerinformationen** an.

Schritt 4 – Setup-Assistent

Der Setup-Assistent von Tenable.ot führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

Wenn Sie die Konfiguration später ändern möchten, können Sie dies im Bildschirm **Einstellungen** in der Verwaltungskonsole (UI) tun.

Bildschirm 1 – Benutzerinformationen



➡ **Geben Sie auf der Seite „Benutzerinformationen“ Ihre Benutzerkontoinformationen wie folgt ein.**

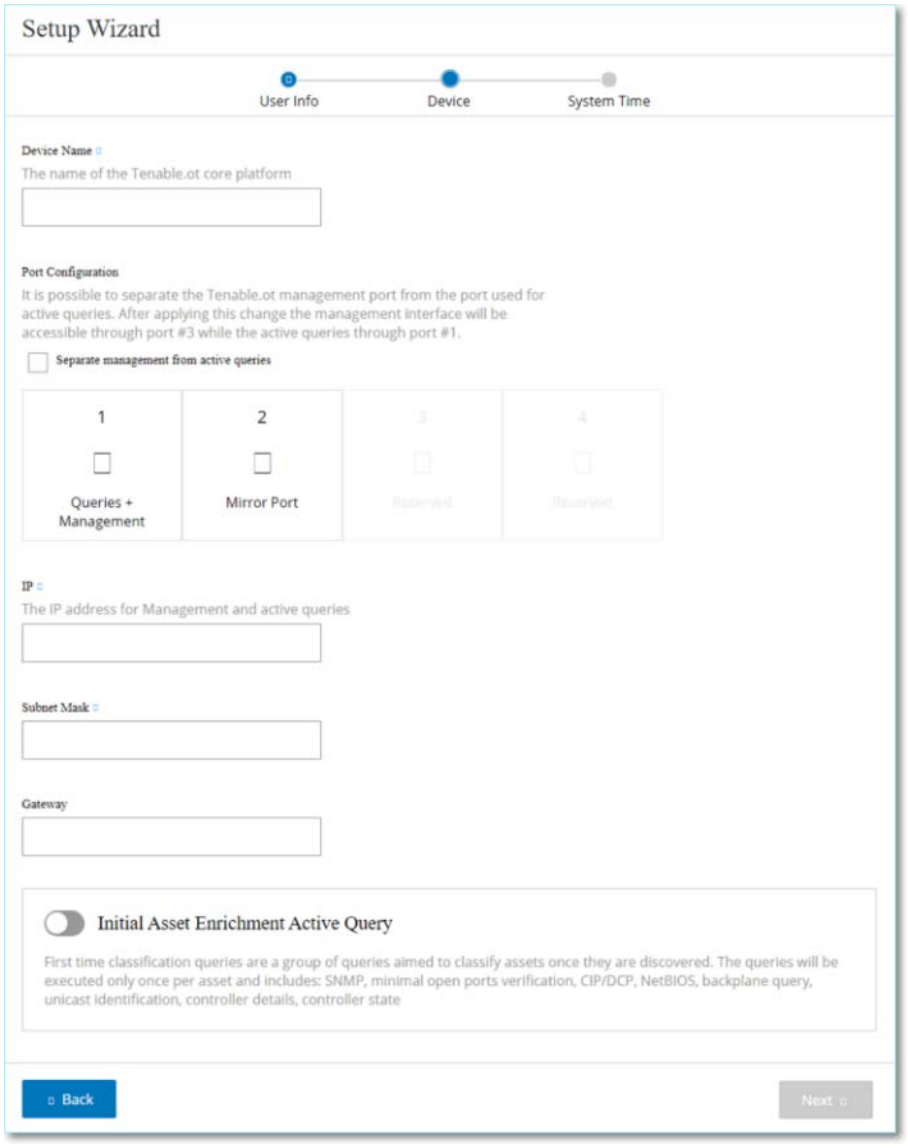
Im Setup-Assistenten konfigurieren Sie die Zugangsdaten für ein Administratorkonto. Nachdem Sie sich bei der Benutzeroberfläche eingeloggt haben, können Sie zusätzliche Benutzerkonten erstellen. Weitere Informationen zu Benutzerkonten finden Sie im Abschnitt **Benutzer und Rollen**.

1. Geben Sie im Feld **Benutzername** einen Benutzernamen ein, der für den Login beim System verwendet werden soll. Der Benutzername kann bis zu 12 Zeichen lang sein und darf nur Kleinbuchstaben und Zahlen enthalten.
2. Geben Sie im Feld **Benutzernamen erneut eingeben** den gleichen Benutzernamen erneut ein.
3. Geben Sie im Abschnitt **Vollständiger Name** Ihren vollständigen **Vor- und Nachnamen** ein.

Dies ist der Name, der in der Kopfleiste und in Protokollen Ihrer Aktivität im System angezeigt wird.

4. Geben Sie im Feld **Passwort** ein Passwort ein, das für das Einloggen beim System verwendet werden soll.
   Mindestanforderungen für Passwörter:
   - 12 Zeichen
   - Ein Großbuchstabe
   - Ein Kleinbuchstabe
   - Eine Zahl
   - Ein Sonderzeichen
5. Geben Sie im Feld **Passwort erneut eingeben** das gleiche Passwort erneut ein.
6. Klicken Sie auf **Weiter**.
   Die Seite **Gerät** des Setup-Assistenten wird geöffnet.

Bildschirm 2 – Gerät



➡ **Geben Sie auf der Seite „Gerät“ die Informationen zur Tenable.ot-Plattform wie folgt ein:**

1. Geben Sie im Feld **Gerätename** eine eindeutige Kennung für die Tenable.ot-Plattform ein.
2. Führen Sie im Abschnitt **Portkonfiguration** einen der folgenden Schritte aus:
   - **Port-Trennung** – Wenn Sie einen Port für die Verwaltung und einen separaten Port für Abfragen verwenden möchten, aktivieren Sie das Kontrollkästchen **Verwaltung von aktiven Abfragen trennen**. Wenn Sie diese Option auswählen, wird *Port 1* als Port *nur* für Abfragen und *Port 3* als Port *nur* für die Verwaltung konfiguriert.

Auf einigen Systemen ist die Option für die **Port-Trennung** möglicherweise nicht verfügbar. Wenden Sie sich an Ihren Support-Mitarbeiter, um Unterstützung zu erhalten.

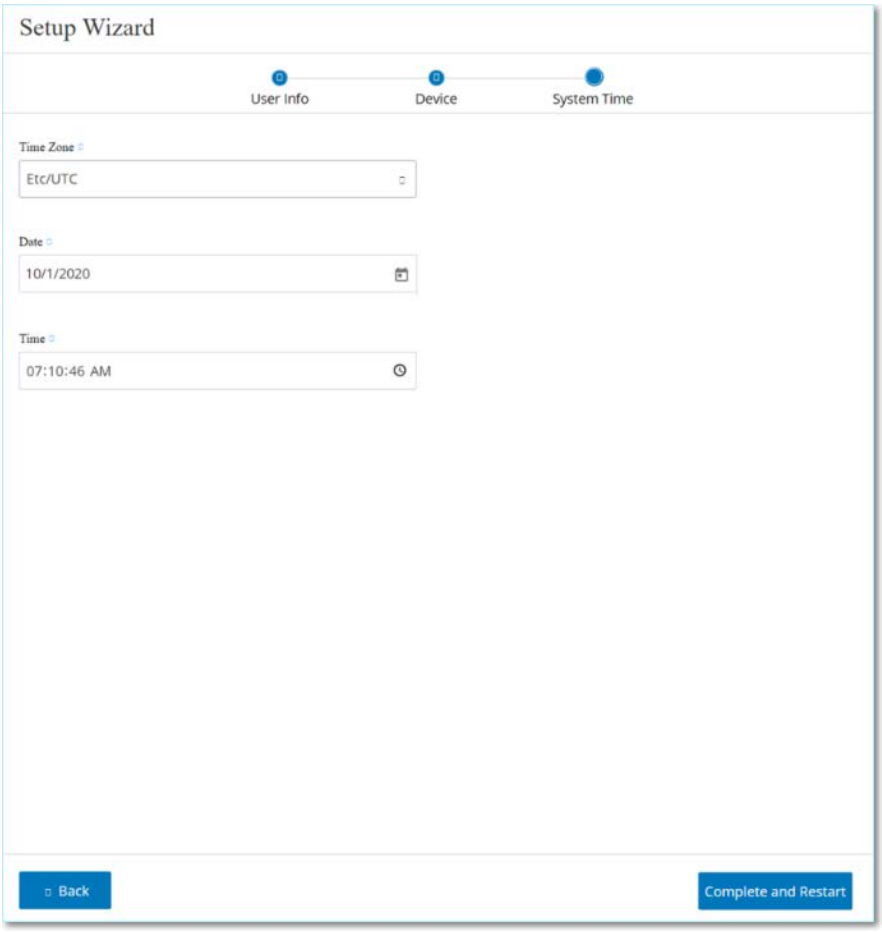
   - **Keine Trennung** – Wenn Sie für Abfragen und Verwaltung denselben Port verwenden möchten, aktivieren Sie nicht das Kontrollkästchen **Verwaltung von aktiven Abfragen trennen**. In diesem Fall können Sie die Anweisungen Nummer 3 bis 5 dieses Verfahrens überspringen und mit **Nummer 6** fortfahren.

3. Wenn Sie die Option für die **Port-Trennung** ausgewählt haben, geben Sie im Feld **IP für aktive Abfragen** die IP-Adresse des *Abfrageports* des Geräts ein. Dieser Port wird mit einem regulären Port im Netzwerk-Switch verbunden, der mit den Controllern kommunizieren kann (d. h. zu diesen umgeleitet werden kann). Und da Tenable.ot aktiv eine Verbindung zu den Controllern herstellt, benötigt es eine IP-Adresse innerhalb des Subnetzes des Netzwerks.
4. Wenn Sie die Option für die **Port-Trennung** ausgewählt haben, geben Sie im Feld **Die Subnetzmaske für aktive Abfragen** die Subnetzmaske des *Abfrageports* ein.
5. Wenn Sie die Option für die **Port-Trennung** ausgewählt haben, geben Sie im Feld **Das Gateway für aktive Abfragen** (optional) die IP-Adresse des Gateways im Betriebsnetzwerk ein.
6. Geben Sie im Feld **Management-IP** eine IP-Adresse (innerhalb des Netzwerk-Subnetzes) ein, die auf die Tenable.ot-Plattform angewendet werden soll. Diese wird zur IP-Adresse für die Verwaltung von Tenable.ot. (Sie ist auch die *Abfragen*-Adresse, wenn keine Trennung zwischen den Ports besteht.)
7. Geben Sie im Feld **Management Subnetzmaske** die Subnetzmaske des Netzwerks ein.
8. Wenn Sie ein Gateway einrichten möchten (optional), geben Sie die Gateway-IP für das Netzwerk in das Feld **Management-Gateway** ein.

Wenn Sie dieses Feld nicht ausfüllen, kann Tenable.ot nicht mit externen Komponenten außerhalb des Subnetzes (z. B. E-Mail-Server, Syslog-Server usw.) kommunizieren.

9. *Erste aktive Abfrage für Asset-Anreicherung* ist eine Reihe von Abfragen, die für jedes Asset ausgeführt werden, das im System erkannt wird. Dies hilft Tenable.ot bei der Klassifizierung der Assets. Wenn Sie diese Abfragen für jedes neu entdeckte Asset ausführen möchten, setzen Sie den Umschalter im unteren Feld auf **EIN**.
10. Klicken Sie auf **Weiter**.
    Die Seite **Systemzeit** des Setup-Assistenten wird geöffnet.

Bildschirm 3 – Systemzeit



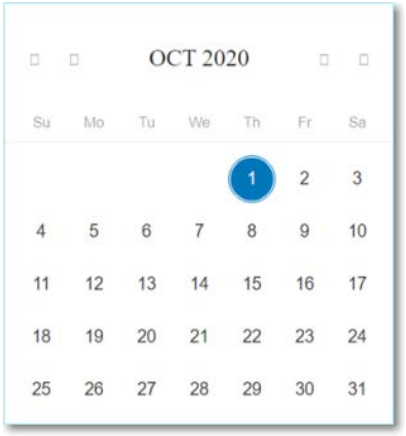
Auf der Seite **Systemzeit** werden die korrekte Uhrzeit und das Datum im Allgemeinen automatisch eingestellt.

Die Einstellung des richtigen Datums und der richtigen Uhrzeit ist für die genaue Aufzeichnung von Protokollen und Warnungen unerlässlich.

➡ **Wenn Datum und Uhrzeit nicht richtig eingestellt sind, geben Sie die Informationen wie folgt ein.**

1. Wählen Sie im Feld **Zeitzone** aus der Dropdown-Liste die lokale Zeitzone am Standort aus.

2. Klicken Sie im Feld **Datum** auf das Kalendersymbol .
   Ein Popup-Kalender wird angezeigt.



3. Wählen Sie das aktuelle Datum aus.
4. Wählen Sie im Feld **Uhrzeit** die Optionen **Stunden**, **Minuten** und **Sekunden AM/PM** aus und geben Sie die richtige Zahl entweder über die Tastatur oder die Aufwärts- und Abwärtspfeile ein.

> Wenn Sie eine der vorherigen Seiten des Setup-Assistenten bearbeiten möchten, klicken Sie auf „Zurück“. Nachdem Sie auf „Abschließen und neu starten“ geklickt haben, können Sie nicht mehr zum Setup-Assistenten zurückkehren. Sie können die Konfigurationseinstellungen jedoch auf der Seite „Einstellungen“ der Benutzeroberfläche ändern.

5. Um den Einrichtungsvorgang abzuschließen, klicken Sie auf **Abschließen und neu starten**.
   Sobald der Neustart abgeschlossen ist, werden Sie zum Bildschirm „Lizenzierung“ weitergeleitet.

Schritt 5 – Lizenzierung

Bevor Sie das System aktivieren können, müssen Sie Ihre Tenable.ot-Lizenz registrieren.

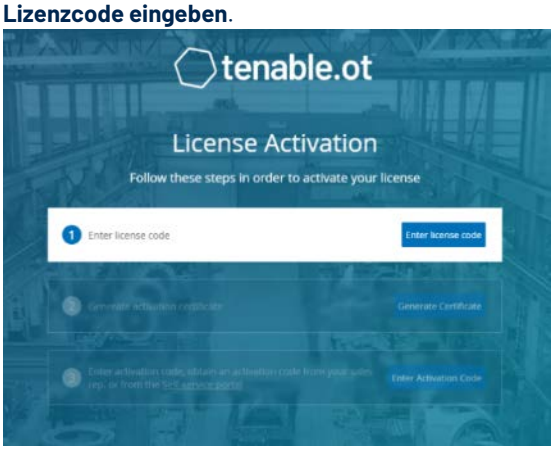
Voraussetzungen

- Der Lizenzcode (20 Buchstaben/Ziffern), den Sie von Tenable erhalten haben, als Sie Ihr Gerät bestellt haben.
- Sie benötigen Zugang zum Internet. Wenn Ihr Tenable.ot-Gerät nicht mit dem Internet verbunden ist, können Sie die Lizenz von jedem PC aus registrieren.

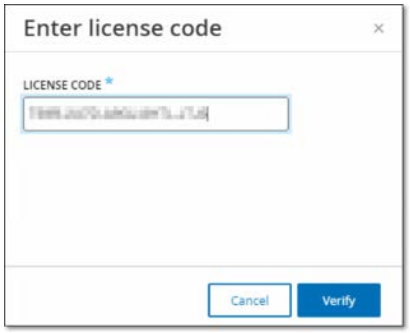
Aktivieren Ihrer Lizenz

➡ So aktivieren Sie Ihre Lizenz:

1. Klicken Sie im Bildschirm **Lizenzaktivierung** in Schritt 1, Feld **Lizenzcode eingeben**, auf die Schaltfläche **Lizenzcode eingeben**.



   Der Seitenbereich **Lizenzcode eingeben** wird auf der rechten Seite angezeigt.
2. Geben Sie im Feld **Lizenzcode** Ihren Lizenzcode ein und klicken Sie auf **Verifizieren**.

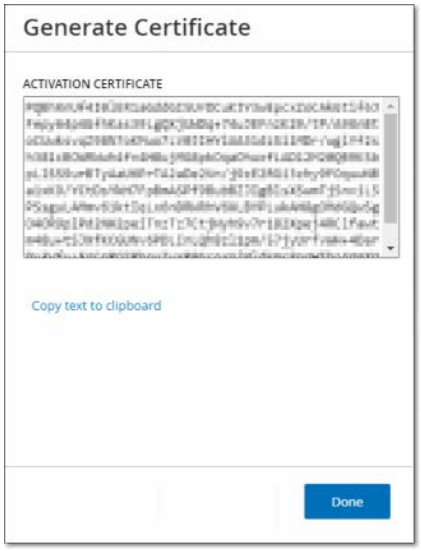


   Der Seitenbereich wird geschlossen.

3. Klicken Sie in Schritt 2, Feld **Aktivierungszertifikat generieren**, auf die Schaltfläche **Zertifikat generieren**.

Der Seitenbereich **Zertifikat generieren** wird mit dem Aktivierungszertifikat angezeigt.

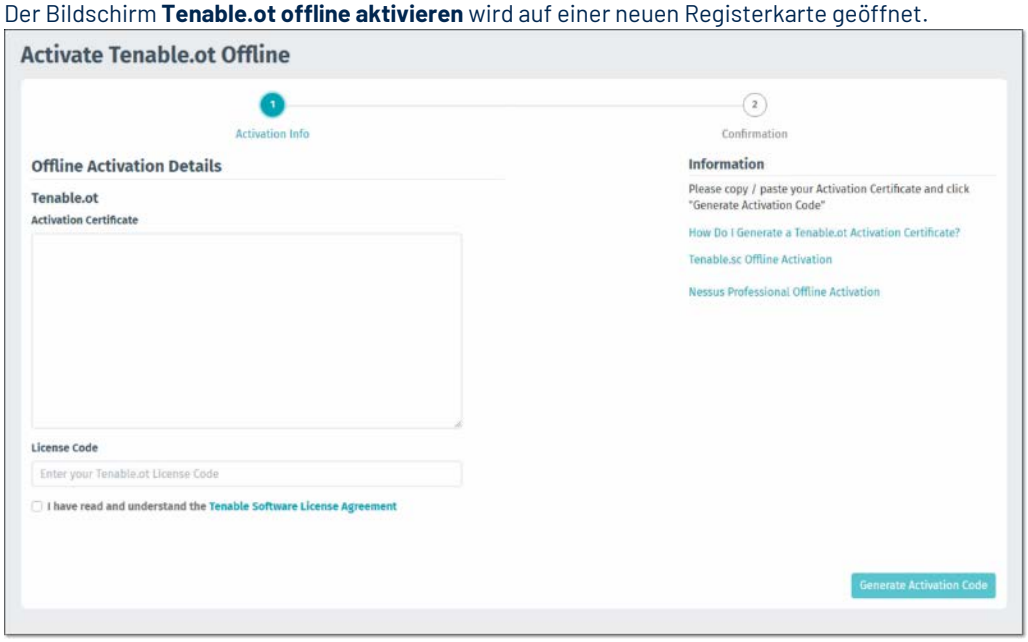
4. Klicken Sie auf die Schaltfläche **Text in die Zwischenablage kopieren** und dann auf **Fertig**.



Der Seitenbereich wird geschlossen.

5. Klicken Sie in Schritt 3, Feld **Aktivierungscode eingeben** auf den Link **Self-Service-Portal**.

Der Bildschirm **Tenable.ot offline aktivieren** wird auf einer neuen Registerkarte geöffnet.



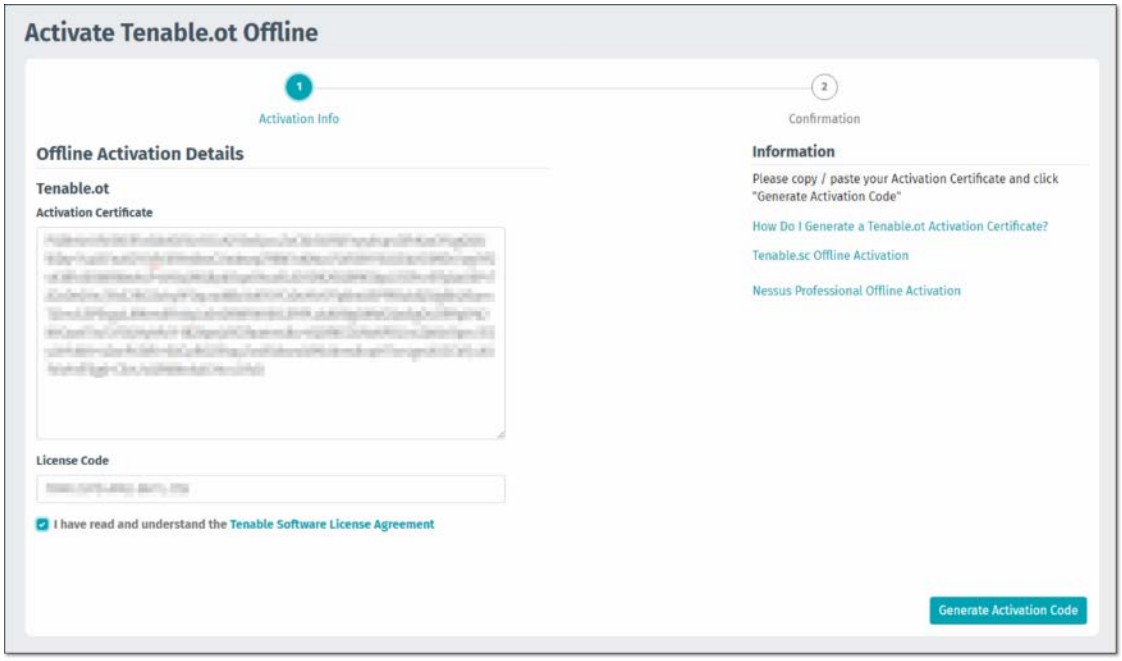
Wenn Ihr Tenable.ot-Gerät nicht mit dem Internet verbunden ist, müssen Sie den Bildschirm „Tenable.ot offline aktivieren“ von einem mit dem Internet verbundenen Gerät über die folgende URL aufrufen: https://provisioning.tenable.com/activate/offline/tenable-ot.

Wenn Sie derzeit nicht bei tenable.com eingeloggt sind, müssen Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort einloggen. Sie müssen das E-Mail-Konto verwenden, über das Sie Ihren Lizenzcode erhalten haben.

Wenn Sie keine Zugangsdaten haben, können Sie entweder auf **Passwort vergessen** klicken (und den Anweisungen folgen) oder sich an Ihren Tenable Account Manager wenden.

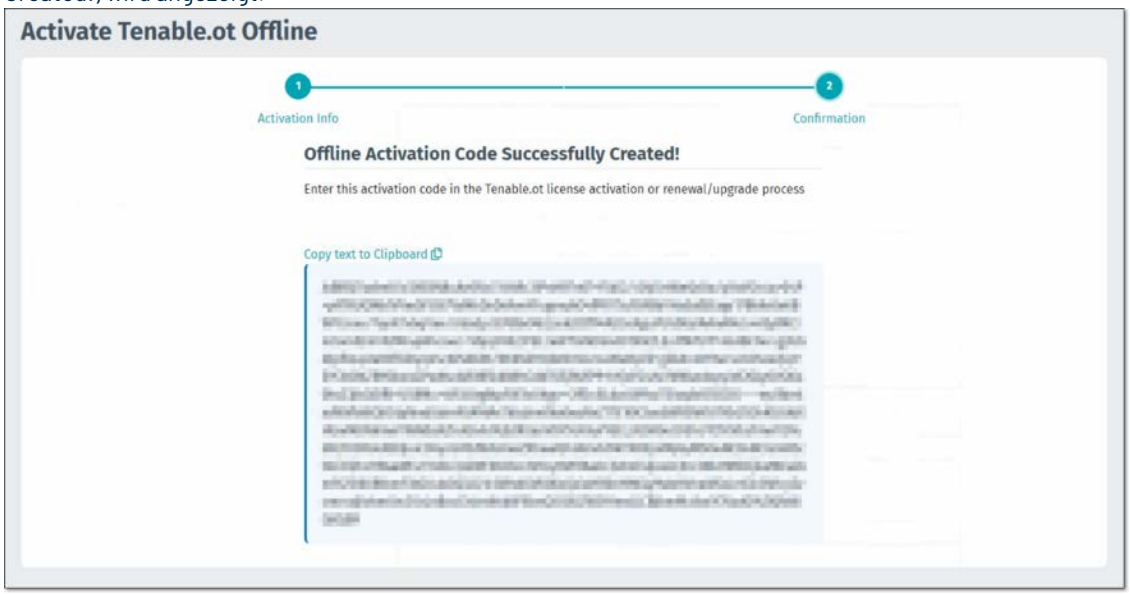
6. Geben Sie im Feld „Aktivierungszertifikat“ das Aktivierungszertifikat ein.
7. Geben Sie im Feld **Lizenzcode** denselben 20-stelligen **Lizenzcode** ein, den Sie in Schritt 2 dieses Verfahrens eingegeben haben.

8. Aktivieren Sie das Kontrollkästchen Ich habe die Tenable-Softwarelizenzvereinbarung gelesen und verstanden.



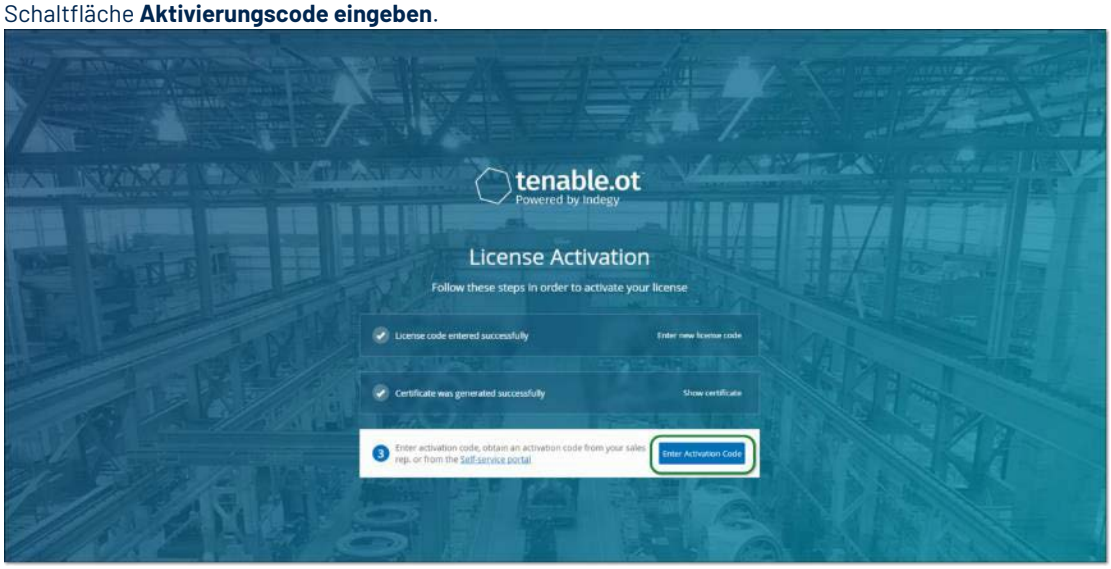
Um die Lizenzvereinbarung anzuzeigen, klicken Sie auf den Link **Tenable-Softwarelizenzvereinbarung**.

9. Klicken Sie auf die Schaltfläche „Aktivierungscode generieren“ (Generate Activation Code).
Der Bildschirm „Offline-Aktivierungscode erfolgreich erstellt!“ (Offline Activation Code Successfully Created!) wird angezeigt.



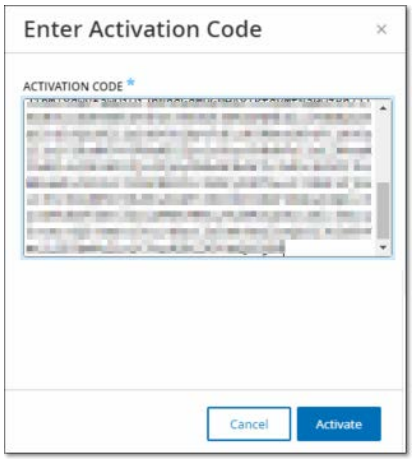
10. Klicken Sie auf „Text in die Zwischenablage kopieren“.

11. Navigieren Sie zurück zum Bildschirm **Lizenzaktivierung** auf Ihrem Tenable.ot-Gerät und klicken Sie auf die Schaltfläche **Aktivierungscode eingeben**.



Der Seitenbereich **Aktivierungscode eingeben** wird angezeigt.

12. Fügen Sie Ihren Aktivierungscode in das Feld **Aktivierungscode** ein und klicken Sie auf die Schaltfläche **Aktivieren**.



Der Seitenbereich wird geschlossen und der Startbildschirm von Tenable.ot wird angezeigt. Die Schaltfläche „Aktivieren“ wird angezeigt.

Informationen zum Aktualisieren Ihrer Lizenz finden Sie unter **AKTUALISIEREN DER LIZENZ**.

Schritt 6 – Aktivieren des Systems

Nach Abschluss der Lizenzaktivierung wird die Schaltfläche *Aktivieren* angezeigt.

Sie müssen das System aktivieren, um die Kernfunktionen des Systems zu aktivieren.

Die folgenden Funktionalitäten werden aktiviert, wenn das System aktiviert ist:

- Identifizieren von Assets im Netzwerk
- Erfassen und Überwachen des gesamten Netzwerkverkehrs
- Protokollieren von „Konversationen" im Netzwerk

Alle zusammengestellten Daten und Analysen aus den oben genannten Funktionalitäten können in der Verwaltungskonsole (UI) eingesehen werden.

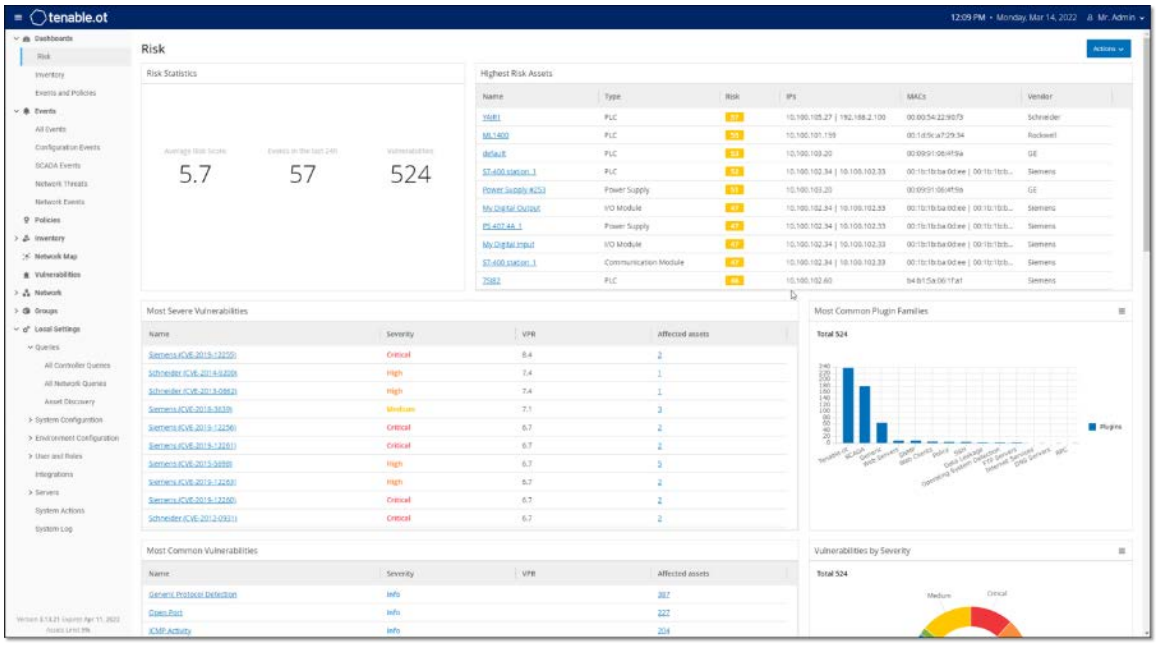
Dies sind laufende Prozesse, die sich über einen längeren Zeitraum erstrecken. Es wird einige Zeit dauern, bis die in der Benutzeroberfläche angezeigten Ergebnisse vollständig aktualisiert sind.

Zusätzliche Funktionen wie aktive Abfragen können im Bildschirm **Lokale Einstellungen** in der Verwaltungskonsole (UI) konfiguriert und aktiviert werden, siehe

Abfragen.

So aktivieren Sie das System:

1. Klicken Sie auf die Schaltfläche **Aktivieren**.
   Das System ist aktiviert. Die Benutzeroberfläche wird geöffnet und zeigt den Bildschirm **Dashboard** > **Risiko** an.



Es dauert einige Minuten, bis das System Ihre Assets identifiziert hat. Möglicherweise müssen Sie die Seite aktualisieren, damit die Daten angezeigt werden.

Schritt 7 – Anschließen des separaten Verwaltungsports (für Option zur Port-Trennung)

Wenn Sie die Option zur Port-Trennung ausgewählt haben (um **Abfragen** von der Verwaltung zu trennen), müssen Sie Port 3 in der Tenable.ot Appliance, der jetzt der Verwaltungsport ist, mit einem Port in einem Netzwerk-Switch verbinden. Dies kann ein anderer Netzwerk-Switch sein, beispielsweise ein Netzwerk-Switch des IT-Netzwerks.

So verbinden Sie den Verwaltungsport:

1. Schließen Sie in der Tenable.ot Appliance ein Ethernet-Kabel (mitgeliefert) an Port 3 an.
2. Schließen Sie das Kabel an einen Port an einem Netzwerk-Switch an.

INSTALLIEREN EINES TENABLE.OT SENSORS

Koppeln von Sensoren mit dem ICP

Der folgende Abschnitt beschreibt das Verfahren zur Konfiguration eines Sensors ab Version 3.14. Verwenden Sie zum Konfigurieren eines Sensors eines früheren Modells das in **Anhang 1 – Installieren eines Sensors (Version 3.13 und niedriger)** beschriebene Verfahren.

Das Koppeln von Sensoren mit dem ICP erfolgt sowohl über die ICP-Verwaltungskonsole als auch über die Tenable Core-Benutzeroberfläche des Sensors.

Sie können die automatische Genehmigung eingehender Kopplungsanfragen aktivieren oder die automatische Genehmigung deaktivieren, um eine manuelle Genehmigung für jede neue Kopplungsanfrage des Sensors zu verlangen.

Voraussetzungen

- Die Sensorhardware ist ordnungsgemäß installiert (siehe **Schritt 1 – Einrichten des Sensors**).
- Der Sensor ist mit Ihrem Netzwerk-Switch verbunden (siehe **Schritt 2 – Verbinden des Sensors mit dem Netzwerk**).
- Der Sensor hat seine eigene statische IPv4-Adresse (siehe **Schritt 3 – Aufrufen des Sensor-Setup-Assistenten**).
- Der Sensor ist mit der Tenable Core-Plattform verbunden und Sie haben einen Benutzernamen und ein Passwort zum Einloggen bei der Core-Benutzeroberfläche. Weitere Informationen zur Verwendung der Tenable Core-Benutzeroberfläche finden Sie unter https://docs.tenable.com/tenablecore/Tenableot/Content/TenableCore/Introduction_OT.htm.
- Überprüfen Sie, ob Sie ein gültiges Zertifikat in der ICP-Konsole haben (siehe **Zertifikat**).
- Es wird empfohlen, einen dedizierten ICP-Benutzer mit Administratorrolle für das Koppeln von Sensoren zu erstellen, um Verbindungsunterbrechungen zu vermeiden (siehe **Hinzufügen lokaler Benutzer**). Ein neuer Admin-Benutzer kann verwendet werden, um mehrere Sensoren zu koppeln.

Koppeln des Sensors

So koppeln Sie einen Sensor v.3.14 oder höher mit dem ICP:

1. Navigieren Sie in der ICP-Verwaltungskonsole (UI) zum Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Sensoren**.

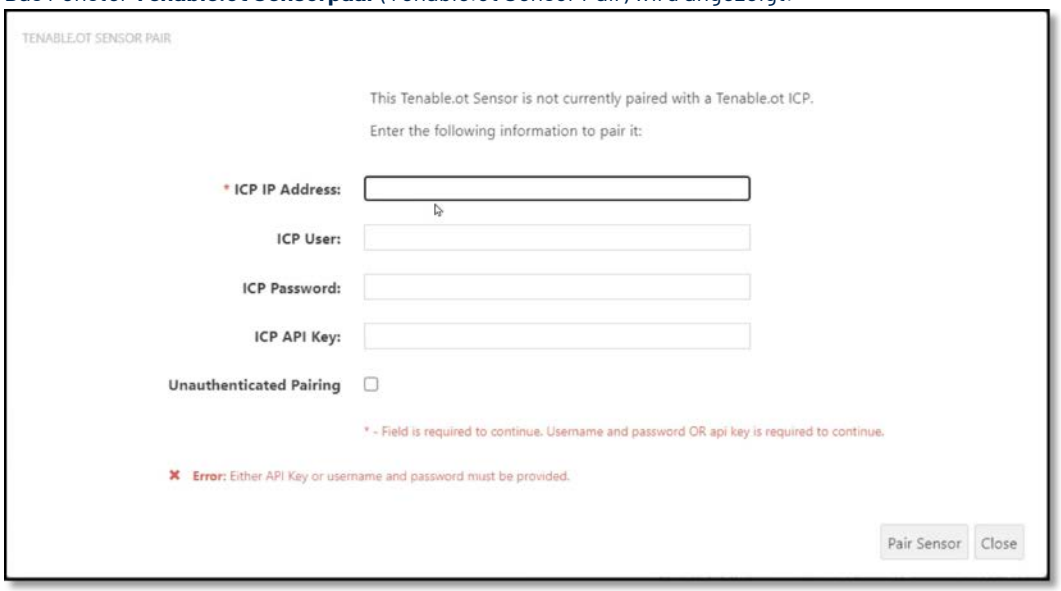
2. Wenn Sie die automatische Genehmigung der Sensorkopplung aktivieren möchten, stellen Sie sicher, dass der Umschalter **Sensorkopplungsanforderungen automatisch genehmigen** oben im Bildschirm auf **EIN** gesetzt ist. Ist diese Option nicht ausgewählt, müssen alle Kopplungsanfragen manuell genehmigt werden.
3. Lassen Sie die ICP-Registerkarte geöffnet und öffnen Sie eine neue Registerkarte. Greifen Sie durch Eingabe von **<Sensor-IP>:8000** auf die Tenable Core-Benutzeroberfläche des Sensors zu.

Auf die Benutzeroberfläche kann nur über einen Chrome-Browser zugegriffen werden. Zudem muss die neueste Version von Chrome verwendet werden.

4. Geben Sie im Login-Fenster der Tenable Core-Konsole Ihre Daten unter **Benutzername** und **Passwort** ein, aktivieren Sie das Kontrollkästchen **Mein Passwort für privilegierte Aufgaben wiederverwenden** (Reuse my password for privileged tasks) und klicken Sie auf **Einloggen** (Log In).

Wenn das Kontrollkästchen **Mein Passwort für privilegierte Aufgaben wiederverwenden** (Reuse my password for privileged tasks) beim Login nicht aktiviert ist, kann der Benutzer den Sensor-Dienst nicht neu starten.

5. Klicken Sie in der Navigationsmenüleiste auf **Tenable.ot Sensor**.
Das Fenster **Tenable.ot Sensorpaar** (Tenable.ot Sensor Pair) wird angezeigt.



Das Fenster **Tenable.ot Sensorpaar** (Tenable.ot Sensor Pair) wird nur beim ersten Laden der Seite angezeigt. Um das Fenster danach zu öffnen, klicken Sie auf die Schaltfläche im Abschnitt **Kopplungsinfo** (Pairing Info) der **Tenable Core**-Konsole.

6. Geben Sie im Feld **ICP-IP-Adresse** (ICP IP Address) die IPv4-Adresse des ICP ein, mit dem Sie diesen Sensor koppeln möchten.
7. Wenn Sie eine nicht authentifizierte (unverschlüsselte) Kopplung verwenden möchten, aktivieren Sie das Kontrollkästchen **Nicht authentifizierte Kopplung** (Unauthenticated Pairing) und fahren Sie mit Schritt 8 fort.

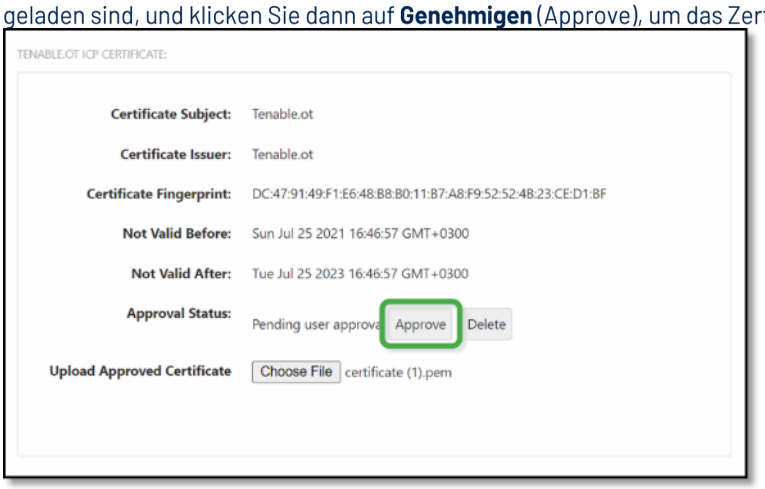
> Sensoren, die nicht authentifizierte Kopplung verwenden, können ihre Netzwerksegmente nur passiv scannen und können nicht vom ICP verwaltet werden, um aktive Abfragen zu senden.

8. Führen Sie einen der folgenden Schritte aus, um die Kopplung zu authentifizieren:
   - Geben Sie den ICP-Benutzernamen in das Feld **ICP-Benutzer** (ICP User) und das ICP-Passwort in das Feld **ICP-Passwort** (ICP Password) ein, ODER
   - Geben Sie im Feld **ICP-API-Schlüssel** (ICP API Key) einen API-Schlüssel für das ICP ein.

> Es wird empfohlen, einen dedizierten ICP-Benutzer für das Koppeln von Sensoren zu erstellen, um Konnektivität während des Koppelns sicherzustellen (siehe **Hinzufügen lokaler Benutzer**).

> Die Methode der Authentifizierung über Benutzername und Passwort hat den Vorteil, dass die Zugangsdaten nicht ablaufen, was bei einem API-Schlüssel der Fall ist.

9. Klicken Sie auf **Sensor koppeln** (Pair Sensor).
10. Wenn Sie ein vom ICP angebotenes Zertifikat nutzen möchten:
    a. Warten Sie in der **Tenable Core**-Konsole im Abschnitt **Tenable-ICP-Zertifikat** (Tenable ICP Certificate) unter **Genehmigungsstatus** (Approval Status), bis die Zertifikatsinformationen geladen sind, und klicken Sie dann auf **Genehmigen** (Approve), um das Zertifikat zu genehmigen.

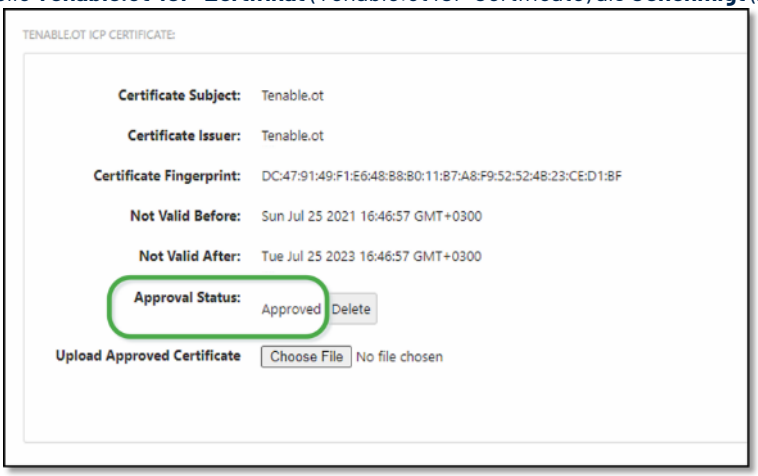


    b. Klicken Sie im Popup-Fenster **Akzeptieren des Tenable.ot-Serverzertifikats bestätigen** (Confirm Accept Tenable.ot Server Certificate) auf **Accept This Certificate** (Dieses Zertifikat akzeptieren).

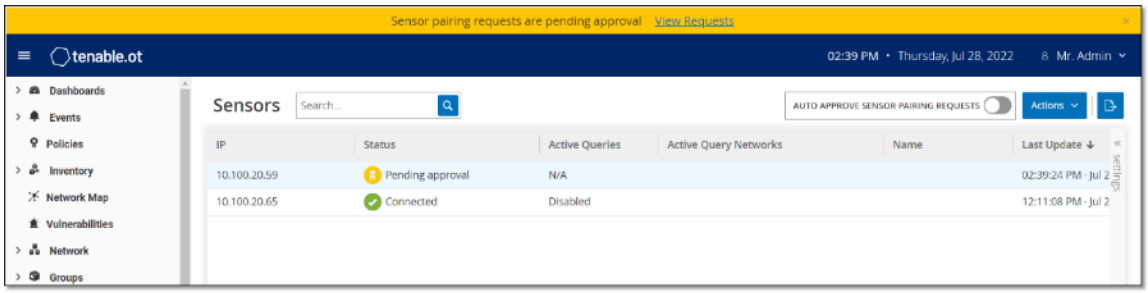
    Wenn Sie es vorziehen, ein Zertifikat manuell hochzuladen:

    a. Befolgen Sie in der **Tenable ICP**-Konsole das unter **Generieren eines HTTPS-Zertifikats** beschriebene Verfahren.
    b. Klicken Sie in der **Tenable Core**-Konsole im Abschnitt **Tenable-ICP-Zertifikat** (Tenable ICP Certificate) unter **Genehmigtes Zertifikat hochladen** (Upload Approved Certificate) auf **Datei auswählen** (Choose File).
    c. Navigieren Sie zur hochzuladenden .pem-Zertifikatsdatei.

Sobald ein gültiges Zertifikat akzeptiert wurde, wird sein **Genehmigungsstatus** (Approval Status) in der Tabelle **Tenable.ot-ICP-Zertifikat** (Tenable.ot ICP Certificate) als **Genehmigt** (Approved) angezeigt.

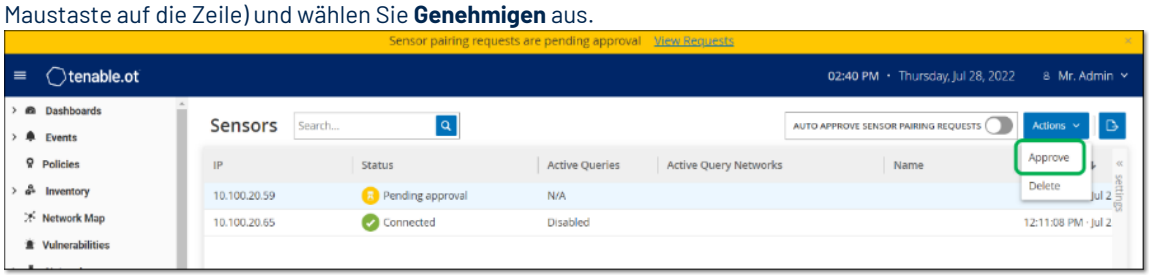


11. Kehren Sie in der ICP-Benutzeroberfläche zum Bildschirm **Lokale Einstellungen > Systemkonfiguration > Sensoren** zurück.



Der neue Sensor wird in der Tabelle angezeigt, der Status sollte *Genehmigung ausstehend* lauten.

12. Klicken Sie auf die Zeile des Sensors, dann auf die Schaltfläche **Aktionen** (oder klicken Sie mit der rechten Maustaste auf die Zeile) und wählen Sie **Genehmigen** aus.



13. Der Status sollte zu *Verbunden* wechseln und anzeigen, dass die Kopplung erfolgreich war. Andere mögliche Status sind:
    - *Verbunden (nicht authentifiziert)* – Der Sensor ist im nicht authentifizierten Modus verbunden. Der Sensor kann nur eine passive Netzwerkerkennung durchführen.
    - *Angehalten* – Der Sensor ist ordnungsgemäß verbunden, wurde jedoch angehalten.
    - *Getrennt* – Der Sensor ist nicht verbunden. Bei einem authentifizierten Sensor kann dies auf einen Fehler bei der Kopplung zurückzuführen sein (z. B. Tunnelfehler, API-Problem).

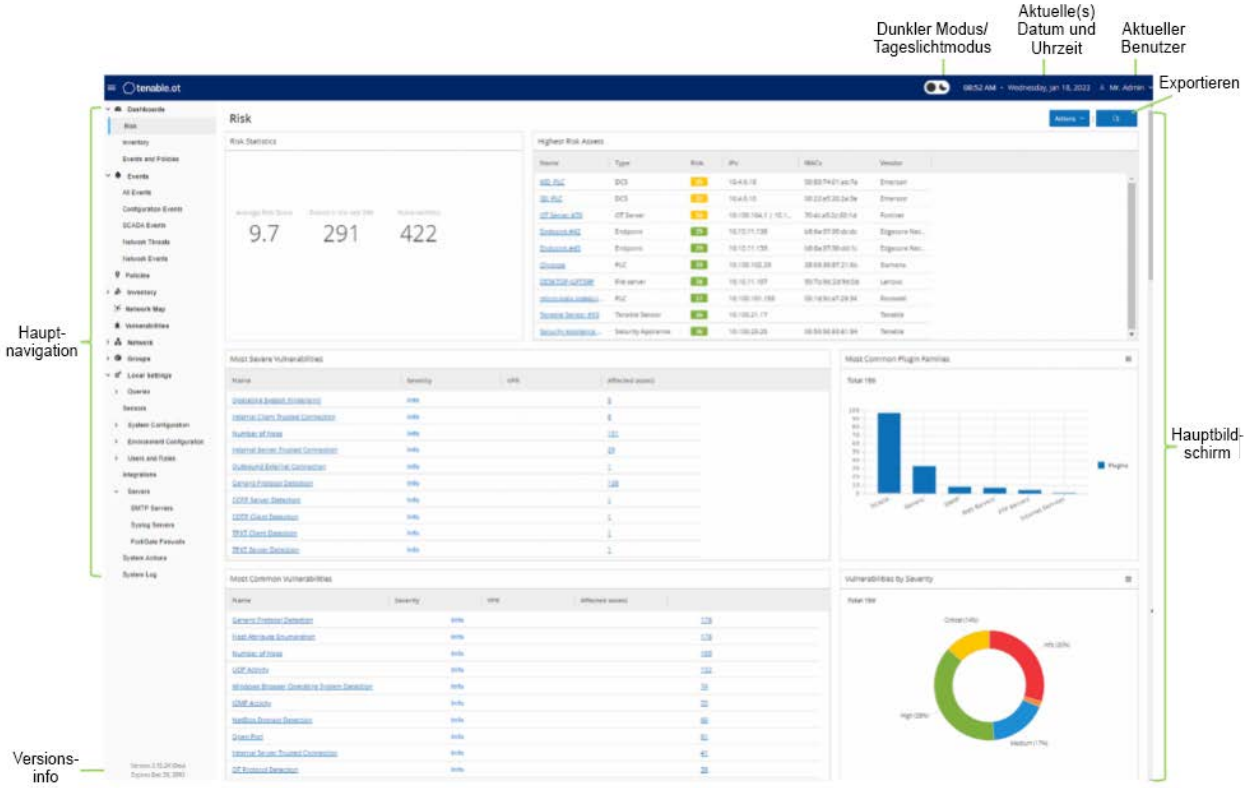
14. Sobald die Kopplung für einen authentifizierten Sensor abgeschlossen ist, können Sie aktive Abfragen so konfigurieren, dass sie auf diesem Sensor ausgeführt werden. Siehe **Konfigurieren aktiver Abfragen**.

Sobald die Kopplung abgeschlossen ist, wird empfohlen, den Sensor nur noch über die ICP-Seite zu verwalten und nicht mehr über die Tenable Core-Benutzeroberfläche.

BEDIENELEMENTE DER VERWALTUNGSKONSOLE

Die Benutzeroberfläche der Verwaltungskonsole bietet einfachen Zugriff auf wichtige Daten, die von Tenable.ot in Bezug auf Asset-Management, Netzwerkaktivität und Sicherheitsereignisse entdeckt wurden. Sie können die Benutzeroberfläche verwenden, um die Funktionen der Tenable.ot-Plattform Ihren Anforderungen entsprechend zu konfigurieren. Dieses Kapitel gibt einen kurzen Überblick über die Elemente der Benutzeroberfläche. Einzelheiten zu bestimmten Benutzeroberflächenfunktionen finden Sie in den folgenden Kapiteln.

Hauptelemente der Benutzeroberfläche



Die folgende Tabelle beschreibt die Hauptelemente der Benutzeroberfläche, die immer angezeigt werden.

Benutzeroberflächenelement	Beschreibung
Hauptnavigation	Hauptnavigationsmenü. Klicken Sie auf das Symbol, um das Navigationsmenü anzuzeigen/auszublenden.
Aktuelle(s) Datum und Uhrzeit	Zeigt das aktuelle Datum und die Uhrzeit an, wie sie im System registriert sind.
Aktueller Benutzername	Zeigt den Namen des Benutzers an, der derzeit beim System eingeloggt ist. Klicken Sie auf den Abwärtspfeil, um ein Auswahlmenü anzuzeigen. Menüoptionen sind „Info“ oder „Ausloggen“.
Lizenzinformationen	Zeigt die Softwareversion von Tenable.ot und das Ablaufdatum der Lizenz an.

Benutzeroberflächenelement	Beschreibung
Hauptbildschirm	Zeigt den Bildschirm an, der in der Hauptnavigation ausgewählt wurde.
Dunkler Modus/Tageslichtmodus	Ändert das Farbschema der Anzeige in den dunklen Modus oder den Tageslichtmodus.
Exportieren	Lädt eine PDF-Datei des Dashboards herunter.

Aktivieren/Deaktivieren des dunklen Modus

Der Benutzer kann das Farbschema des dunklen Modus in allen Bildschirmen verwenden, indem er den Schalter für den dunklen Modus umschaltet.

So aktivieren/deaktivieren Sie den dunklen Modus:

1. Klicken Sie oben im Bildschirm auf die Schaltfläche **Dunkler Modus**  , um den dunklen Modus zu aktivieren.

   Die Einstellung wird auf alle Bildschirme angewendet und die Schaltfläche **Tageslichtmodus**  wird angezeigt.
2. Um die Einstellung des Tageslichtmodus wiederherzustellen, klicken Sie auf die Schaltfläche **Tageslichtmodus**.

Überprüfen der aktuellen Softwareversion

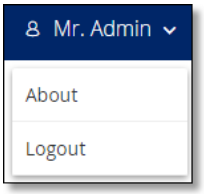
Der Benutzer kann die Version seiner Software über die Schaltfläche „Benutzername“ in der oberen rechten Ecke der Kopfleiste überprüfen.

So zeigen Sie die aktuelle Softwareversion an:

1. Klicken Sie in der Hauptkopfleiste auf die Schaltfläche „Benutzername“ in der oberen rechten Ecke, um das Menü zu öffnen.

   Das Menü „Benutzer“ wird angezeigt.

2. Klicken Sie im Menü auf **Info**.
   Die aktuelle Softwareversion wird angezeigt.

Hauptbildschirme

Die Benutzeroberfläche verfügt über mehrere Hauptbildschirme, auf die über die **Hauptnavigation** zugegriffen werden kann. Im Folgenden finden Sie eine kurze Beschreibung der verschiedenen Bildschirme. Jede wird in den folgenden Kapiteln ausführlicher erklärt.

- **Dashboards** – Hier können Sie Widgets anzeigen, die Diagramme und Tabellen enthalten, die einen Überblick über das Inventar und die Sicherheitslage Ihres Netzwerks geben. Es gibt separate Dashboards für *Risiko*, *Inventar* sowie *Ereignisse und Richtlinien*. Siehe Kapitel **Dashboards**.
- **Ereignisse** – Zeigt alle Ereignisse an, die als Folge von Richtlinientreffern im System aufgetreten sind. Es gibt einen Bildschirm zum Anzeigen *aller Ereignisse* sowie separate Bildschirme zum Anzeigen von Ereignissen jedes spezifischen Typs (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse). Siehe Kapitel **Ereignisse**.
- **Richtlinien** – Hier können Sie Richtlinien im System anzeigen, bearbeiten und aktivieren. Siehe Kapitel **Richtlinien**.
- **Inventar** – Zeigt ein Inventar aller erfassten Assets an und ermöglicht so ein umfassendes Asset-Management, die Überwachung des Status jedes Assets und die Anzeige der zugehörigen Ereignisse. Es gibt einen Bildschirm zur Anzeige *aller* Assets sowie separate Bildschirme zur Anzeige bestimmter Asset-Typen (*Controller und Module*, *Netzwerk-Assets* und *IoT*). Siehe Kapitel **Inventar**.
- **Netzwerkübersicht** – Zeigt eine visuelle Darstellung der Netzwerk-Assets und ihrer Verbindungen an.
- **Schwachstellen** – Zeigt eine detaillierte Liste aller Bedrohungen im Netzwerk an, die von Tenable.ot-Plug-ins erkannt wurden, und bietet empfohlene Behebungsmaßnahmen. Dieser Abschnitt enthält CVEs sowie andere Bedrohungen für Assets in Ihrem Netzwerk (z. B. veraltete Betriebssysteme, Verwendung anfälliger Protokolle, anfällige offene Ports usw.).

- **Netzwerk** – Bietet eine umfassenden Überblick über den Netzwerk-Traffic, indem Daten zu Konversationen angezeigt werden, die im Laufe der Zeit zwischen Assets im Netzwerk stattgefunden haben.
  Siehe Kapitel **Netzwerk.**
  Die Informationen werden auf drei separaten Bildschirmen angezeigt:
  - **Netzwerk – Zusammenfassung** – Zeigt eine Übersicht über den Netzwerk-Traffic
  - **Paketerfassungen** – Zeigt die Erfassung vollständiger Pakete des Netzwerk-Traffic
  - **Konversationen** – Zeigt eine Liste aller im Netzwerk erkannten Konversationen mit Details über den Zeitpunkt, an dem sie stattgefunden haben, beteiligte Assets usw.
- **Gruppen** – Hier können Sie Gruppen, die in der Richtlinienkonfiguration verwendet werden, anzeigen, erstellen und bearbeiten. Siehe Kapitel **Gruppen**.
- **Lokale Einstellungen** – Ermöglicht das Anzeigen und Konfigurieren der Systemeinstellungen. Siehe Kapitel **Lokale Einstellungen**.

Arbeiten mit Listen

Die verschiedenen Bildschirme von Tenable.ot zeigen die für den jeweiligen Bildschirm relevanten Daten im Tabellenformat mit einer Liste für jedes Element an. Diese Tabellen verfügen über standardisierte Anpassungsfunktionen, die dem Benutzer einen einfachen Zugriff auf die relevanten Informationen ermöglichen. In den folgenden Abschnitten werden die Anpassungsfunktionen beschrieben.

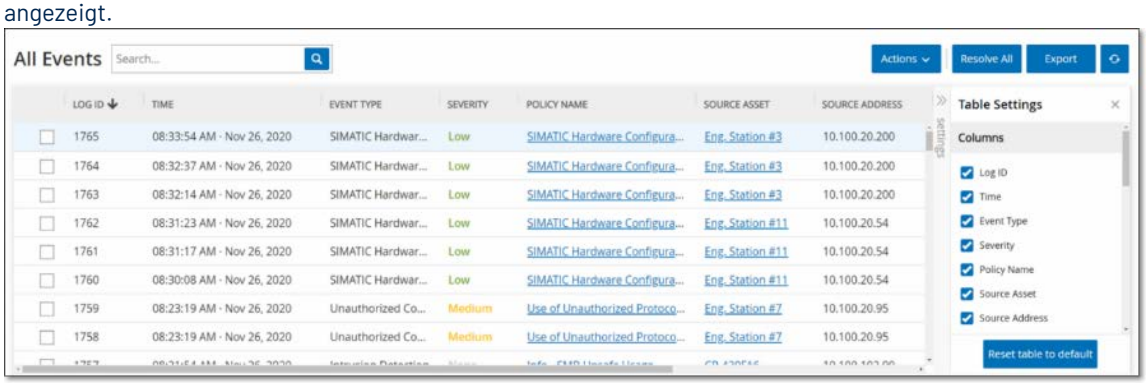
> Beispiele werden für die Bildschirme „Alle Ereignisse“ und „Alle Assets“ gezeigt, aber ähnliche Funktionen sind für die meisten Bildschirme in der Benutzeroberfläche verfügbar.
>
> Sie können jederzeit zu den standardmäßigen Anzeigeeinstellungen zurückkehren, indem Sie auf **Einstellungen** > **Tabelle auf Standard zurücksetzen** klicken.

Anpassen der Spaltenanzeige

Sie können anpassen, welche Spalten angezeigt werden und wie sie organisiert sind.

So wählen Sie aus, welche Spalten angezeigt werden:

1. Klicken Sie am rechten Rand der Tabelle auf die Registerkarte **Einstellungen**.
   Der Bereich **Tabelleneinstellungen** wird auf der rechten Seite des Bildschirms mit dem Abschnitt **Spalten** angezeigt.



2. Aktivieren Sie im Abschnitt **Spalten** das Kontrollkästchen neben jeder Spalte, die angezeigt werden soll.
3. Deaktivieren Sie das Kontrollkästchen neben jeder Spalte, die Sie ausblenden möchten.
   Nur die ausgewählten Spalten werden angezeigt.
4. Klicken Sie auf das „**x**“ (oder auf die Registerkarte **Einstellungen**), um das Fenster *Tabelleneinstellungen* zu schließen.

So passen Sie die Reihenfolge an, in der die Spalten angezeigt werden:

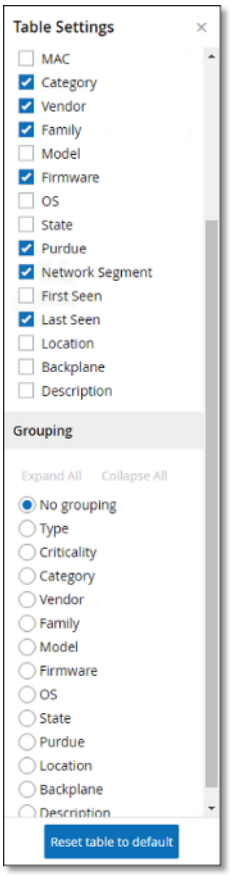
1. Klicken Sie auf eine Spalte und ziehen Sie sie an die gewünschte Position.

Gruppierung

Für jeden der Inventar-Bildschirme können Sie die Listen nach verschiedenen Parametern gruppieren, die für diesen bestimmten Bildschirm relevant sind.

So gruppieren Sie die Listen:

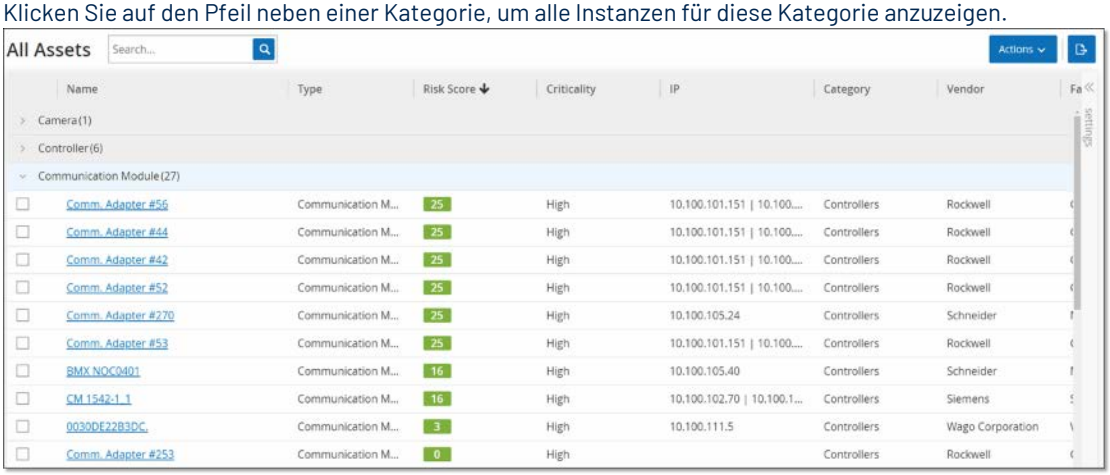
1. Klicken Sie am rechten Rand der Tabelle auf die Registerkarte **Einstellungen**.
   Der Bereich **Tabelleneinstellungen** wird auf der rechten Seite des Bildschirms mit den Abschnitten **Spalten** und **Gruppierung** angezeigt.
2. Scrollen Sie nach unten zum Abschnitt **Gruppierung**.



3. Aktivieren Sie das Optionsfeld neben dem Parameter, nach dem die Listen gruppiert werden sollen (z. B. „Typ“).

Die Gruppenkategorien werden im Hauptfenster angezeigt.

4. Klicken Sie auf das „**x**" (oder auf die Registerkarte **Einstellungen**), um das Fenster *Tabelleneinstellungen* zu schließen.
5. Klicken Sie auf den Pfeil neben einer Kategorie, um alle Instanzen für diese Kategorie anzuzeigen.



Sortierung

➡ So sortieren Sie die Listen:

1. Klicken Sie auf eine Spaltenüberschrift, um die Assets nach diesem Parameter zu sortieren (z. B. klicken Sie auf die Überschrift **Name**, um die Assets in alphabetischer Reihenfolge nach Namen anzuzeigen).
2. Klicken Sie ein zweites Mal auf die Spaltenüberschrift, wenn Sie die Anzeigereihenfolge umkehren möchten (d. h. A→Z, Z→A).

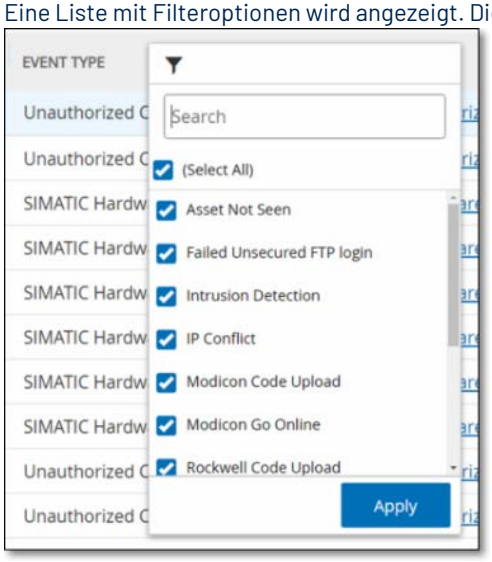
Filtern

Sie können Filter für eine oder mehrere Spaltenüberschriften festlegen. Die Filter sind kumulativ, sodass nur Listen angezeigt werden, die allen Filterkriterien entsprechen. Die Filteroptionen sind für jede Spaltenüberschrift spezifisch. Jeder Bildschirm bietet eine Auswahl relevanter Filter. Im Bildschirm „Controller-Inventar" können Sie beispielsweise nach *Name*, *Adressen*, *Typ*, *Backplane*, *Anbieter* usw. filtern.

➡ So filtern Sie die Listen:

1. Bewegen Sie den Mauszeiger über eine Spaltenüberschrift, um das Filtersymbol ▼ anzuzeigen.

2. Klicken Sie auf das Filtersymbol .
   Eine Liste mit Filteroptionen wird angezeigt. Die Optionen sind für jeden Parameter spezifisch.



3. Wählen Sie die Elemente aus, die Sie anzeigen möchten, und deaktivieren Sie diejenigen, die Sie ausblenden möchten.

> Sie können beginnen, indem Sie das Kontrollkästchen **Alle auswählen** deaktivieren und dann diejenigen aktivieren, die Sie anzeigen möchten.

4. Sie können die Liste nach Filtern durchsuchen und diese aktivieren oder deaktivieren.
5. Klicken Sie auf **Anwenden**.
   Die Listen werden wie angegeben gefiltert.
6. Das Filtersymbol neben der Spaltenüberschrift zeigt an, dass die Ergebnisse nach diesem Parameter gefiltert werden.

So entfernen Sie die Filter:

1. Klicken Sie auf das Filtersymbol .
2. Klicken Sie auf das Kontrollkästchen *Alle auswählen*, um Ihre Auswahl aufzuheben.
3. Klicken Sie **ein zweites Mal** auf das Kontrollkästchen *Alle auswählen*, um alle Elemente auszuwählen.
4. Klicken Sie auf **Anwenden**.

Suchen

Auf jedem Bildschirm können Sie nach bestimmten Datensätzen suchen.

So durchsuchen Sie die Listen:

1. Geben Sie den Suchtext in das Suchfeld ein.
2. Klicken Sie auf das Symbol .
3. Um den Suchtext zu löschen, klicken Sie auf das „**x**“.

Exportieren von Daten

Sie können Daten aus jeder der in der Benutzeroberfläche von Tenable.ot angezeigten Listen (z. B. Ereignisse, Inventar usw.) als CSV-Datei exportieren.

> Die exportierte Datei enthält alle Daten für diese Seite, selbst wenn Filter auf die aktuelle Anzeige angewendet wurden.

So exportieren Sie Daten:

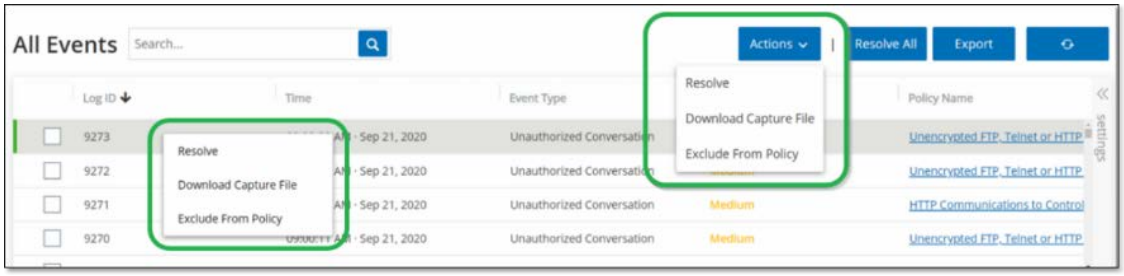
1. Gehen Sie zu dem Bildschirm, für den Sie Daten exportieren möchten.
2. Klicken Sie in der Kopfleiste auf **Exportieren**.

Aktionsmenüs

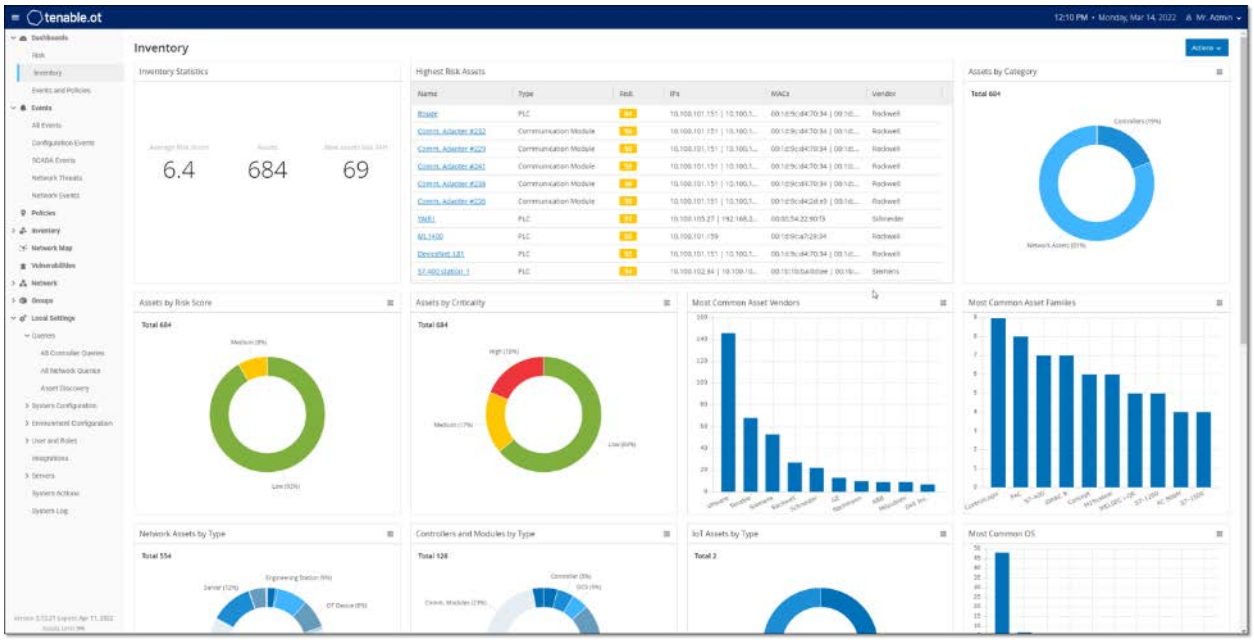
Jeder Bildschirm verfügt über eine Reihe von Aktionen, die für die auf diesem Bildschirm aufgeführten Elemente ausgeführt werden können. Beispielsweise können Sie im Bildschirm „Richtlinien" eine Richtlinie *anzeigen*, *bearbeiten*, *duplizieren* oder *löschen*. Im Bildschirm „Ereignisse" können Sie für ein Ereignis die Aktionen *Auflösen* und *Erfassungsdatei herunterladen* usw. ausführen.

Es gibt zwei Möglichkeiten, auf das Menü „Aktionen" zuzugreifen:

- Wählen Sie ein Element aus und klicken Sie dann auf die Schaltfläche **Aktionen** in der Kopfleiste ODER.
- Klicken Sie mit der rechten Maustaste auf das Element.



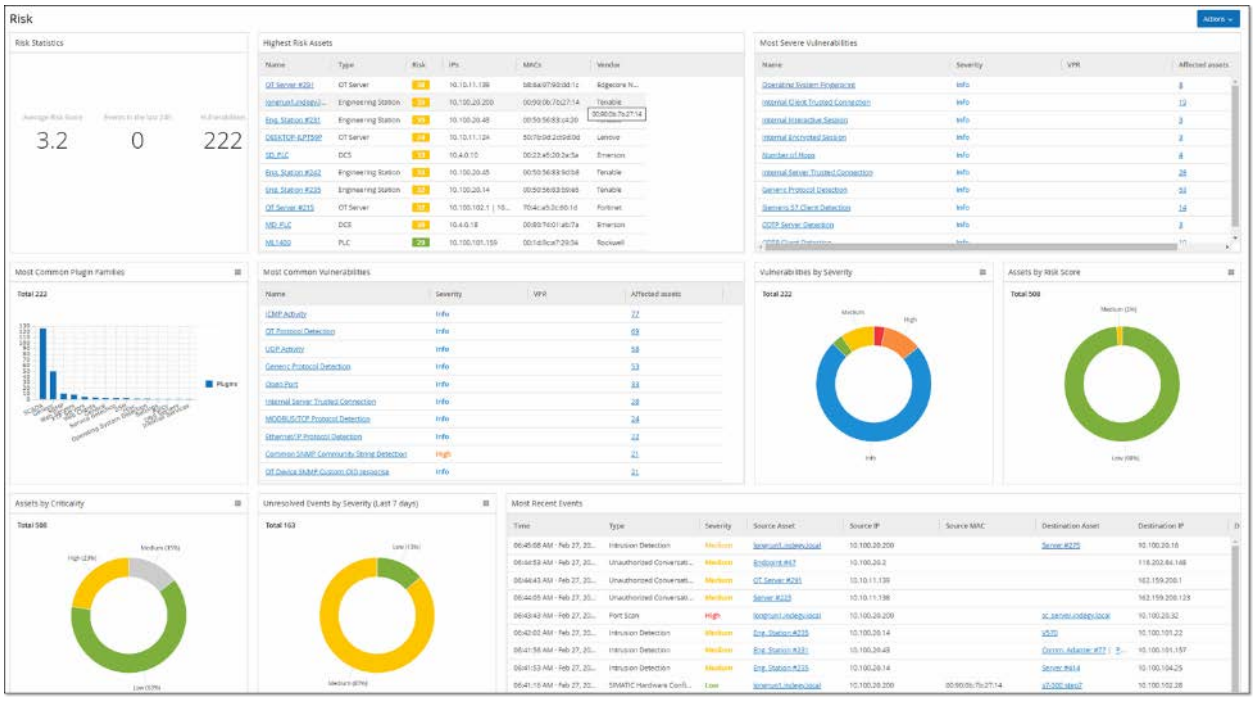
DASHBOARDS



Es gibt drei Dashboards: *Risiko*, *Inventar* sowie *Ereignisse und Richtlinien*. Die Dashboards enthalten Widgets, die einen Überblick über das Inventar und die Sicherheitslage Ihres Netzwerks geben. Sie können ein Dashboard aus der Hauptnavigation auswählen oder auf die Schaltfläche **Dashboards** in der oberen rechten Ecke klicken und eines aus dem daraufhin angezeigten Menü auswählen. Das Dashboard *Risiko* ist die anfängliche Standardansicht. Sie können die Standardansicht jedoch in ein anderes Dashboard ändern.

Sie können mit Dashboards interagieren, indem Sie die Anzeigeeinstellungen anpassen und Filter setzen, siehe **Interagieren mit Dashboards**.

Dashboard „Risiko“

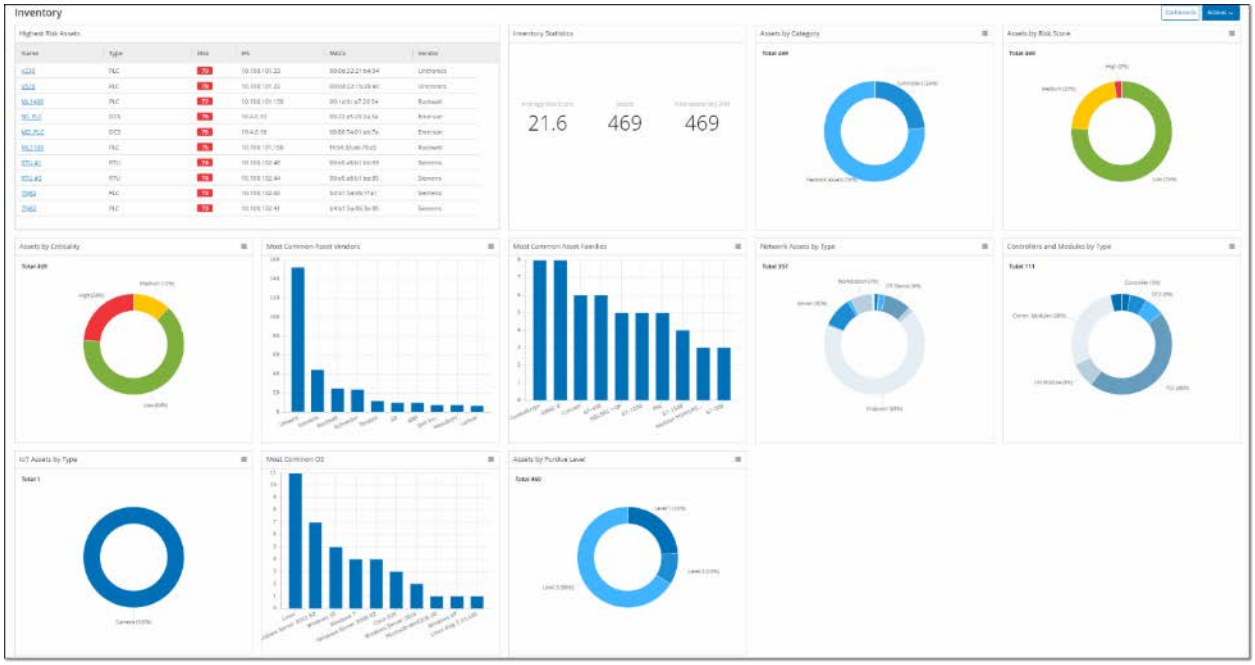


Das Dashboard **Risiko** bietet Informationen zur Cyber Exposure des Netzwerks, indem es Asset-Risikowerte und Kennzahlen für das Schwachstellen-Management analysiert.

Das Dashboard **Risiko** zeigt Widgets wie: Risikostatistik, Assets nach Risikowert, Assets nach Kritikalität, Ereignisse nach Schweregrad, Häufigste Schwachstellen usw.

Durch Klicken auf einen Asset- oder Schwachstellen-Link gelangen Sie zum entsprechenden Element im Bildschirm „Inventar" bzw. „Schwachstellen".

Dashboard „Inventar"

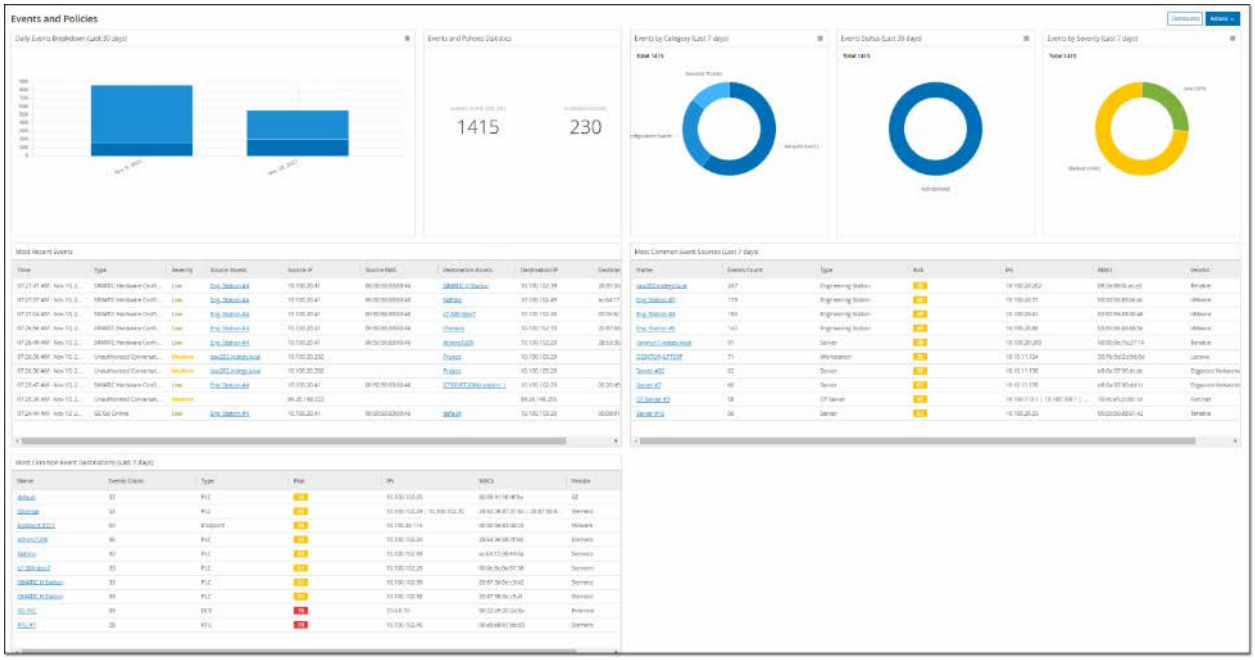


Das Dashboard **Inventar** bietet Einblick in die Asset-Inventarisierung und erleichtert Asset-Management und -Tracking.

Das Dashboard **Inventar** zeigt Widgets wie: Assets mit höchstem Risiko, Inventar-Statistik, Assets nach Risikowert, Controller und Module nach Typ, Assets nach Purdue-Level usw.

Wenn Sie auf einen Asset-Link klicken, gelangen Sie zum entsprechenden Asset im Bildschirm „Inventar".

Dashboard „Ereignisse und Richtlinien“



Das Dashboard **Ereignisse und Richtlinien** bietet eine Möglichkeit, Netzwerkbedrohungen zu erkennen, indem es die identifizierten Ereignisse und die daraus resultierenden Richtlinienverletzungen überwacht.

Das Dashboard **Ereignisse und Richtlinien** zeigt Widgets wie: Aufschlüsselung täglicher Ereignisse, Ereignis- und Richtlinienstatistiken, Ereignisstatus, Häufigste Ereignisziele usw.

Durch Klicken auf einen Ereignis-Link gelangen Sie zum entsprechenden Element im Bildschirm „Inventar“ bzw. „Ereignisse“.

Interagieren mit Dashboards

Sie können die Dashboard-Anzeige anpassen, indem Sie mit Widgets interagieren. Es gibt zwei Modi zum Anzeigen von Daten in den Dashboards, den Diagrammmodus und den Tabellenmodus. Einige Widgets haben einen festen Anzeigemodus, und einige können zwischen den Modi hin und her geschaltet werden. Widgets mit einem Symbol in der oberen rechten Ecke können im Diagrammmodus oder im Tabellenmodus angezeigt werden. Klicken Sie auf das Tabellen-/Diagrammsymbol, um zwischen den Modi umzuschalten.

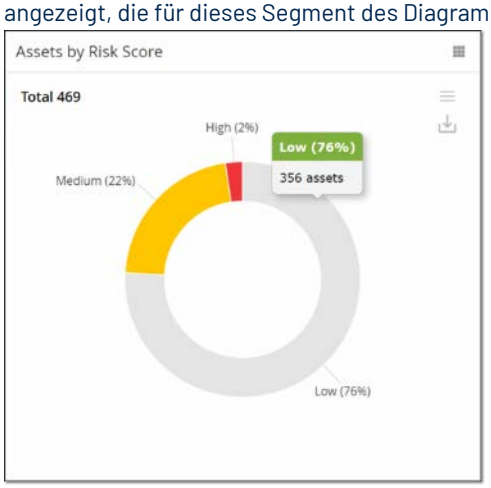
Filter können nur im Tabellenmodus gesetzt werden. Sobald ein Filter festgelegt wurde, wird er auch im Diagrammmodus angewendet.

Diagrammmodus

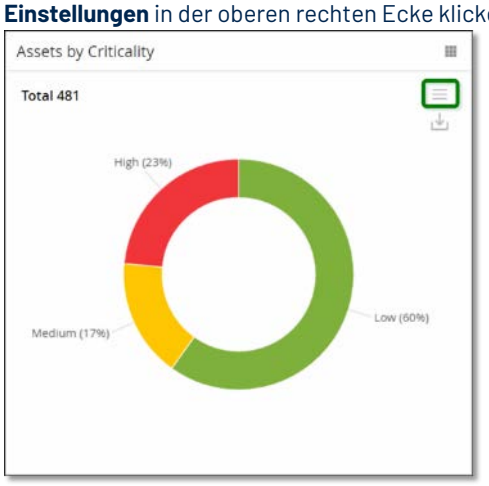
Der Diagrammmodus zeigt eine grafische Visualisierung der Widget-Daten.

Sie können auf folgende Weise mit den Widgets interagieren:

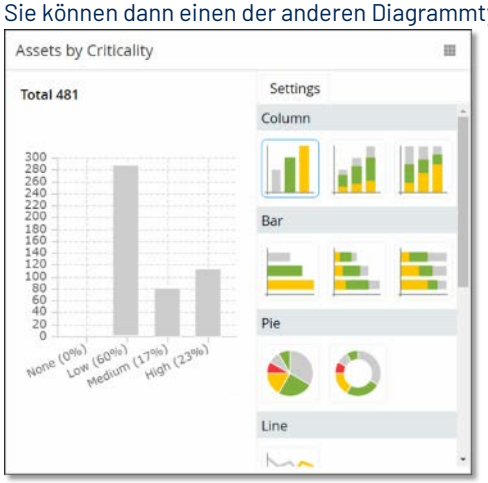
- Wenn Sie den Mauszeiger über einen Punkt im Diagramm bewegen, wird ein Popout-Fenster mit Daten angezeigt, die für dieses Segment des Diagramms spezifisch sind.



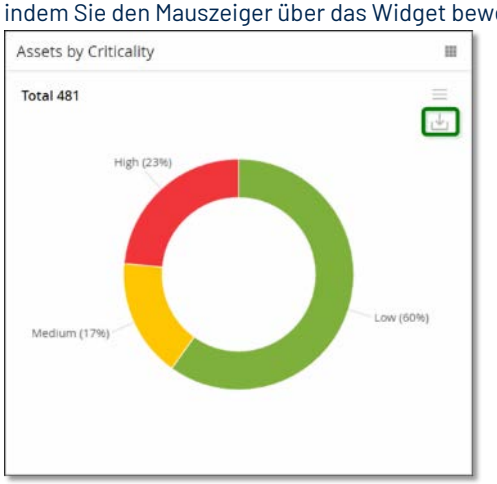
Sie können den für die Anzeige verwendeten Diagrammtyp anpassen, indem Sie auf die Schaltfläche **Einstellungen** in der oberen rechten Ecke klicken.



Sie können dann einen der anderen Diagrammtypen aus dem Menü **Einstellungen** auswählen.

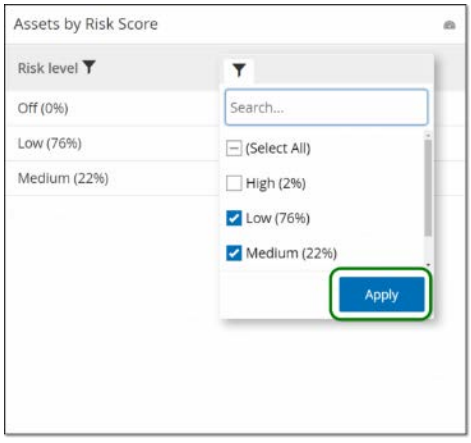


- Wenn Sie ein Widget im Diagrammmodus anzeigen, können Sie ein Bild des Diagramms herunterladen, indem Sie den Mauszeiger über das Widget bewegen und auf das **Download**-Symbol klicken.



Tabellenmodus

Wenn Sie ein Widget im Tabellenmodus anzeigen, können Sie jede Spalte filtern, indem Sie den Mauszeiger über die Spaltenüberschrift bewegen, auf das Filtersymbol klicken, Ihre Filter auswählen und auf **Anwenden** klicken. Die Filter werden auch auf das Diagramm angewendet, wenn Sie in den Diagrammmodus wechseln.

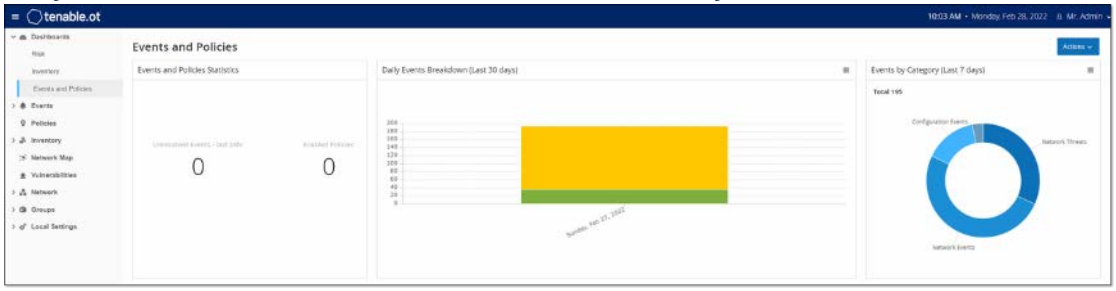


Ändern des Standard-Dashboards

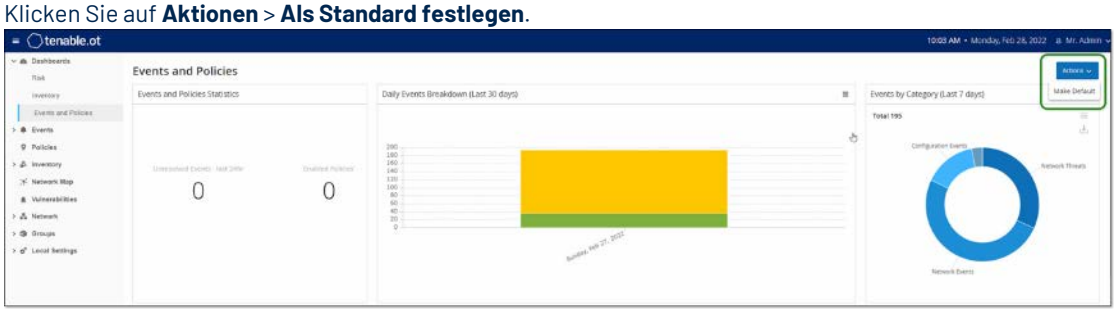
Das Risiko-Dashboard ist die anfängliche Standardansicht der Verwaltungskonsole. Sie können ein anderes Dashboard als Standardansicht anzeigen lassen.

So ändern Sie die standardmäßige Dashboard-Ansicht:

1. Navigieren Sie zu dem Dashboard, das Sie als Standardansicht festlegen möchten.



2. Klicken Sie auf **Aktionen** > **Als Standard festlegen**.



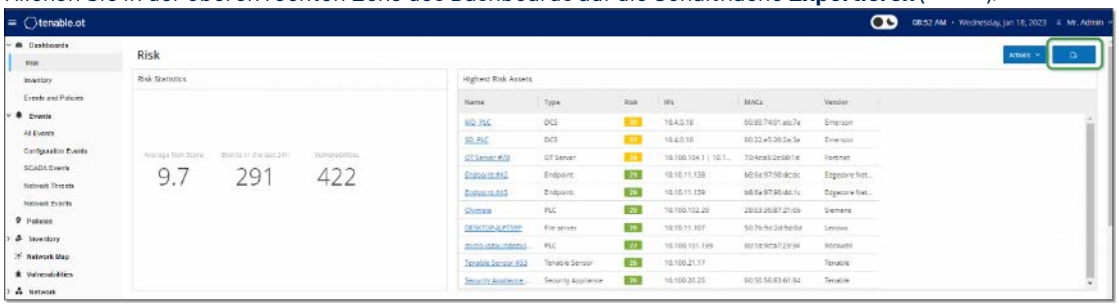
Das Standard-Dashboard wird aktualisiert. Beim nächsten Zugriff auf die Verwaltungskonsole wird dieses Dashboard angezeigt.

Exportieren des Dashboards

Über die Schaltfläche „Exportieren“ des Dashboard-Bildschirms kann eine PDF-Datei exportiert werden, die für jedes Dashboard-Widget eine separate Seite enthält.

So exportieren Sie das Dashboard:

1. Klicken Sie in der oberen rechten Ecke des Dashboards auf die Schaltfläche **Exportieren** ( ).



Die PDF-Datei wird automatisch in den Standardordner für Downloads heruntergeladen.

> Achten Sie darauf, dass die Registerkarte „Dashboard“ in Ihrem Browser geöffnet bleibt, während die PDF-Datei heruntergeladen wird (2 bis 3 Sekunden).

2. Navigieren Sie nach Abschluss des Downloads zu der gerade heruntergeladenen Datei, um sie anzuzeigen oder freizugeben.

RICHTLINIEN

Richtlinien werden verwendet, um bestimmte Arten von Ereignissen zu definieren, die verdächtig, nicht autorisiert, anormal oder anderweitig auffällig sind und im Netzwerk stattfinden. Wenn ein Ereignis eintritt, das alle Bedingungen der *Richtliniendefinition* für eine bestimmte Richtlinie erfüllt, wird im System ein Ereignis generiert. Das Ereignis wird im System protokolliert und Benachrichtigungen werden gemäß den für die Richtlinien konfigurierten *Richtlinienaktionen* versendet.

Es gibt zwei Arten von Richtlinienereignissen:

- **Richtlinienbasierte Erkennung** – Löst ein Ereignis aus, wenn die genauen Bedingungen der Richtlinie, wie durch eine Reihe von Ereignisdeskriptoren definiert, erfüllt sind.
- **Anomalie-Erkennung** – Löst ein Ereignis aus, wenn anomale oder verdächtige Aktivitäten im Netzwerk identifiziert werden.

Das System verfügt über eine Reihe vordefinierter (sofort einsetzbarer) Richtlinien. Darüber hinaus bietet das System die Möglichkeit, die vordefinierten Richtlinien zu bearbeiten oder neue benutzerdefinierte Richtlinien zu definieren.

Standardmäßig sind die *meisten* Richtlinien aktiviert. Informationen zum Aktivieren/Deaktivieren von Richtlinien finden Sie unter **Aktivieren und Deaktivieren von Richtlinien**.

Richtlinienkonfiguration

Jede Richtlinie besteht aus einer Reihe von Bedingungen, die einen bestimmten Verhaltenstyp im Netzwerk definieren. Dazu gehören Überlegungen wie die Aktivität, die beteiligten Assets und der Zeitpunkt des Ereignisses. Nur ein Ereignis, das **allen** in der Richtlinie festgelegten Parametern entspricht, löst ein Ereignis für diese Richtlinie aus. Jede Richtlinie hat eine bestimmte Konfiguration für Richtlinienaktionen, die den Schweregrad, die Benachrichtigungsmethoden und die Protokollierung des Ereignisses definiert.

Gruppen

Eine wesentliche Komponente bei der Definition von Richtlinien in Tenable.ot ist die Verwendung von *Gruppen*. Bei der Konfiguration einer Richtlinie wird jeder der Parameter durch eine Gruppe und nicht durch einzelne Entitäten bestimmt. Dadurch wird der Prozess für die Richtlinienkonfiguration erheblich optimiert. Wenn beispielsweise die Aktivität *Firmware-Aktualisierung* als verdächtige Aktivität gilt, wenn sie auf einem Controller zu bestimmten Tageszeiten (z. B. während der Arbeitszeit) durchgeführt wird, können Sie statt einer separaten Richtlinie für jeden Controller in Ihrem Netzwerk eine einzige Richtlinie erstellen, die für die Asset-Gruppe *Controller* gilt.

Die folgenden Arten von Gruppen werden im Rahmen der Richtlinienkonfiguration verwendet:

- **Asset-Gruppen** – Das System verfügt über vordefinierte Asset-Gruppen basierend auf dem Asset-Typ. Sie können benutzerdefinierte Gruppen hinzufügen, die auf anderen Faktoren wie Standort, Abteilung, Kritikalität usw. basieren.
- **Netzwerksegmente** – Das System erstellt automatisch generierte Netzwerksegmente basierend auf Asset-Typ und IP-Bereich. Sie können benutzerdefinierte Netzwerksegmente erstellen, die eine beliebige Gruppe von Assets definieren, die ähnliche Kommunikationsmuster haben sollten.
- **E-Mail-Gruppen** – Sie können mehrere E-Mail-Konten gruppieren, die E-Mail-Benachrichtigungen für bestimmte Ereignisse erhalten. Zum Beispiel Gruppierung nach Rolle, Abteilung usw.
- **Port-Gruppen** – Ähnlich genutzte Ports können zu Gruppen zusammengefasst werden. Zum Beispiel Ports, die auf Rockwell-Controllern im Allgemeinen offen sind.

- **Protokollgruppen** – Kommunikationsprotokolle können nach Protokolltyp (z. B. Modbus), Anbieter (z. B. von Rockwell zugelassene Protokolle) usw. gruppiert werden.
- **Planungsgruppen** – Mehrere Zeitbereiche können als Planungsgruppe mit einem bestimmten gemeinsamen Merkmal gruppiert werden. Zum Beispiel Arbeitszeiten, Wochenende usw.
- **Tag-Gruppen** – Sie können Tags gruppieren, die ähnliche Betriebsdaten in verschiedenen Controllern enthalten. Zum Beispiel Tags, die die Ofentemperatur steuern.
- **Regelgruppen** – Regelgruppen bestehen aus einer Gruppe verwandter Regeln, die durch ihre Suricata-Signatur-IDs (SIDs) identifiziert werden. Diese Gruppen werden als Richtlinienbedingung zum Definieren von Intrusion Detection-Richtlinien verwendet.

Richtlinien können nur mit Gruppen definiert werden, die in Ihrem System konfiguriert wurden. Das System wird mit einer Reihe vordefinierter Gruppen geliefert. Sie können diese Gruppen bearbeiten und eigene Gruppen hinzufügen, siehe Kapitel **Gruppen**.

Richtlinienparameter können **nur** mithilfe von Gruppen festgelegt werden. Selbst wenn Sie möchten, dass eine Richtlinie auf eine einzelne Entität angewendet wird, müssen Sie eine Gruppe konfigurieren, die nur diese Entität enthält.

Schweregradstufen

Jeder Richtlinie ist ein bestimmter Schweregrad zugewiesen, der den Grad des Risikos angibt, das von der Situation ausgeht, die das Ereignis ausgelöst hat. Die Bedeutung der verschiedenen Ereignisstufen ist in der folgenden Tabelle beschrieben.

Schweregrad	Beschreibung
Kein	Das Ereignis ist kein Grund zur Besorgnis.
Gering	Kein unmittelbarer Grund zur Sorge. Sollte bei Gelegenheit geprüft werden.
Mittel	Moderate Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte behandelt werden, wenn es passt.
Hoch	Schwerwiegende Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte sofort behandelt werden.

Ereignisbenachrichtigungen

Wenn ein Ereignis eintritt, das die Bedingungen der Richtlinie erfüllt, wird ein Ereignis ausgelöst. Alle Ereignisse werden unter den Ereignissen angezeigt. (Jedes Ereignis wird außerdem im Bildschirm „Richtlinien“ unter der Richtlinie aufgeführt, die das Ereignis ausgelöst hat, und im Bildschirm „Inventar“ unter dem Asset, das von dem Ereignis betroffen war.) Darüber hinaus können Richtlinien so konfiguriert werden, dass Benachrichtigungen über Ereignisse per Syslog-Protokoll an ein externes SIEM gesendet werden und/oder an bestimmte E-Mail-Empfänger.

- **Syslog-Benachrichtigung** – Syslog-Nachrichten verwenden das CEF-Protokoll sowohl mit Standardschlüsseln als auch mit benutzerdefinierten Schlüsseln (die für die Verwendung mit Tenable.ot konfiguriert sind). Eine Erläuterung zur Interpretation von Syslog-Benachrichtigungen finden Sie im **TENABLE.OT SYSLOG INTEGRATION GUIDE**.
- **E-Mail-Benachrichtigungen** – E-Mail-Nachrichten enthalten Details über das Ereignis, das die Benachrichtigung generiert hat, sowie Vorschläge für Schritte, die unternommen werden sollten, um die Bedrohung zu mindern.

Richtlinienkategorien und Unterkategorien

Die Richtlinien sind nach folgenden Kategorien geordnet:

- **Richtlinien für Konfigurationsereignisse** – Diese Richtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Es gibt zwei Unterkategorien von Konfigurationsereignisrichtlinien:
    - **Controller-Validierung** – Diese Richtlinien beziehen sich auf Änderungen, die in den Controllern im Netzwerk stattfinden. Dabei kann es sich um Statusänderungen eines Controllers, aber auch um Änderungen an Firmware, Asset-Eigenschaften oder Codeblöcken handeln. Die Richtlinien können auf bestimmte Zeitpläne (z. B. Firmware-Upgrade während eines Arbeitstages) und/oder bestimmte Controller beschränkt werden.
    - **Controller-Aktivitäten** – Diese Richtlinien beziehen sich auf bestimmte Engineering-Befehle, die sich auf den Status und die Konfiguration von Controllern auswirken. Es ist möglich, bestimmte Aktivitäten zu definieren, die immer Ereignisse generieren, oder eine Reihe von Kriterien zum Generieren von Ereignissen festzulegen. Zum Beispiel, wenn bestimmte Aktivitäten zu bestimmten Zeiten und/oder auf bestimmten Controllern ausgeführt werden. Es werden Sperrlisten und Zulassungslisten für Assets, Aktivitäten und Zeitpläne unterstützt.
- **Richtlinien für Netzwerkereignisse** – Diese Richtlinien beziehen sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets. Dies schließt Assets ein, die dem Netzwerk hinzugefügt oder daraus entfernt wurden. Dazu gehören auch Traffic-Muster, die für das Netzwerk ungewöhnlich sind oder die als besorgniserregend gekennzeichnet wurden. Wenn beispielsweise eine Engineering-Station mit einem Controller über ein Protokoll kommuniziert, das nicht Teil eines vorkonfigurierten Satzes von Protokollen ist (z. B. Protokolle, die von Controllern verwendet werden, die von einem bestimmten Anbieter hergestellt werden), wird ein Ereignis ausgelöst. Diese Richtlinien können auf bestimmte Zeitpläne und/oder bestimmte Assets beschränkt werden. Anbieterspezifische Protokolle werden der Einfachheit halber nach Anbieter organisiert, während jedes Protokoll in einer Richtliniendefinition verwendet werden kann.
- **SCADA-Ereignisrichtlinien** – Diese Richtlinien erkennen Änderungen der Sollwerte, die den industriellen Prozess beeinträchtigen können. Diese Änderungen können aus einem Cyberangriff oder menschlichem Fehlverhalten resultieren.
- **Netzwerkbedrohungsrichtlinien** – Diese Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert wurden.

Richtlinientypen

Innerhalb jeder Kategorie und Unterkategorie gibt es eine Reihe verschiedener Typen von Richtlinien. Das System wird mit vordefinierten Richtlinien der einzelnen Typen geliefert. Sie können auch Ihre eigenen benutzerdefinierten Richtlinien der einzelnen Typen erstellen. Die folgenden Tabellen erläutern die verschiedenen Richtlinientypen, gruppiert nach Kategorie.

Konfigurationsereignis – Typen von Controller-Aktivitätsereignissen

Controller-Aktivitäten beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden (d. h. die „Befehle“, die zwischen Assets im Netzwerk implementiert werden). Es gibt viele verschiedene Typen von Controller-Aktivitätsereignissen. Jeder Typ wird durch den Controller-Typ definiert, auf dem die Aktivität ausgeführt wird, und die spezifische Aktivität, die identifiziert wird (z. B. Rockwell-SPS-Stopp, SIMATIC-Code-Download, Modicon-Online-Sitzung usw.).

Die Parameter für die Richtliniendefinition (d. h. Richtlinienbedingungen), die für Controller-Aktivitätsereignisse gelten, sind *Quell-Asset*, *Ziel-Asset* und *Zeitplan*.

Konfigurationsereignis – Typen von Controller-Validierungsereignissen

Die folgende Tabelle beschreibt die verschiedenen Typen von Controller-Validierungsereignissen.

Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine *Asset-Gruppe* oder ein *Netzwerksegment* ausgewählt wird.

Ereignistyp	Richtlinienbedingungen	Beschreibung
Änderung des Schlüsselschalters	Betroffenes Asset, Zeitplan	Durch Anpassen der Position des physischen Schlüssels wurde eine Änderung am Controller-Status vorgenommen. (Derzeit nur für Rockwell-Controller unterstützt.)
Statusänderung	Betroffenes Asset, Zeitplan	Der Controller wechselte von einem Betriebsstatus (z. B. Läuft, Angehalten, Test usw.) in einen anderen.
Änderung der Firmware-Version	Betroffenes Asset, Zeitplan	An der auf dem Controller ausgeführten Firmware wurde eine Änderung vorgenommen.
Modul nicht gesehen	Betroffenes Asset, Zeitplan	Erkennt ein zuvor identifiziertes Modul, das von einer Backplane entfernt wurde.
Neues Modul erfasst	Betroffenes Asset, Zeitplan	Erkennt ein neues Modul, das einer vorhandenen Backplane hinzugefügt wird.
Snapshot-Konflikt	Betroffenes Asset, Zeitplan	Der letzte Snapshot eines Controllers (der den aktuellen Status des auf einem Controller bereitgestellten Programms erfasst) war nicht identisch mit dem vorherigen Snapshot dieses Controllers.

Netzwerkereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von Netzwerkereignissen.

Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine *Asset-Gruppe* oder ein *Netzwerksegment* ausgewählt wird.

Ereignistyp	Richtlinienbedingungen	Beschreibung
Asset nicht gesehen	Nicht gesehen für, Betroffenes Asset, Zeitplan	Erkennt zuvor identifizierte Assets in der Gruppe *Betroffene Assets*, die für die angegebene Zeitdauer innerhalb des angegebenen Zeitraums aus dem Netzwerk entfernt wurden.

Ereignistyp	Richtlinienbedingungen	Beschreibung
Änderung der USB-Konfiguration	Betroffene Assets, Zeitplan	Erkennt, wenn ein USB-Gerät an eine Windows-basierte Workstation angeschlossen oder von dieser entfernt wird. Die Richtlinie gilt für Änderungen an einem Asset in der Gruppe „Betroffene Assets" während des angegebenen Zeitraums.
IP-Konflikt	Zeitplan	Erkennt, wenn mehrere Assets im Netzwerk die gleiche IP-Adresse verwenden. Dies kann auf einen Cyberangriff hindeuten oder auf mangelhafte Netzwerkverwaltung zurückzuführen sein. Die Richtlinie gilt für IP-Konflikte, die während des angegebenen Zeitraums erfasst wurden.
Netzwerk-Baseline-Abweichung	Quelle, Ziel, Protokoll, Zeitplan	Erkennt neue Verbindungen zwischen Assets, die während der Netzwerk-Baseline-Stichprobe nicht miteinander kommuniziert haben. Diese Option ist nur verfügbar, nachdem eine Netzwerk-Baseline im System eingerichtet wurde. Um die anfängliche Netzwerk-Baseline festzulegen oder die Netzwerk-Baseline zu aktualisieren, befolgen Sie die im Abschnitt **Festlegen einer Netzwerk-Baseline** beschriebenen Verfahren. Die Richtlinie gilt für die Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe unter Verwendung eines Protokolls aus der Protokollgruppe während des angegebenen Zeitraums.
Neues Asset erfasst	Betroffenes Asset, Zeitplan	Erkennt neue Assets des in der *Quell*-Asset-Gruppe angegebenen Typs, die während des angegebenen Zeitraums in Ihrem Netzwerk angezeigt werden.
Offener Port	Betroffenes Asset, Port	Erkennt neue offene Ports in Ihrem Netzwerk. Ungenutzte offene Ports können ein Sicherheitsrisiko darstellen. Die Richtlinie gilt für Assets in der Gruppe „Betroffene Assets" und für Ports, die sich in der Port-Gruppe befinden.
Spitze im Netzwerk-Traffic	Zeitfenster, Empfindlichkeitsstufe, Zeitplan	Erkennt anomale Spitzen im Netzwerk-Traffic-Volumen. Die Richtlinie gilt für Spitzen relativ zum angegebenen Zeitfenster und basierend auf der angegebenen Empfindlichkeitsstufe. Sie ist auch auf den angegebenen Zeitbereich begrenzt.
Spike in Konversation	Zeitfenster, Empfindlichkeitsstufe, Zeitplan	Erkennt anomale Spitzen in der Anzahl der Konversationen im Netzwerk. Die Richtlinie gilt für Spitzen relativ zum angegebenen Zeitfenster und basierend auf der angegebenen Empfindlichkeitsstufe. Sie ist auch auf den angegebenen Zeitbereich begrenzt.

Ereignistyp	Richtlinienbedingungen	Beschreibung
RDP-Verbindung (authentifiziert)	Quelle, Ziel, Zeitplan	Im Netzwerk wurde eine RDP-Verbindung (Remote Desktop Protocol) mit Authentifizierungsdaten hergestellt. Die Richtlinie gilt für ein Asset in der *Quell*-Asset-Gruppe, das eine Verbindung zu einem Asset in der *Ziel*-Asset-Gruppe während des angegebenen Zeitraums herstellt.
RDP-Verbindung (nicht authentifiziert)	Quelle, Ziel, Zeitplan	Im Netzwerk wurde eine RDP-Verbindung (Remote Desktop Protocol) ohne Authentifizierungsdaten hergestellt. Die Richtlinie gilt für ein Asset in der *Quell*-Asset-Gruppe, das eine Verbindung zu einem Asset in der *Ziel*-Asset-Gruppe während des angegebenen Zeitraums herstellt.
Nicht autorisierte Konversation	Quelle, Ziel, Protokoll, Zeitplan	Erkennt Kommunikation, die zwischen Assets im Netzwerk gesendet wird. Die Richtlinie gilt für die Kommunikation von einem Asset in der *Quell*-Asset-Gruppe zu einem Asset in der *Ziel*-Asset-Gruppe unter Verwendung eines *Protokolls* aus der Protokollgruppe während des angegebenen Zeitraums.
Erfolgreiches ungesichertes FTP-Login	Quelle, Ziel, Zeitplan	FTP gilt als unsicheres Protokoll. Diese Richtlinie erkennt erfolgreiche Logins über FTP.
Fehlgeschlagenes ungesichertes FTP-Login	Quelle, Ziel, Zeitplan	FTP gilt als unsicheres Protokoll. Diese Richtlinie erkennt fehlgeschlagene Login-Versuche über FTP.
Erfolgreiches ungesichertes Telnet-Login	Quelle, Ziel, Zeitplan	Telnet gilt als unsicheres Protokoll. Diese Richtlinie erkennt erfolgreiche Logins über Telnet.
Fehlgeschlagenes ungesichertes Telnet-Login	Quelle, Ziel, Zeitplan	Telnet gilt als unsicheres Protokoll. Diese Richtlinie erkennt fehlgeschlagene Login-Versuche über Telnet.
Ungesicherter Telnet-Login-Versuch	Quelle, Ziel, Zeitplan	Telnet gilt als unsicheres Protokoll. Diese Richtlinie erkennt Login-Versuche über Telnet (für die der Ergebnisstatus nicht erkannt wurde).

Netzwerkbedrohungs-Ereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von Netzwerkbedrohungsereignissen.

Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine *Asset-Gruppe* oder ein *Netzwerksegment* ausgewählt wird.

Ereignistyp	Richtlinienbedingungen	Beschreibung
Intrusion Detection	Quelle, betroffenes Asset, Regelgruppe, Zeitplan	Intrusion Detection-Richtlinien verwenden signaturbasierte OT- und IT-Bedrohungserkennung, um Netzwerk-Traffic zu identifizieren, der auf Bedrohungen durch Eindringlinge hinweist. Die Erkennung basiert auf Regeln, die in der Threats-Engine von Suricata katalogisiert wurden. Die Regeln sind in Kategorien (z. B. ICS-Angriffe, Denial of Service, Malware usw.) und Unterkategorien (z. B. ICS-Angriffe – Stuxnet, ICS-Angriffe – Black Energy usw.) gruppiert. Das System wird mit einer Reihe von vordefinierten Gruppen verwandter Regeln geliefert. Sie können auch Ihre eigenen benutzerdefinierten Gruppierungen verschiedener Regeln konfigurieren.
ARP-Scan	Betroffenes Asset, Zeitplan	Erkennt ARP-Scans (Netzwerkaufklärungsaktivität), die im Netzwerk ausgeführt werden. Die Richtlinie gilt für Scans, die in der Gruppe *„Betroffene* Assets“ während des angegebenen Zeitraums übertragen werden.
Port-Scan	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt SYN-Scans (Netzwerkaufklärungsaktivität), die im Netzwerk ausgeführt werden, um offene (anfällige) Ports zu erkennen. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums.

SCADA-Ereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von SCADA-Ereignistypen.

Richtlinienbedingungen in Bezug auf betroffene Assets, Quellen oder Ziele können festgelegt werden, indem entweder eine *Asset-Gruppe* oder ein *Netzwerksegment* ausgewählt wird.

Ereignistyp	Richtlinienbedingungen	Beschreibung
Unzulässige Modbus-Datenadresse	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt den Fehlercode „Unzulässige Datenadresse“ im Modbus-Protokoll. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums.

Ereignistyp	Richtlinienbedingungen	Beschreibung
Unzulässiger Modbus-Datenwert	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt den Fehlercode „Unzulässiger Datenwert“ im Modbus-Protokoll. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums.
Unzulässige Modbus-Funktion	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt den Fehlercode „Unzulässige Funktion“ im Modbus-Protokoll. Die Richtlinie gilt für Kommunikation von einem Asset in der Quell-Asset-Gruppe zu einem Asset in der Ziel-Asset-Gruppe während des angegebenen Zeitraums.
Nicht autorisierter Schreibvorgang	Quell-Asset, Tag-Gruppe, Tag-Wert, Zeitplan	Erkennt nicht autorisierte Tag-Schreibvorgänge für die angegebenen Tags auf einem Controller (derzeit unterstützt für Rockwell- und S7-Controller) in der angegebenen Quell-Asset-Gruppe. Die Richtlinie kann so konfiguriert werden, dass sie jeden neuen Schreibvorgang, eine Änderung von einem angegebenen Wert oder einen Wert außerhalb eines angegebenen Bereichs erkennt. Die Richtlinie gilt nur während des angegebenen Zeitraums.
ABB – Nicht autorisierter Schreibvorgang	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt über MMS an ABB 800xA-Controller gesendete Schreibbefehle, die außerhalb des zulässigen Bereichs liegen.
IEC 60870-5-104-Befehle (Start/Stopp der Datenübertragung, Abfragebefehl, Zählerabfragebefehl, Uhrensynchronisationsbefehl, Befehl zur Prozessrücksetzung, Testbefehl mit Zeitmarke)	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt bestimmte Befehle, die an IEC-104-Master- oder -Slave-Einheiten gesendet werden und als riskant gelten.
DNP3-Befehle	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt alle Hauptbefehle, die über das DNP3-Protokoll gesendet werden, z. B. Select, Operate, Warm/Cold Restart usw. Erkennt auch Fehler, die auf interne Indikatoren wie nicht unterstützte Funktionscodes und Parameterfehler zurückzuführen sind.

Aktivieren und Deaktivieren von Richtlinien

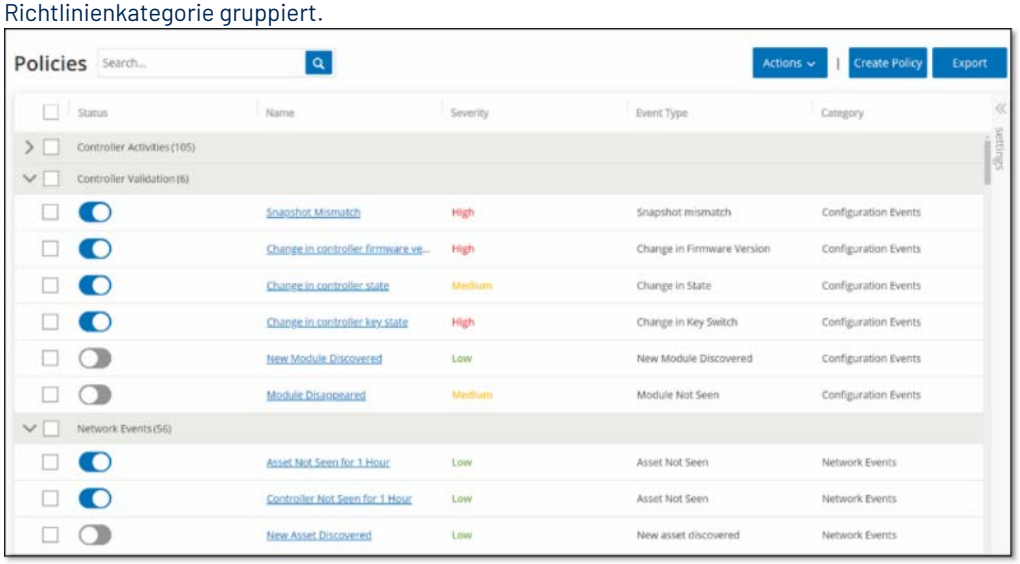
Jede Richtlinie, die bereits in Ihrem System konfiguriert ist (sowohl vorkonfiguriert als auch benutzerdefiniert), kann ganz einfach aktiviert oder deaktiviert werden. Sie können Richtlinien einzeln aktivieren und deaktivieren oder mehrere Richtlinien auswählen, um sie gesammelt zu aktivieren/deaktivieren.

Viele Richtlinien sind bei der Erfassung von Daten auf Abfragen angewiesen. Wenn einige oder alle Abfragefunktionen deaktiviert sind, können die entsprechenden Richtlinien nicht angewendet werden. Abfragen können unter **Lokale Einstellungen** > **Abfragen** aktiviert werden, siehe

Abfragen.

So aktivieren/deaktivieren Sie eine Richtlinie:

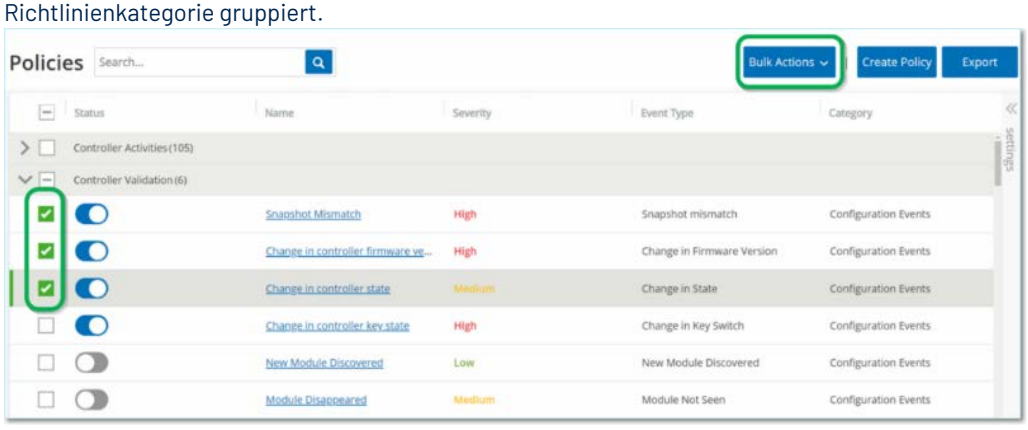
1. Rufen Sie den Bildschirm **Richtlinien** auf.
   Für jede Richtlinie, die im System konfiguriert ist, wird eine Liste angezeigt. Die Richtlinienlisten sind nach Richtlinienkategorie gruppiert.



2. Stellen Sie den Umschalter **Status** neben der entsprechenden Richtlinie auf **EIN/AUS**.

So aktivieren/deaktivieren Sie mehrere Richtlinien:

1. Rufen Sie den Bildschirm **Richtlinien** auf.
   Für jede Richtlinie, die im System konfiguriert ist, wird eine Liste angezeigt. Die Richtlinienlisten sind nach Richtlinienkategorie gruppiert.



2. Aktivieren Sie das Kontrollkästchen neben jeder Richtlinie, die Sie aktivieren/deaktivieren möchten. Verwenden Sie eine der folgenden Auswahlmethoden:
   - **Einzelne Richtlinien auswählen** – Klicken Sie auf das Kontrollkästchen neben bestimmten Richtlinien.
   - **Richtlinientypen auswählen** – Klicken Sie auf das Kontrollkästchen neben der Überschrift eines Richtlinientyps.
   - **Alle Richtlinien auswählen** – Klicken Sie auf das Kontrollkästchen in der Titelleiste oben in der Tabelle.
3. Klicken Sie in der Kopfleiste auf die Schaltfläche **Massenaktionen**.
4. Wählen Sie die gewünschte Aktion (**Aktivieren** oder **Deaktivieren**) aus der Dropdown-Liste aus. Alle ausgewählten Richtlinien werden aktiviert/deaktiviert.

Anzeigen von Richtlinien

Der Bildschirm **Richtlinien** zeigt eine Liste für jede Richtlinie, die in Ihrem System konfiguriert ist. Die Listen sind für jede Richtlinienkategorie unter separaten Registerkarten gruppiert. Auf diesem Bildschirm werden sowohl vorkonfigurierte Richtlinien als auch benutzerdefinierte Richtlinien aufgelistet. In der Auflistung für jede Richtlinie gibt es einen Umschalter, der den aktuellen Status der Richtlinie anzeigt, sowie mehrere Parameter, die die Richtlinienkonfiguration angeben.

Sie können Spalten ein- und ausblenden und die Asset-Listen sortieren und filtern sowie nach Schlüsselwörtern suchen. Eine Erläuterung der Anpassungsfunktionen finden Sie unter **Arbeiten mit Listen**.

Die Richtlinienparameter werden in der folgenden Tabelle beschrieben.

Parameter	Beschreibung
Status	Zeigt an, ob die Richtlinie aktiviert oder deaktiviert ist. Wenn die Richtlinie vom System automatisch deaktiviert wurde, weil sie zu viele Ereignisse generiert hat, wird ein Warnsymbol angezeigt. Schalten Sie den Status-Schalter um, um eine Richtlinie zu aktivieren/deaktivieren.
Richtlinien-ID	Ein eindeutiger Bezeichner für die Richtlinie im System. Richtlinien-IDs sind nach Kategorie gruppiert, mit einem anderen Präfix für jede Kategorie (z. B. P1 für Controller-Aktivitäten, P2 für Netzwerkereignisse usw.).
Name	Der Name der Richtlinie.
Schweregrad	Der Schweregrad des Ereignisses. Mögliche Werte sind: Kein, Gering, Mittel oder Hoch. Eine Beschreibung der Schweregrade finden Sie im Abschnitt **Schweregradstufen**.
Ereignistyp	Der spezifische Ereignistyp, der diese Ereignisrichtlinie auslöst.
Kategorie	Die allgemeine Kategorie für den Ereignistyp, der diese Ereignisrichtlinie auslöst. Mögliche Werte sind: Konfiguration, SCADA, Netzwerkbedrohungen oder Netzwerkereignis. Eine Erläuterung der verschiedenen Kategorien finden Sie unter **Richtlinienkategorien und Unterkategorien**.
Quelle	Eine Richtlinienbedingung. Die Quell-Asset-Gruppe/das Quell-Netzwerksegment (d. h. das Asset, das die Aktivität initiiert hat), für die die Richtlinie gilt.

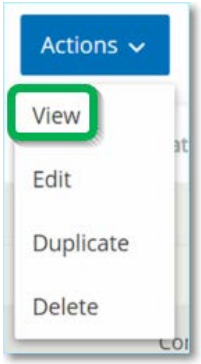
Parameter	Beschreibung
Ziel/Betroffenes Asset	Eine Richtlinienbedingung. Die Ziel-Asset-Gruppe/das Ziel-Netzwerksegment (d. h. das Asset, das die Aktivität erhält), für die die Richtlinie gilt. Bei Richtlinien, die ein einzelnes Asset betreffen (ohne Quelle und Ziel), zeigt dieser Parameter das Asset an, das von dem Ereignis betroffen war.
Zeitplan	Eine Richtlinienbedingung. Der Zeitraum, für den die Richtlinie gilt.
Syslog	Der Syslog-Server (SIEM), auf dem Ereignisse für diese Richtlinie protokolliert werden.
E-Mail	Die E-Mail-Gruppe, an die Ereignisbenachrichtigungen für diese Richtlinie gesendet werden.
Unterkategorie	Die Unterkategorieklassifizierung des Ereignisses. Die Kategorie *Konfigurationsereignisse* setzt sich aus den Unterkategorien *Controller-Aktivitäten* und *Controller-Validierung* zusammen. Eine Erläuterung der verschiedenen Unterkategorien finden Sie unter **Richtlinienkategorien und Unterkategorien**.
Anzahl der Ereignisse pro Richtlinie	Listet die Anzahl der Ereignisse auf, die von jeder Richtlinie generiert wurden. Durch Klicken auf die Spalte ist es möglich, die Liste zu sortieren, um sich auf die Richtlinien mit den meisten Verstößen/Ereignissen zu konzentrieren.
Ausschlüsse	Listet die Anzahl der Ausschlüsse auf, die jeder Richtlinie hinzugefügt wurden. Weitere Informationen finden Sie unter **Erstellen von Richtlinienausschlüssen**.

Anzeigen von Richtliniendetails

Sie können den Bildschirm „Richtliniendetails“ für eine Richtlinie öffnen, um weitere Details zur Richtlinie anzuzeigen. Dieser Bildschirm zeigt eine vollständige Liste aller Richtlinienbedingungen. Er zeigt auch eine Liste aller Ereignisse, die von der ausgewählten Richtlinie ausgelöst wurden.

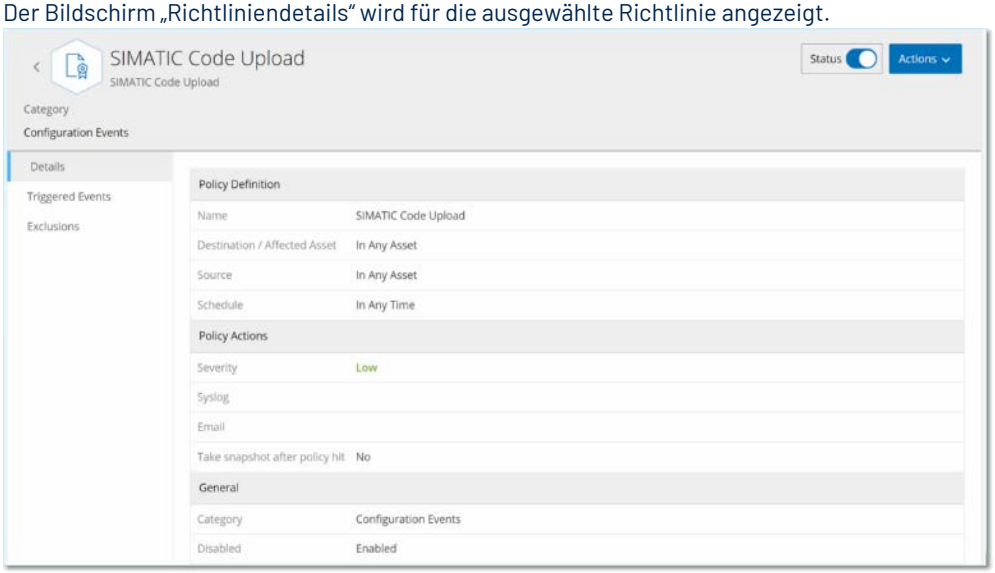
So öffnen Sie den Bildschirm „Richtliniendetails“ für eine bestimmte Richtlinie:

1. Wählen Sie im Bildschirm **Richtlinien** die gewünschte Richtlinie aus.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **Anzeigen** aus der Dropdown-Liste aus.



Alternativ können Sie das Menü „Aktionen“ aufrufen, indem Sie mit der rechten Maustaste auf die entsprechende Richtlinie klicken.

Der Bildschirm „Richtliniendetails“ wird für die ausgewählte Richtlinie angezeigt.



Der Bildschirm „Richtliniendetails“ enthält die folgenden Elemente:

- **Kopfleiste** – Zeigt Namen, Typ und Kategorie der Richtlinie an. Dort finden Sie auch einen Umschalter zum Aktivieren und Deaktivieren der Richtlinie und eine Dropdown-Liste der verfügbaren Aktionen (Bearbeiten, Duplizieren und Löschen).
- **Registerkarte „Details“** – Zeigt Details zur Richtlinienkonfiguration in drei Abschnitten an:
    - **Richtliniendefinition** – Zeigt alle Richtlinienbedingungen an. Dies umfasst alle relevanten Felder gemäß dem Typ der Richtlinie.
    - **Richtlinienaktionen** – Zeigt den Schweregrad sowie das Ziel (Syslog, E-Mail) von Ereignisbenachrichtigungen an. Zeigt auch an, ob die Funktion *Nach erstem Treffer deaktivieren* aktiviert ist.
    - **Allgemein** – Zeigt die Kategorie und den Status der Richtlinie an.
- **Registerkarte „Ausgelöste Ereignisse“** – Zeigt eine Liste von Ereignissen an, die von dieser Richtlinie ausgelöst wurden. Für jedes Ereignis werden Informationen über die an dem Ereignis beteiligten Assets und die Art des Ereignisses angezeigt. Die auf dieser Registerkarte angezeigten Informationen sind **identisch mit den Informationen, die im Bildschirm „Ereignisse“ angezeigt werden,** außer dass hier nur Ereignisse für die angegebene Richtlinie angezeigt werden. Eine Erläuterung der Ereignisinformationen finden Sie unter **Anzeigen von Ereignissen**. **Registerkarte „Ausschlüsse“** – Wenn Sie feststellen, dass eine Richtlinie Ereignisse für bestimmte Bedingungen generiert, die keine Sicherheitsbedrohung darstellen, können Sie diese Bedingungen von der Richtlinie *ausschließen* (d. h. keine Ereignisse mehr für diese bestimmten Bedingungen generieren). Dies erfolgt im Bildschirm „Ereignisse“, siehe **Erstellen von Richtlinienausschlüssen**. Die Registerkarte „Ausschlüsse“ zeigt alle Ausschlüsse, die auf diese Richtlinie angewendet wurden. Für jeden Ausschluss werden die spezifischen ausgeschlossenen Bedingungen angezeigt. Auf dieser Registerkarte können Sie einen Ausschluss löschen (was es dem System ermöglicht, die Generierung von Ereignissen für die angegebenen Bedingungen fortzusetzen).

Erstellen von Richtlinien

Sie können benutzerdefinierte Richtlinien basierend auf den spezifischen Überlegungen für Ihr ICS-Netzwerk erstellen. Sie können genau festlegen, auf welche Art von Ereignissen Ihre Mitarbeiter aufmerksam gemacht werden sollen und wie die Benachrichtigungen zugestellt werden. Sie haben völlige Flexibilität bei der Bestimmung, wie spezifisch oder weit gefasst Sie jede Richtlinie definieren möchten.

Richtlinien werden mithilfe von Gruppen definiert, die in Ihrem System konfiguriert wurden. Wenn die Dropdown-Liste für einen bestimmten Parameter nicht die spezifische Gruppierung anzeigt, auf die Sie die Richtlinie anwenden möchten, können Sie eine neue Gruppe entsprechend Ihren Anforderungen erstellen, siehe „Gruppen“.

Wenn Sie eine neue Richtlinie erstellen, wählen Sie zunächst die *Kategorie* und den *Typ* der Richtlinie aus, die Sie erstellen möchten. Der Assistent zum *Erstellen von Richtlinien* führt Sie durch den Einrichtungsvorgang. Jeder Richtlinientyp hat seinen eigenen Satz relevanter Parameter für Richtlinienbedingungen. Der Assistent zum Erstellen von Richtlinien zeigt Ihnen die relevanten Parameter für Richtlinienbedingungen für den ausgewählten Richtlinientyp an.

Für die Parameter *Quelle*, *Ziel* und *Zeitplan* können Sie festlegen, ob die angegebene Gruppe auf die Zulassungsliste oder die Sperrliste gesetzt werden soll.

- Wählen Sie **Einschließen** aus, um die angegebene Gruppe auf die Zulassungsliste zu setzen (d. h. sie in die Richtlinie aufzunehmen), ODER
- Wählen Sie **Ausschließen** aus, um die angegebene Gruppe auf die Sperrliste zu setzen (d. h. sie aus der Richtlinie herauszulassen).

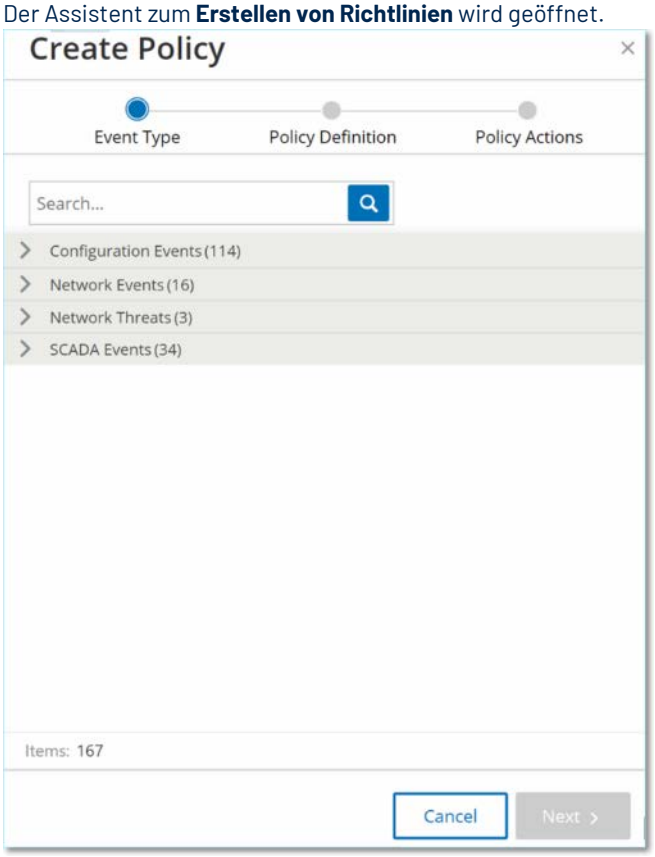
Für Asset-Gruppen- und Netzwerksegmentparameter (d. h. *Quelle, Ziel* und *betroffene Assets*) können Sie logische Operatoren (und/oder) verwenden, um die Richtlinie auf verschiedene Kombinationen oder Teilmengen Ihrer vordefinierten Gruppen anzuwenden. Wenn Sie beispielsweise möchten, dass eine Richtlinie auf jedes Gerät angewendet wird, das entweder ein *ICS-Gerät* oder ein *ICS-Server* ist, wählen Sie *ICS-Geräte* **oder** *ICS-Server* aus. Wenn Sie möchten, dass eine Richtlinie nur für *Controller* gilt, die sich in *Werk A* befinden, wählen Sie *Controller* **und** *Geräte Werk A* aus.

Wenn Sie eine neue Richtlinie mit ähnlichen Parametern wie eine vorhandene Richtlinie erstellen möchten, können Sie die ursprüngliche Richtlinie *duplizieren* und die erforderlichen Änderungen vornehmen, siehe Abschnitt **Duplizieren von Richtlinien**.

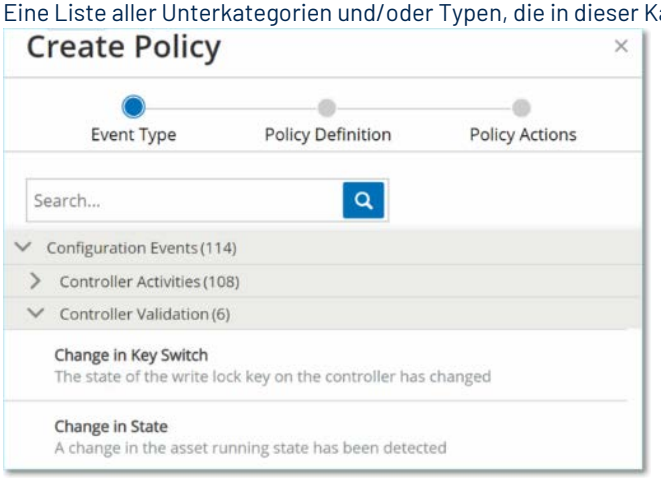
Wenn Sie nach dem Erstellen einer Richtlinie feststellen, dass die Richtlinie Ereignisse für Situationen generiert, die keine Aufmerksamkeit erfordern, können Sie bestimmte Bedingungen aus der Richtlinie ausschließen, siehe **Erstellen von Richtlinienausschlüssen**.

So erstellen Sie eine neue Richtlinie:

1. Klicken Sie im Bildschirm **Richtlinien** auf **Richtlinie erstellen**.
   Der Assistent zum **Erstellen von Richtlinien** wird geöffnet.

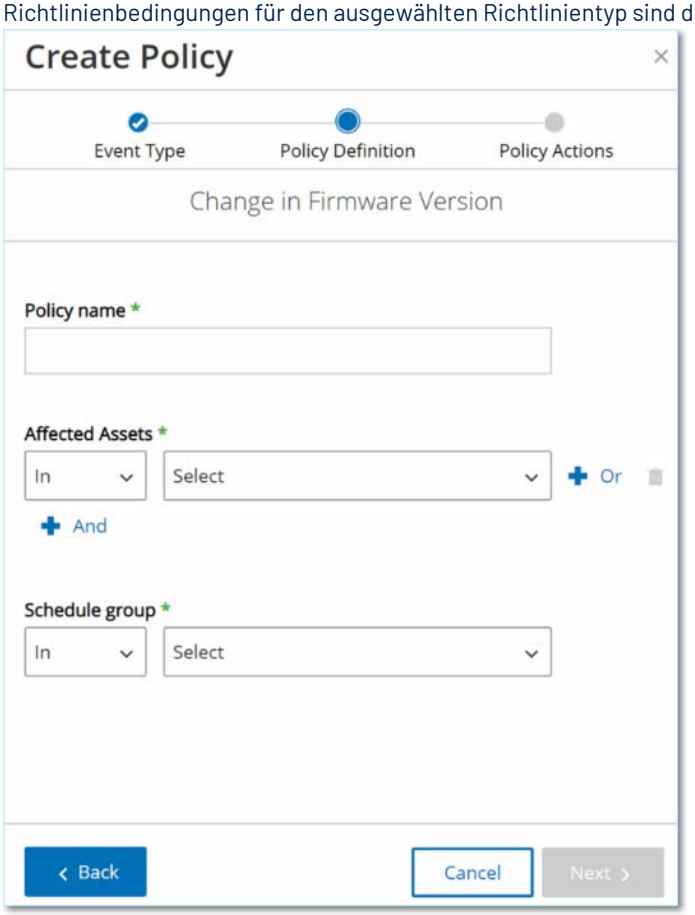


2. Klicken Sie auf eine **Richtlinienkategorie**, um die Unterkategorien und/oder Richtlinientypen anzuzeigen.
   Eine Liste aller Unterkategorien und/oder Typen, die in dieser Kategorie enthalten sind, wird angezeigt.



3. Wählen Sie einen Richtlinientyp aus.

4. Klicken Sie auf **Weiter**.
   Eine Reihe von Parametern zum Definieren der Richtlinie werden angezeigt. Alle relevanten Richtlinienbedingungen für den ausgewählten Richtlinientyp sind darin enthalten.

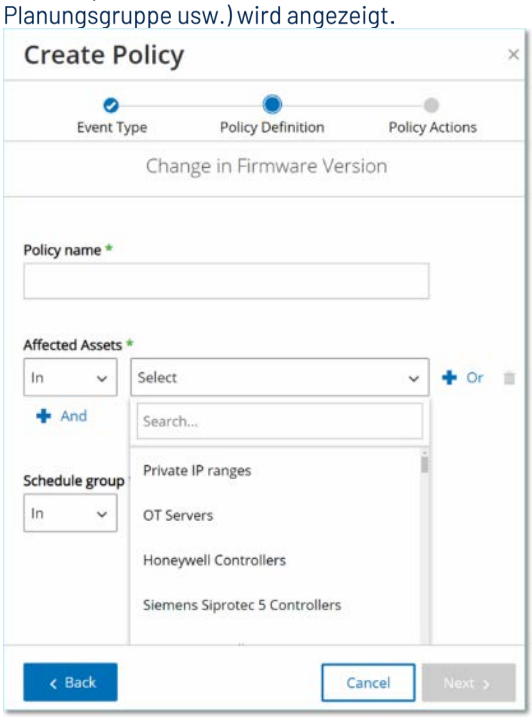


5. Geben Sie im Feld **Richtlinienname** einen Namen für diese Richtlinie ein.

> Wählen Sie einen Namen aus, der die spezifische Art des Ereignistyps beschreibt, den die Richtlinie erkennen soll.

6. Für jeden angezeigten Parameter:
   a. Wählen Sie gegebenenfalls **Einschließen** (Standard) aus, um das ausgewählte Element auf die Zulassungsliste zu setzen, oder **Ausschließen**, um das ausgewählte Element auf die Sperrliste zu setzen.

b. Klicken Sie auf **Auswählen**.
Eine Dropdown-Liste relevanter Elemente (z. B. Asset-Gruppe, Netzwerksegment, Port-Gruppe, Planungsgruppe usw.) wird angezeigt.



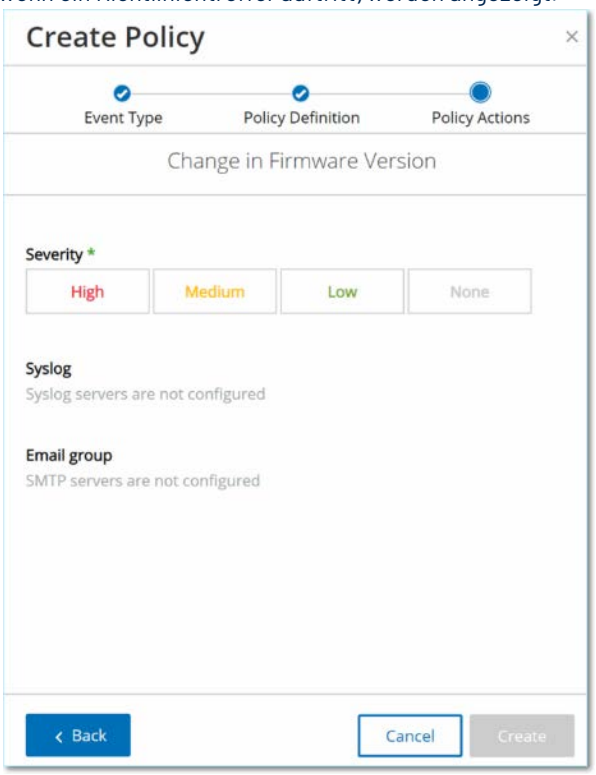
c. Wählen Sie das gewünschte Element aus.

> Wenn die genaue Gruppierung, auf die Sie die Richtlinie anwenden möchten, nicht vorhanden ist, können Sie eine neue Gruppe entsprechend Ihren Anforderungen erstellen, siehe **GRUPPEN**.

d. Wenn Sie für Asset-Parameter (d. h. *Quelle*, *Ziel* und *Betroffene Assets*) eine zusätzliche Asset-Gruppe/ein zusätzliches Netzwerksegment mit einer „Oder"-Bedingung hinzufügen möchten, klicken Sie auf die blaue **+ Oder** -Schaltfläche neben dem Feld und wählen Sie eine andere Asset-Gruppe/ein anderes Netzwerksegment aus.

e. Wenn Sie für Asset-Parameter (d. h. *Quelle*, *Ziel* und *Betroffene Assets*) eine zusätzliche Asset-Gruppe/ein zusätzliches Netzwerksegment mit einer „Und"-Bedingung hinzufügen möchten, klicken Sie auf die blaue **+ Und** -Schaltfläche unter dem Feld und wählen Sie eine andere Asset-Gruppe/ein anderes Netzwerksegment aus.

7. Wenn alle Felder ausgefüllt sind, klicken Sie auf **Weiter**.
   Eine Reihe von Parametern für Richtlinienaktionen (d. h. die Aktionen, die vom System ausgeführt werden, wenn ein Richtlinientreffer auftritt) werden angezeigt.



8. Klicken Sie im Abschnitt **Schweregrad** auf den gewünschten Schweregrad für diese Richtlinie.
9. Wenn Sie Ereignisprotokolle an einen oder mehrere Syslog-Server senden möchten, aktivieren Sie im Abschnitt **Syslog** das Kontrollkästchen neben jedem Server, an den Sie die Ereignisprotokolle senden möchten.

Informationen zum Hinzufügen eines Syslog-Servers finden Sie unter **Syslog-Server**.

10. Wenn Sie E-Mail-Benachrichtigungen über Ereignisse senden möchten, wählen Sie im Feld **E-Mail-Gruppe** aus der Dropdown-Liste die zu benachrichtigende E-Mail-Gruppe aus.

Informationen zum Hinzufügen eines SMTP-Servers finden Sie unter **SMTP-Server**.

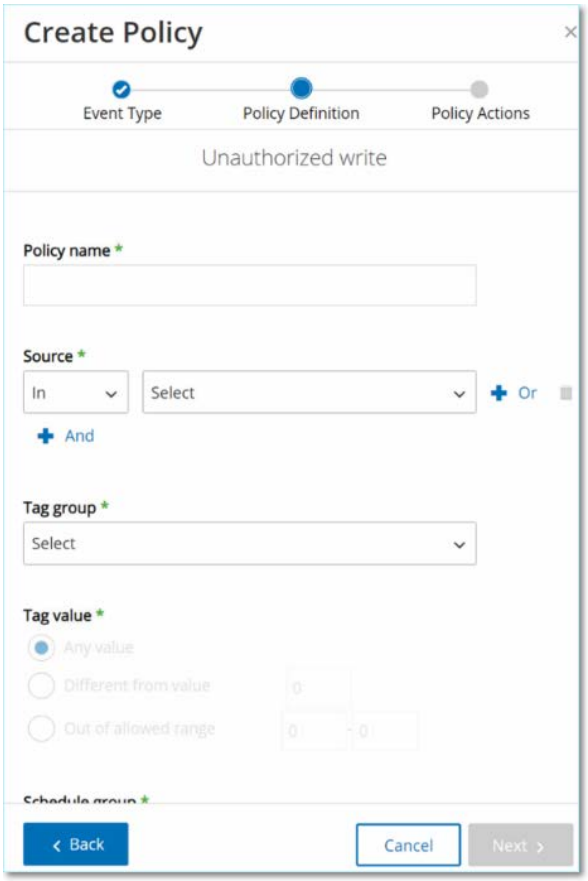
11. Im Abschnitt **Zusätzliche Aktionen**, wo die angegebene Aktion relevant ist:
    - Wenn Sie die Richtlinie nach dem ersten Richtlinientreffer deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Richtlinie nach erstem Treffer deaktivieren**. (Diese Aktion ist für einige Typen von Netzwerkereignisrichtlinien und einige Typen von SCADA-Ereignisrichtlinien relevant.)
    - Wenn Sie jedes Mal einen automatischen Snapshot des betroffenen Assets initiieren möchten, wenn ein Richtlinientreffer erkannt wird, aktivieren Sie das Kontrollkästchen **Snapshot nach Richtlinientreffer erstellen**. (Diese Aktion ist für einige Typen von Richtlinien für *Konfigurationsereignisse* relevant.)
12. Wenn alle Felder ausgefüllt sind, klicken Sie auf **Erstellen**.
    Die neue Richtlinie wird erstellt und automatisch aktiviert. Die Richtlinie wird in den Listen im Bildschirm „Richtlinien“ angezeigt.

Erstellen von Richtlinien für nicht autorisierte Schreibvorgänge

Dieser Richtlinientyp erkennt nicht autorisierte Schreibvorgänge für Controller-Tags. Die Richtliniendefinition umfasst die Angabe der relevanten Tag-Gruppen und des Schreibvorgangstyps, der einen Richtlinientreffer generiert.

So legen Sie die Richtliniendefinition für eine Richtlinie für nicht autorisierte Schreibvorgänge fest:

1. Erstellen Sie eine neue Richtlinie für nicht autorisierte Schreibvorgänge, wie unter **Erstellen von Richtlinien** beschrieben.



2. Wählen Sie im Abschnitt „Policy Definition“ im Feld **Tag-Gruppe** die Tag-Gruppe aus, für die diese Richtlinie gilt.
3. Wählen Sie im Abschnitt **Tag-Wert** die gewünschte Option aus, indem Sie auf das Optionsfeld klicken und die erforderlichen Felder ausfüllen. Verfügbare Optionen:
   - **Beliebiger Wert** – Wählen Sie diese Option aus, um Änderungen am Tag-Wert zu erkennen.
   - **Abweichend von Wert** – Wählen Sie diese Option aus, um einen anderen als den angegebenen Wert zu erkennen. Geben Sie den angegebenen Wert in das Feld neben dieser Auswahl ein.
   - **Außerhalb des zulässigen Bereichs** – Wählen Sie diese Option aus, um Werte außerhalb des angegebenen Bereichs zu erkennen. Geben Sie die Unter- und Obergrenze des zulässigen Bereichs in die entsprechenden Felder neben dieser Auswahl ein.

> Die Optionen *Abweichend von Wert* und *Außerhalb des zulässigen Bereichs* sind nur für Standard-Tag-Typen (z. B. Ganzzahl, Boolesch usw.) verfügbar, nicht jedoch für benutzerdefinierte Tags oder Zeichenfolgen.

4. Führen Sie die Verfahren zur Erstellung von Richtlinien wie unter **Erstellen von Richtlinien** beschrieben durch.

Andere Aktionen zu Richtlinien

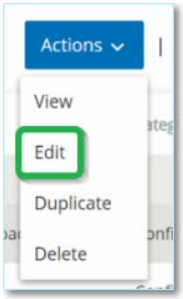
Bearbeiten von Richtlinien

Sie können die Konfiguration sowohl vordefinierter als auch benutzerdefinierter Richtlinien bearbeiten. Für die meisten Richtlinien können Sie sowohl die Parameter für die Richtliniendefinition (Richtlinienbedingungen) als auch die Parameter für Richtlinienaktionen anpassen. Für Intrusion Detection-Richtlinien können Sie nur die Parameter für die Richtlinienaktionen anpassen.

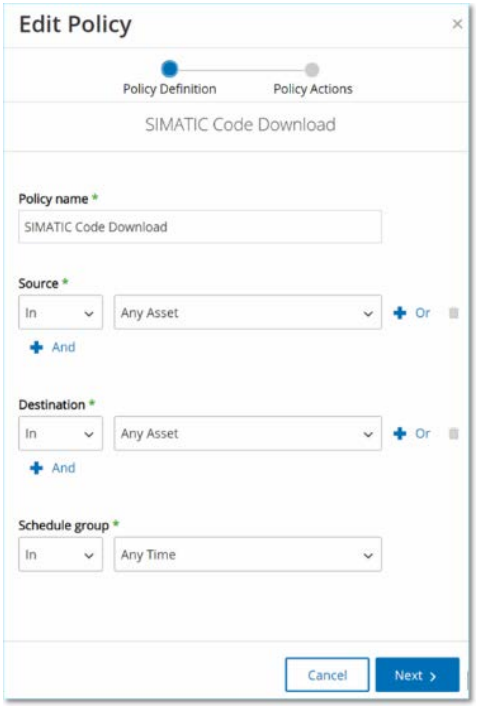
Außerdem können Sie die Parameter für Richtlinienaktionen für mehrere Richtlinien in einer Massenaktion bearbeiten.

So bearbeiten Sie eine Richtlinie:

1. Aktivieren Sie im Bildschirm **Richtlinien** das Kontrollkästchen neben der gewünschten Richtlinie.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **Bearbeiten** aus der Dropdown-Liste aus.



Der Bildschirm **Richtlinie bearbeiten** wird mit der aktuellen Konfiguration angezeigt.

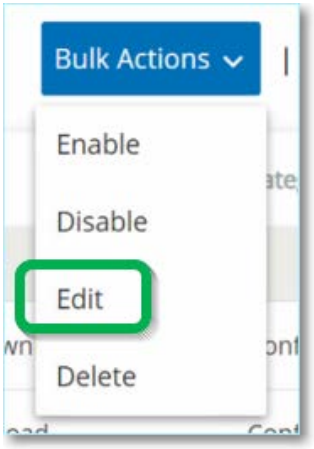


3. Passen Sie die Parameter der *Richtliniendefinition* wie gewünscht an.
4. Klicken Sie auf **Weiter**.
5. Passen Sie die Parameter der *Richtlinienaktionen* wie gewünscht an.
6. Klicken Sie auf **Speichern**.
   Die Richtlinie wird mit der neuen Konfiguration gespeichert.

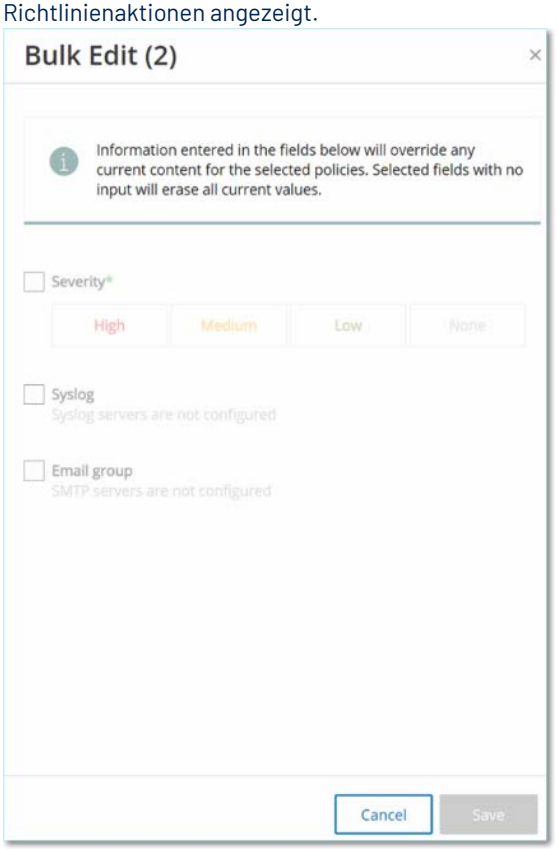
So bearbeiten Sie mehrere Richtlinien (Massenprozess):

1. Aktivieren Sie im Bildschirm **Richtlinien** das Kontrollkästchen neben zwei oder mehr Richtlinien.

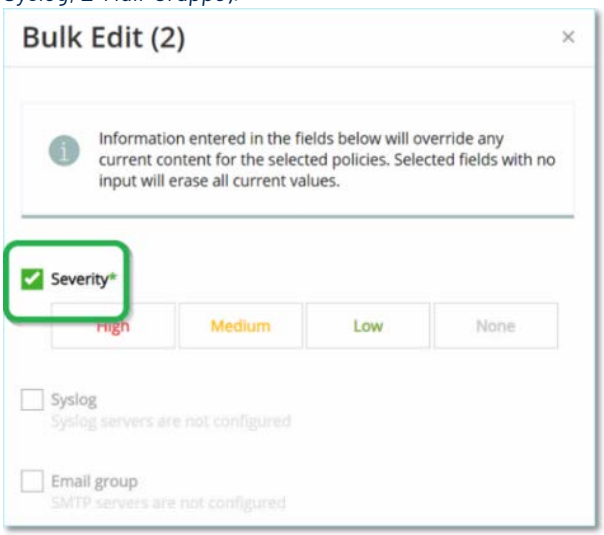
2. Klicken Sie auf das Menü **Massenaktionen** und wählen Sie **Bearbeiten** aus der Dropdown-Liste aus.



Der Bildschirm **Massenbearbeitung** wird mit den für die Massenbearbeitung verfügbaren Richtlinienaktionen angezeigt.



3. Aktivieren Sie das Kontrollkästchen neben jedem Parameter, den Sie bearbeiten möchten (*Schweregrad*, *Syslog*, *E-Mail-Gruppe*).



4. Stellen Sie jeden Parameter wie gewünscht ein.

> Durch die in die Felder für die Massenbearbeitung eingegebenen Informationen werden alle aktuellen Inhalte für die ausgewählten Richtlinien überschrieben. Wenn Sie das Kontrollkästchen neben einem Parameter aktivieren, aber keine Auswahl treffen, werden die aktuellen Werte für diesen Parameter gelöscht.

5. Klicken Sie auf **Speichern**.
   Die Richtlinien werden mit der neuen Konfiguration gespeichert.

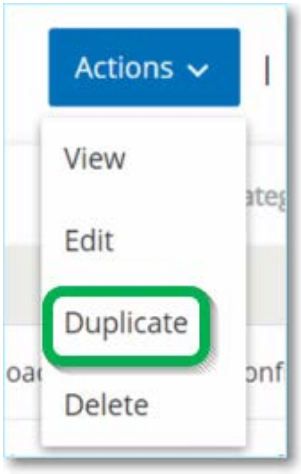
Duplizieren von Richtlinien

Sie können eine neue Richtlinie erstellen, die einer bestehenden Richtlinie ähnlich ist, indem Sie die ursprüngliche Richtlinie *duplizieren* und die gewünschten Anpassungen vornehmen. Sie können sowohl vordefinierte als auch benutzerdefinierte Richtlinien duplizieren (mit Ausnahme von Intrusion Detection-Richtlinien).

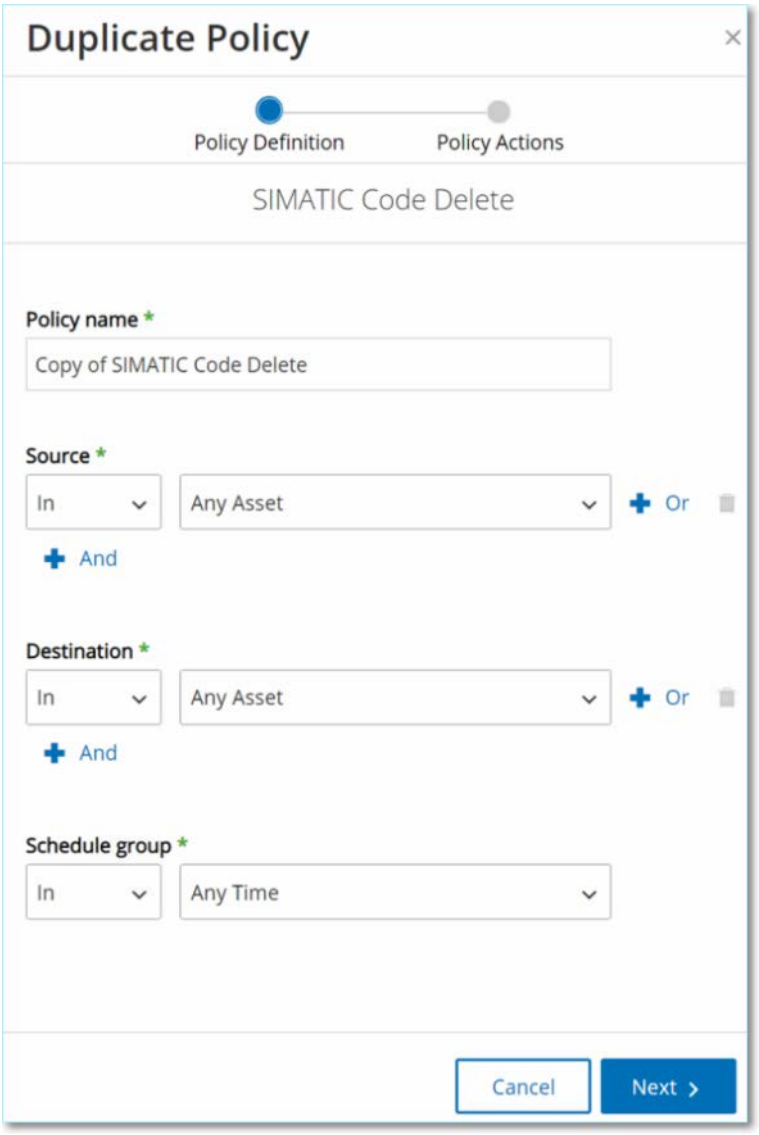
So duplizieren Sie eine Richtlinie:

1. Aktivieren Sie im Bildschirm **Richtlinien** das Kontrollkästchen neben der gewünschten Richtlinie.

2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **Duplizieren** aus der Dropdown-Liste aus.



Der Bildschirm **Richtlinie duplizieren** wird mit der aktuellen Konfiguration angezeigt und der Name ist standardmäßig auf „Kopie von <Name der ursprünglichen Richtlinie>" festgelegt.



3. Passen Sie die Parameter der *Richtliniendefinition* wie gewünscht an.
4. Klicken Sie auf **Weiter**.
5. Passen Sie die Parameter der *Richtlinienaktionen* wie gewünscht an.
6. Klicken Sie auf **Speichern**.
   Die Richtlinie wird mit der neuen Konfiguration gespeichert.

Löschen von Richtlinien

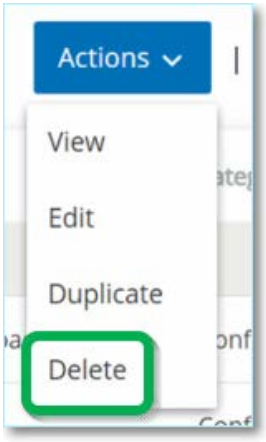
Sie können eine Richtlinie aus dem System löschen. Sie können sowohl vordefinierte als auch benutzerdefinierte Richtlinien löschen (mit Ausnahme von Intrusion Detection-Richtlinien, die nicht gelöscht werden können).

Sie können auch mehrere Richtlinien in einer Massenaktion löschen.

> Nachdem Sie eine Richtlinie aus dem System gelöscht haben, können Sie sie nicht erneut aktivieren. Eine Alternative besteht darin, den Status auf AUS umzuschalten, um sie vorübergehend zu deaktivieren. Dann können Sie sie später wieder aktivieren.

So löschen Sie eine Richtlinie:

1. Aktivieren Sie im Bildschirm **Richtlinien** das Kontrollkästchen neben der gewünschten Richtlinie.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **Löschen** aus der Dropdown-Liste aus.

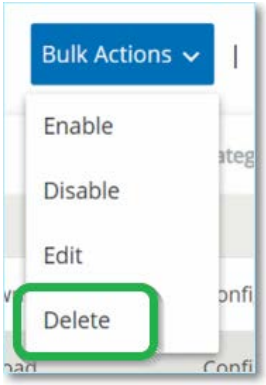


Ein Bestätigungsfenster wird angezeigt.

3. Klicken Sie auf **Löschen**.
Die Richtlinie wird aus dem System gelöscht.

So löschen Sie mehrere Richtlinien (Massenaktion):

1. Aktivieren Sie im Bildschirm **Richtlinien** das Kontrollkästchen neben jeder gewünschten Richtlinie.
2. Klicken Sie auf das Menü **Massenaktionen** und wählen Sie **Löschen** aus der Dropdown-Liste aus.



Ein Bestätigungsfenster wird angezeigt.

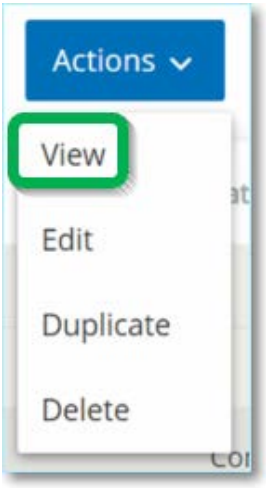
3. Klicken Sie auf **Löschen**.
Die Richtlinien werden aus dem System gelöscht.

Löschen von Richtlinienausschlüssen

Wenn Sie einen Ausschluss löschen möchten, der auf eine bestimmte Richtlinie angewendet wurde, ist dies im Bildschirm „Richtlinien“ möglich.

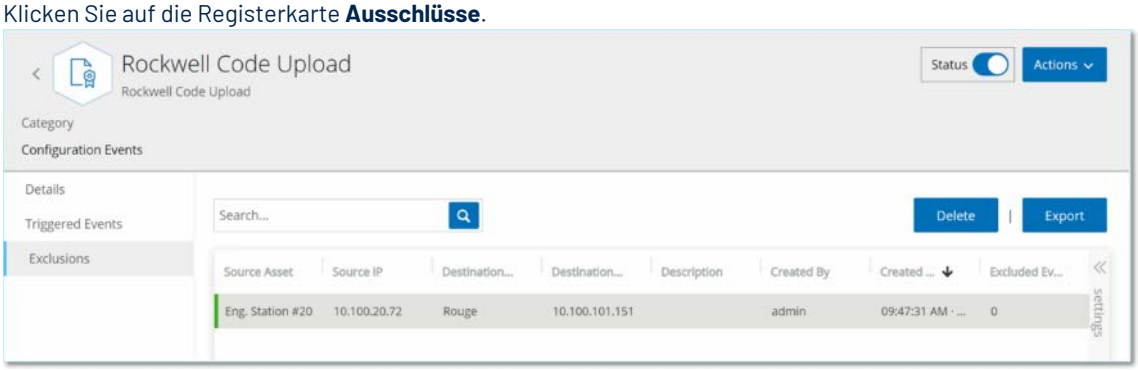
So löschen Sie einen Richtlinienausschluss:

1. Wählen Sie im Bildschirm **Richtlinien** die gewünschte Richtlinie aus.
2. Klicken Sie auf das Menü **Aktionen** und wählen Sie **Anzeigen** aus der Dropdown-Liste aus.



Alternativ können Sie das Menü „Aktionen“ aufrufen, indem Sie mit der rechten Maustaste auf die entsprechende Richtlinie klicken.

3. Klicken Sie auf die Registerkarte **Ausschlüsse**.



Eine Liste der Ausschlüsse wird angezeigt.

4. Wählen Sie den Richtlinienausschluss aus, den Sie löschen möchten.
5. Klicken Sie auf **Löschen**.
   Ein Bestätigungsfenster wird angezeigt.
6. Klicken Sie im Bestätigungsfenster auf **Löschen**.
   Der Ausschluss wird aus dem System gelöscht.

Gruppen

Gruppen sind die grundlegenden Bausteine, die zum Erstellen von Richtlinien verwendet werden. Bei der Konfiguration einer Richtlinie wird jede der Richtlinienbedingungen mittels Gruppen festgelegt und nicht durch einzelne Entitäten. Das System wird mit einigen vordefinierten Gruppen geliefert. Sie können auch Ihre eigenen benutzerdefinierten Gruppen erstellen. Daher wird empfohlen, die benötigten Gruppen im Voraus zu konfigurieren, um den Prozess der Bearbeitung und Erstellung von Richtlinien zu optimieren.

Richtlinienparameter können nur mithilfe von Gruppen festgelegt werden. Wenn Sie möchten, dass eine Richtlinie auf eine einzelne Entität angewendet wird, müssen Sie eine Gruppe konfigurieren, die nur diese Entität enthält.

Unter **Gruppen** können Sie alle Gruppen anzeigen, die in Ihrem System konfiguriert wurden. Die Gruppen sind in zwei Kategorien unterteilt:

- **Vordefinierte Gruppen** – Sind im System vorkonfiguriert und können nicht bearbeitet werden.
- **Benutzerdefinierte Gruppen** – Können vom Endbenutzer erstellt und bearbeitet werden.

Es gibt mehrere verschiedene Arten von Gruppen, von denen jede für die Konfiguration verschiedener Richtlinientypen verwendet wird. Jeder Gruppentyp wird auf einem separaten Bildschirm unter „Gruppen“ angezeigt. Die Gruppentypen sind:

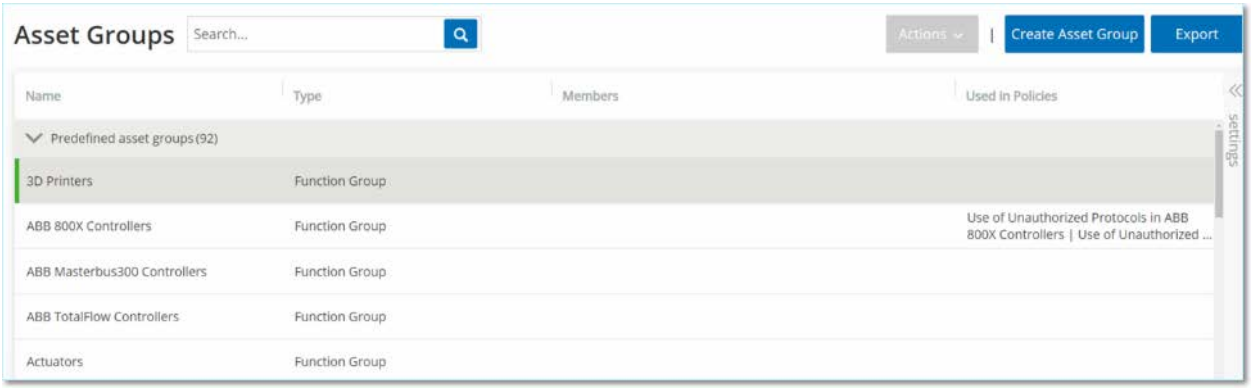
- **Asset-Gruppen** – Assets sind Hardwareentitäten im Netzwerk. Asset-Gruppen werden als Richtlinienbedingung für eine Vielzahl von Richtlinientypen verwendet.
- **Netzwerksegmente** – Die Netzwerksegmentierung ist eine Methode zur Erstellung von Gruppen zusammengehöriger Netzwerk-Assets. Sie hilft dabei, eine Gruppe von Assets logisch von einer anderen zu trennen.
- **E-Mail-Gruppen** – Gruppen von E-Mails, die benachrichtigt werden, wenn ein Richtlinienereignis eintritt. Wird für alle Richtlinientypen verwendet.
- **Port-Gruppen** – Gruppen von Ports, die von Assets im Netzwerk verwendet werden. Wird für Richtlinien verwendet, die offene Ports identifizieren.
- **Protokollgruppen** – Gruppen von Protokollen, mit denen Konversationen zwischen Assets im Netzwerk geführt werden. Wird als Richtlinienbedingung für Netzwerkereignisse verwendet.
- **Planungsgruppen** – Planungsgruppen sind Zeitbereiche, die verwendet werden, um zu konfigurieren, zu welcher Zeit das angegebene Ereignis eintreten muss, um die Richtlinienbedingungen zu erfüllen.
- **Tag-Gruppen** – Tags sind Parameter in Controllern, die spezifische Betriebsdaten enthalten. Tag-Gruppen werden als Richtlinienbedingung für SCADA-Ereignisse verwendet.
- **Regelgruppen** – Regelgruppen bestehen aus einer Gruppe verwandter Regeln, die durch ihre Suricata-Signatur-IDs (SIDs) identifiziert werden. Diese Gruppen werden als Richtlinienbedingung zum Definieren von Intrusion Detection-Richtlinien verwendet.

Das Verfahren zum Erstellen der einzelnen Gruppentypen wird in den folgenden Abschnitten beschrieben. Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe **Aktionen für Gruppen**.

Asset-Gruppen

Assets sind Hardwareentitäten im Netzwerk. Durch Gruppieren ähnlicher Assets können Sie Richtlinien erstellen, die für alle Assets in der Gruppe gelten. Beispielsweise könnten Sie eine Asset-Gruppe *Controller* verwenden, um eine Richtlinie zu erstellen, die bei Firmware-Änderungen an einem Controller warnt. Asset-Gruppen werden als Richtlinienbedingung für eine Vielzahl von Richtlinientypen verwendet. Asset-Gruppen können verwendet werden, um das *Quell*-Asset, das *Ziel*-Asset oder das *betroffene Asset* für verschiedene Richtlinientypen anzugeben.

Anzeigen von Asset-Gruppen



Der Bildschirm **Asset-Gruppen** zeigt alle Asset-Gruppen, die derzeit im System konfiguriert sind. Die Registerkarte *Vordefiniert* enthält Gruppen, die in das System integriert sind und nicht bearbeitet, dupliziert oder gelöscht werden können. Die Registerkarte *Benutzerdefiniert* enthält benutzerdefinierte Gruppen, die vom Benutzer erstellt wurden. Diese Gruppen können bearbeitet, dupliziert oder gelöscht werden.

Die auf diesem Bildschirm angezeigten Informationen werden in der folgenden Tabelle beschrieben.

Parameter	Beschreibung
Status	Zeigt an, ob die Richtlinie aktiviert oder deaktiviert ist. Wenn die Richtlinie vom System automatisch deaktiviert wurde, weil sie zu viele Ereignisse generiert hat, wird ein Warnsymbol angezeigt. Schalten Sie den Status-Schalter um, um eine Richtlinie zu aktivieren/deaktivieren.
Name	Der Name der Richtlinie.
Schweregrad	Der Schweregrad des Ereignisses. Mögliche Werte sind: Kein, Gering, Mittel oder Hoch. Eine Beschreibung der Schweregrade finden Sie im Abschnitt **Schweregradstufen**.
Ereignistyp	Der spezifische Ereignistyp, der diese Ereignisrichtlinie auslöst.
Kategorie	Die allgemeine Kategorie für den Ereignistyp, der diese Ereignisrichtlinie auslöst. Mögliche Werte sind: Konfiguration, SCADA, Netzwerkbedrohungen oder Netzwerkereignis. Eine Erläuterung der verschiedenen Kategorien finden Sie unter **Richtlinienkategorien und Unterkategorien**.
Quelle	Eine Richtlinienbedingung. Die Quell-Asset-Gruppe (d. h. das Asset, das die Aktivität initiiert hat), für die die Richtlinie gilt.
Name	Der Name, der zur Identifizierung der Gruppe dient.

Parameter	Beschreibung
Typ	Zeigt den Gruppentyp an. Optionen sind: • Funktion – Eine vordefinierte Asset-Gruppe, die erstellt wurde, um eine bestimmte Funktion zu erfüllen. • Asset-Liste – Angegebene Assets sind in der Gruppe enthalten. • IP-Liste – Assets mit der angegebenen IP-Adresse. • IP-Bereich – Assets innerhalb des angegebenen Bereichs von IP-Adressen.
Mitglieder	Zeigt die Liste der Assets an, die in dieser Gruppe enthalten sind. Für Funktionsgruppen wird kein Wert angezeigt. **Hinweis:** Wenn in dieser Zeile nicht genug Platz ist, um alle Assets anzuzeigen, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > Mitglieder**.
In Richtlinien verwendet	Zeigt den Namen jeder Richtlinie an, die diese Asset-Gruppe in ihrer Konfiguration verwendet. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen die Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Die Verfahren zum Erstellen verschiedener Typen von Asset-Gruppen werden im folgenden Abschnitt beschrieben. Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe **Aktionen für Gruppen**.

Erstellen von Asset-Gruppen

Sie können benutzerdefinierte Asset-Gruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Indem Sie ähnliche Assets in Gruppen zusammenfassen, können Sie Richtlinien erstellen, die für alle Assets in der Gruppe gelten.

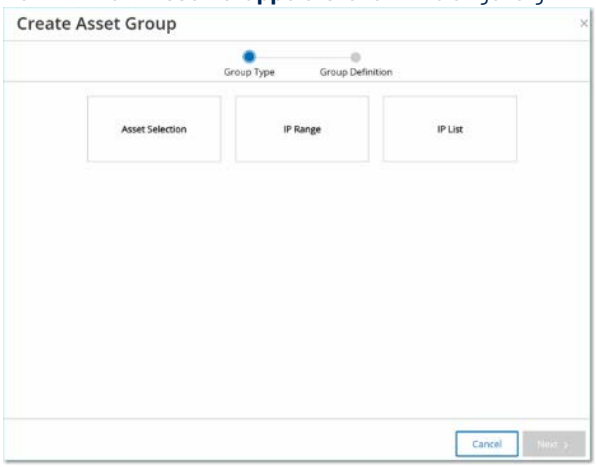
Es gibt drei Arten von benutzerdefinierten Asset-Gruppen:

- **Asset-Liste** – Angabe der Assets, die in der Gruppe enthalten sind.
- **IP-Liste** – Angabe der IP-Adressen der Assets, die in der Gruppe enthalten sind.
- **IP-Bereich** – Angabe des Bereichs der IP-Adressen der Assets, die in der Gruppe enthalten sind.

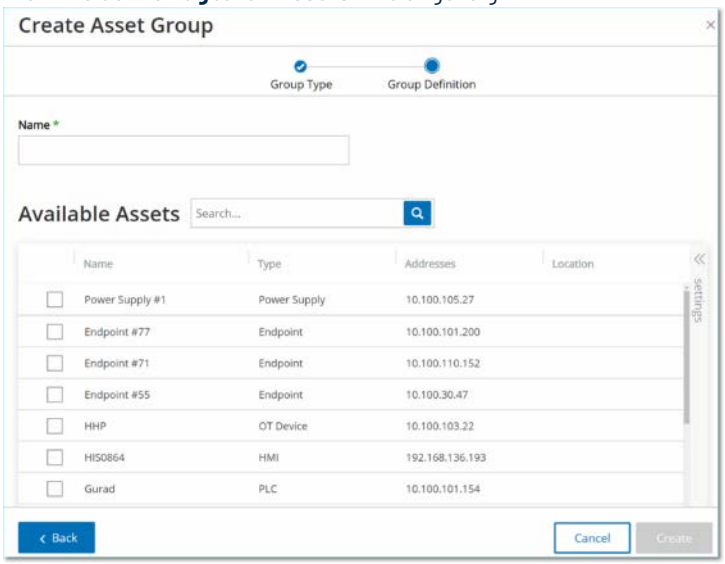
Es gibt verschiedene Verfahren zum Erstellen der einzelnen Arten von Asset-Gruppen.

So erstellen Sie eine Asset-Gruppe vom Typ „Asset-Auswahl“:

1. Wählen Sie unter „Gruppen“ die Option „Asset-Gruppen“ aus.
2. Klicken Sie auf „Asset-Gruppe erstellen“.
   Der Assistent **Asset-Gruppe erstellen** wird angezeigt.



3. Klicken Sie auf „Asset-Auswahl“.
4. Klicken Sie auf **Weiter**.
   Die Liste der **verfügbaren Assets** wird angezeigt.

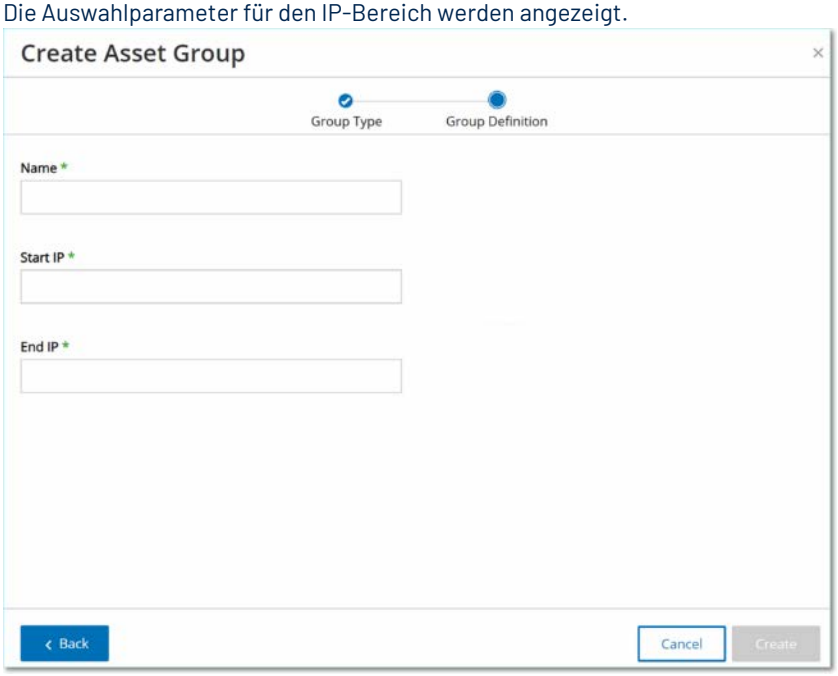


5. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
   Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.
6. Aktivieren Sie das Kontrollkästchen neben jedem Asset, das Sie in die Gruppe aufnehmen möchten.
7. Wenn Sie Ihre Auswahl abgeschlossen haben, klicken Sie auf **Erstellen**.
   Die neue Asset-Gruppe wird erstellt und im Bildschirm „Asset-Gruppen“ angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

So erstellen Sie eine Asset-Gruppe vom Typ „IP-Bereich“:

1. Wählen Sie unter „Gruppen“ die Option „Asset-Gruppen“ aus.
2. Klicken Sie auf „Asset-Gruppe erstellen“.
   Der Assistent „Asset-Gruppe erstellen“ wird angezeigt.

3. Klicken Sie auf **IP-Bereich**.
4. Klicken Sie auf **Weiter**.
   Die Auswahlparameter für den IP-Bereich werden angezeigt.



5. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
   Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.
6. Geben Sie im Feld **Start-IP** die IP-Adresse am Anfang des Bereichs ein, den Sie einschließen möchten.
7. Geben Sie im Feld **End-IP** die IP-Adresse am Ende des Bereichs ein, den Sie einschließen möchten.
8. Klicken Sie auf **Erstellen**.
   Die neue Asset-Gruppe wird erstellt und im Bildschirm „Asset-Gruppen“ angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

So erstellen Sie eine Asset-Gruppe vom Typ „IP-Liste“:

1. Wählen Sie unter „Gruppen“ die Option „Asset-Gruppen“ aus.

2. Klicken Sie auf „Asset-Gruppe erstellen“.
   Der Assistent „Asset-Gruppe erstellen“ wird angezeigt.

3. Klicken Sie auf **IP-Liste**.
4. Klicken Sie auf **Weiter**.
   Die Parameter für die IP-Liste werden angezeigt.

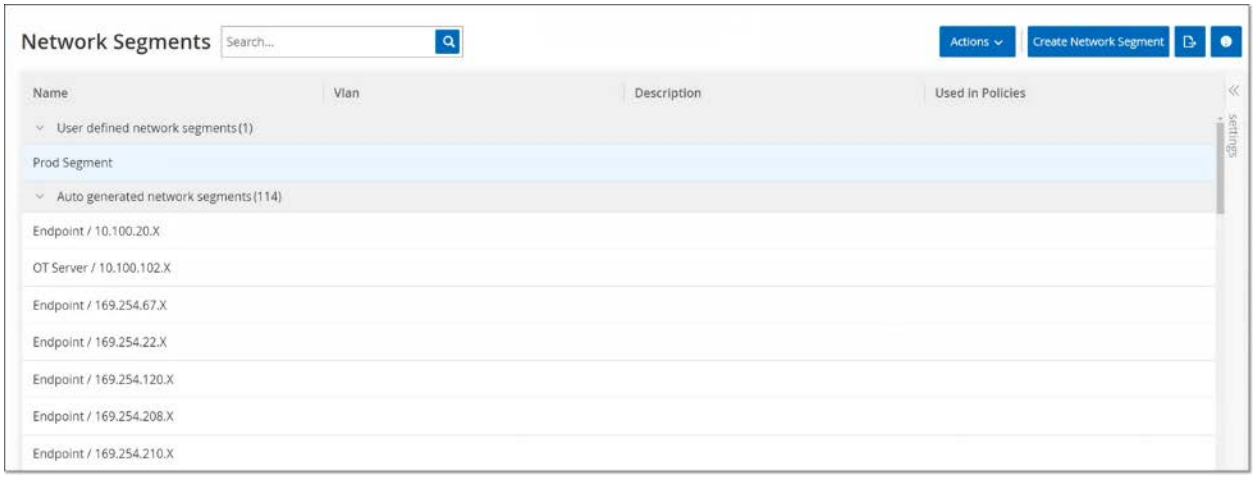
5. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
   Wählen Sie einen Namen, der ein gemeinsames Element beschreibt, das die in der Gruppe enthaltenen Assets kategorisiert.
6. Geben Sie im Feld **IP-Liste** eine IP-Adresse oder ein Subnetz ein, die bzw. das in die Gruppe aufgenommen werden soll.
7. Um der Gruppe weitere Assets hinzuzufügen, geben Sie jede zusätzliche IP-Adresse oder jedes zusätzliche Subnetz in einer separaten Zeile ein.
8. Klicken Sie auf **Erstellen**.
   Die neue Asset-Gruppe wird erstellt und im Bildschirm „Asset-Gruppen“ angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

Netzwerksegmente

Die Netzwerksegmentierung ist eine Methode zur Erstellung von Gruppen zusammengehöriger Netzwerk-Assets. Sie hilft dabei, eine Gruppe von Assets logisch von einer anderen zu trennen. Tenable.ot weist automatisch jede IP-Adresse, die mit einem Asset in Ihrem Netzwerk verknüpft ist, einem Netzwerksegment zu. (Bei Assets mit mehr als einer IP-Adresse ist jede IP einem Netzwerksegment zugeordnet.) Jedes automatisch generierte Segment enthält alle Assets einer bestimmten Kategorie (Controller, OT-Server, Netzwerkgeräte usw.), die IPs mit derselben Netzwerkadresse der Klasse C haben (d. h. die IPs haben die gleichen ersten 24 Bit).

Sie können benutzerdefinierte Netzwerksegmente erstellen und angeben, welche Assets diesem Segment zugewiesen werden. In den Inventar-Bildschirmen gibt es eine Spalte, die das Netzwerksegment für jedes Asset anzeigt, sodass Sie Ihre Assets einfach nach Netzwerksegment sortieren und filtern können.

Anzeigen von Netzwerksegmenten



Der Bildschirm „Netzwerksegmente" zeigt alle Netzwerksegmente, die derzeit im System konfiguriert sind. Die Registerkarte *Automatisch generiert* enthält Netzwerksegmente, die automatisch vom System generiert werden. Die Registerkarte *Benutzerdefiniert* enthält benutzerdefinierte Netzwerksegmente, die vom Benutzer erstellt wurden.

Die Informationen in diesem Bildschirm werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Name	Der Name, der zur Identifizierung des Netzwerksegments verwendet wird.
VLAN	Die VLAN-Nummer des Netzwerksegments. (Optional)
Beschreibung	Eine Beschreibung des Netzwerksegments. (Optional)
In Richtlinien verwendet	Zeigt die Namen der Richtlinien an, die für dieses Netzwerksegment gelten. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen das Netzwerksegment verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Das Verfahren zum Erstellen von Netzwerksegmenten wird im folgenden Abschnitt beschrieben. Darüber hinaus können Sie ein vorhandenes Netzwerksegment anzeigen, bearbeiten, duplizieren oder löschen, siehe **Aktionen für Gruppen**.

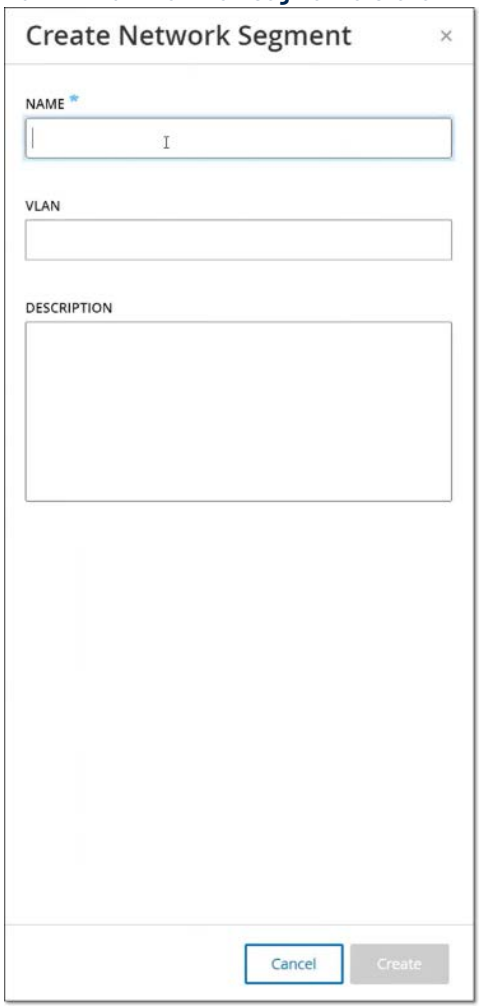
Erstellen von Netzwerksegmenten

Sie können Netzwerksegmente erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Indem Sie zusammengehörige Netzwerk-Assets gruppieren, ermöglichen Sie die Erstellung von Richtlinien, die den akzeptablen Netzwerk-Traffic für Assets in diesem Segment definieren.

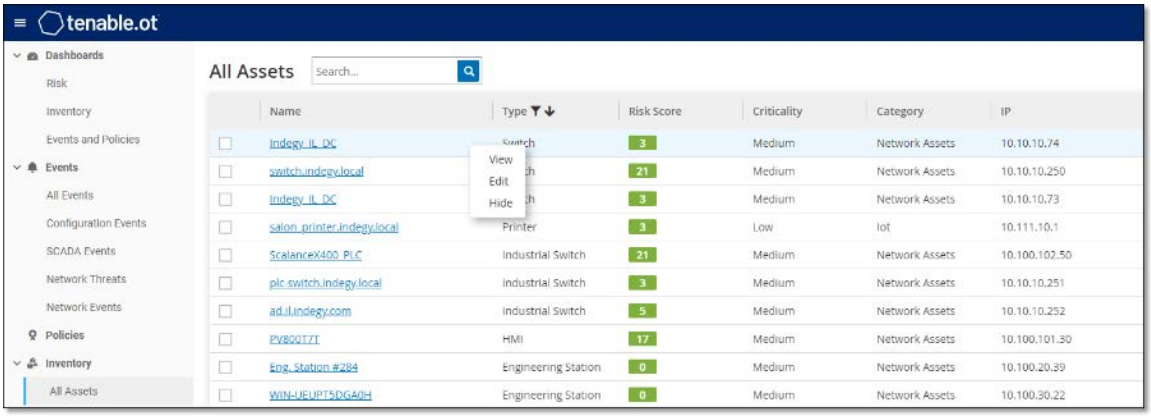
➡ So erstellen Sie ein Netzwerksegment:

1. Wählen Sie unter **Gruppen** die Option **Netzwerksegmente** aus.
2. Klicken Sie auf **Netzwerksegment erstellen**.

Der Assistent **Netzwerksegment erstellen** wird angezeigt.

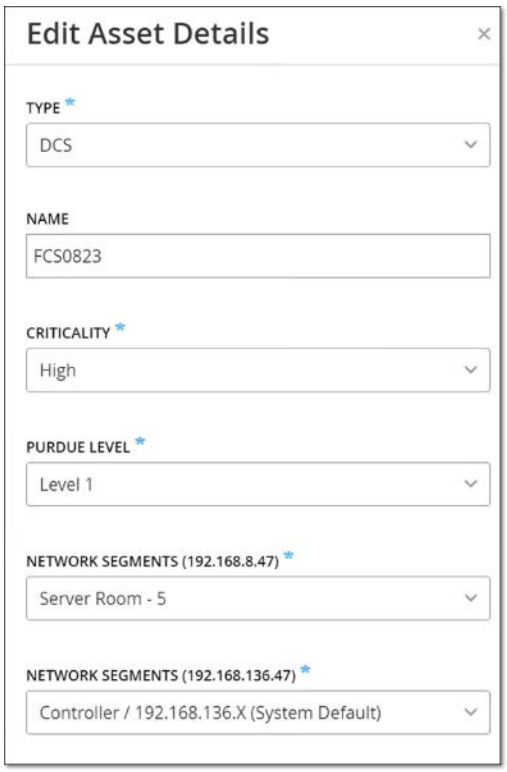


3. Geben Sie im Feld **Name** einen Namen für das Netzwerksegment ein.
4. Geben Sie im Feld **VLAN** eine VLAN-Nummer für das Netzwerksegment ein. (Optional)
5. Geben Sie im Feld **Beschreibung** eine Beschreibung des Netzwerksegments ein. (Optional)
6. Klicken Sie auf **Erstellen**.
   Das neue Netzwerksegment wird erstellt und in der Liste der Netzwerksegmente angezeigt.
7. Wählen Sie unter **Inventar** die Option **Alle Assets** aus.
8. Klicken Sie mit der rechten Maustaste auf das Asset, das Sie dem neu erstellten Netzwerksegment zuweisen möchten, und wählen Sie **Bearbeiten** aus.



Das Fenster **Asset-Details bearbeiten** wird geöffnet.

9. Wählen Sie im Feld **Netzwerksegmente** das entsprechende Netzwerksegment aus der Dropdown-Liste aus.



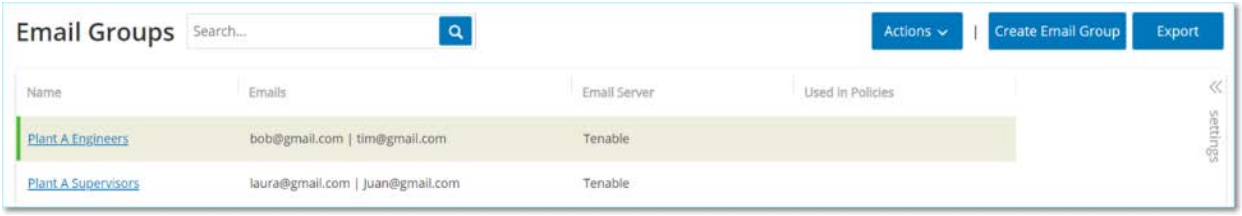
Einigen Assets ist mehr als eine IP-Adresse zugeordnet und Sie können für jede das entsprechende Netzwerksegment auswählen.

Das Netzwerksegment wird dem Asset zugewiesen und in der Spalte „Netzwerksegment“ angezeigt. Sie können dieses Netzwerksegment jetzt beim Konfigurieren von Richtlinien verwenden.

E-Mail-Gruppen

E-Mail-Gruppen sind Gruppen von E-Mail-Adressen relevanter Parteien. E-Mail-Gruppen werden verwendet, um Empfänger für Ereignis-Benachrichtigungen anzugeben, die durch bestimmte Richtlinien ausgelöst werden. Eine Gruppierung nach Rolle, Abteilung usw. ermöglicht es Ihnen beispielsweise, die Benachrichtigungen für bestimmte Richtlinienereignisse an die relevanten Parteien zu senden.

Anzeigen von E-Mail-Gruppen



Der Bildschirm „E-Mail-Gruppen" zeigt alle E-Mail-Gruppen, die derzeit im System konfiguriert sind.

Die Informationen in diesem Bildschirm werden in der folgenden Tabelle beschrieben:

Sie können zusätzliche Details zu einer bestimmten Gruppe anzeigen, indem Sie die Gruppe auswählen und auf **Tabellenaktionen** > **Anzeigen** klicken.

Parameter	Beschreibung
Name	Der Name, der zur Identifizierung der Gruppe dient.
E-Mails	Die Liste der in der Gruppe enthaltenen E-Mails. **Hinweis:** Wenn nicht genügend Platz vorhanden ist, um alle Mitglieder der Gruppe anzuzeigen, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > Mitglieder**.
E-Mail-Server	Der dem SMTP-Server zugewiesene Name, der zum Versenden der E-Mails an diese Gruppe verwendet wird.
In Richtlinien verwendet	Zeigt die Namen der Richtlinien an, für die Benachrichtigungen an diese Gruppe gesendet werden. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen die Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Das Verfahren zum Erstellen einer E-Mail-Gruppe wird im folgenden Abschnitt beschrieben. Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe **Aktionen für Gruppen**.

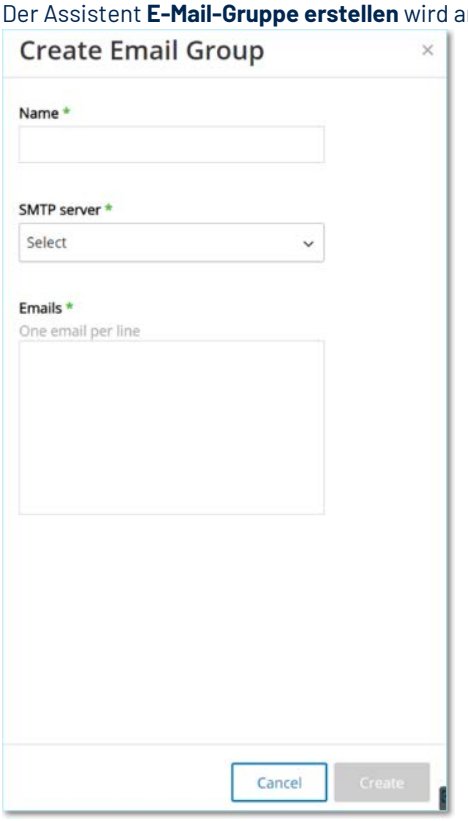
Erstellen von E-Mail-Gruppen

Sie können E-Mail-Gruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Indem Sie zusammengehörige E-Mail-Adressen gruppieren, legen Sie fest, dass Benachrichtigungen zu Richtlinienereignissen an alle relevanten Mitarbeiter gesendet werden.

Sie können jeder Richtlinie nur eine E-Mail-Gruppe zuweisen. Daher ist es sinnvoll, sowohl weit gefasste, allgemeine Gruppen als auch spezifische, begrenzte Gruppen zu erstellen, damit Sie jeder Richtlinie die entsprechende Gruppe zuweisen können.

So erstellen Sie eine E-Mail-Gruppe:

1. Wählen Sie unter **Gruppen** die Option **E-Mail-Gruppen** aus.
2. Klicken Sie auf **E-Mail-Gruppe erstellen**.
   Der Assistent **E-Mail-Gruppe erstellen** wird angezeigt.



3. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
4. Wählen Sie im Feld **SMTP-Server** aus der Dropdown-Liste den Server aus, der zum Versenden der E-Mail-Benachrichtigungen verwendet wird.

Wenn im System kein SMTP-Server konfiguriert wurde, müssen Sie zuerst einen Server konfigurieren, bevor Sie eine E-Mail-Gruppe erstellen können, siehe **SMTP-Server**.

5. Geben Sie im Feld **E-Mails** die E-Mail-Adresse jedes Mitglieds der Gruppe in einer separaten Zeile ein.
6. Klicken Sie auf **Erstellen**.
   Die neue E-Mail-Gruppe wird erstellt und im Bildschirm „E-Mail-Gruppen“ angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

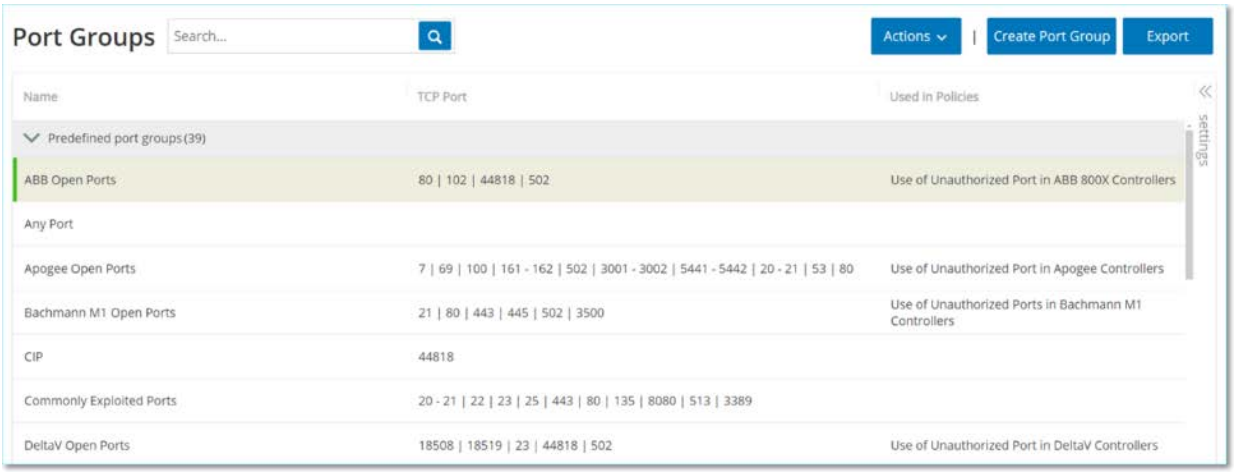
Port-Gruppen

Port-Gruppen sind Gruppen von Ports, die von Assets im Netzwerk verwendet werden. Port-Gruppen werden als Richtlinienbedingung zum Definieren von Netzwerkereignis-Richtlinien für **offene Ports** verwendet, die offene Ports im Netzwerk erkennen.

Die Registerkarte *Vordefiniert* zeigt die im System vordefinierten Portgruppen. Diese Gruppen umfassen Ports, von denen erwartet wird, dass sie auf Controllern eines bestimmten Anbieters offen sind. Beispielsweise umfasst die Gruppe „Siemens-SPS – Offene Ports“: 20, 21, 80, 102, 443 und 502. Dies ermöglicht die Konfiguration von Richtlinien, die offene Ports erkennen, von denen nicht erwartet wird, dass sie für Controller von diesem Anbieter geöffnet sind. Diese Gruppen können nicht bearbeitet oder gelöscht werden, sie können aber dupliziert werden.

Die Registerkarte *Benutzerdefiniert* enthält benutzerdefinierte Gruppen, die vom Benutzer erstellt wurden. Diese Gruppen können bearbeitet, dupliziert oder gelöscht werden.

Anzeigen von Port-Gruppen



Die Informationen in diesem Bildschirm werden in der folgenden Tabelle beschrieben:

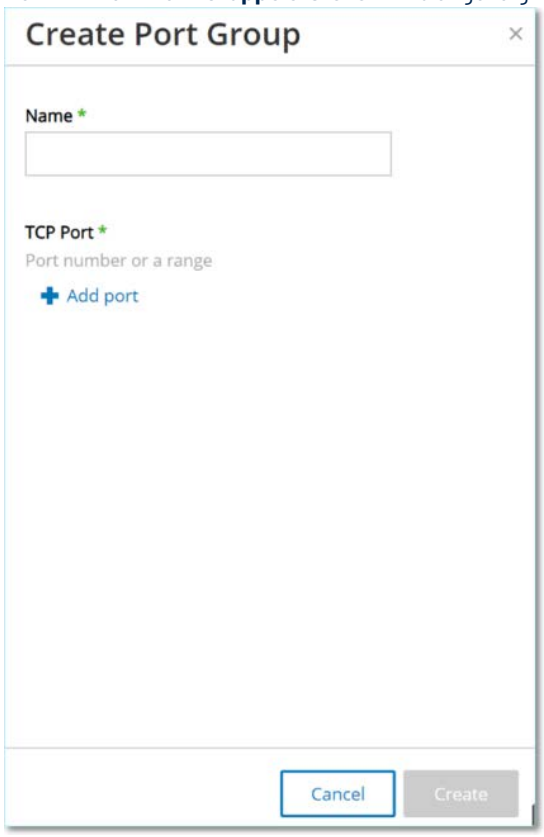
Parameter	Beschreibung
Name	Der Name, der zur Identifizierung der Gruppe dient.
TCP-Ports	Die Liste der Ports und/oder Port-Bereiche, die in der Gruppe enthalten sind. **Hinweis:** Wenn nicht genügend Platz vorhanden ist, um alle Mitglieder der Gruppe anzuzeigen, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > Mitglieder**.
In Richtlinien verwendet	Zeigt den Namen jeder Richtlinie an, die diese Port-Gruppe in ihrer Konfiguration verwendet. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Erstellen von Port-Gruppen

Sie können benutzerdefinierte Port-Gruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Durch Gruppieren ähnlicher Ports ermöglichen Sie die Erstellung von Richtlinien, die vor offenen Ports warnen, die ein besonderes Sicherheitsrisiko darstellen.

So erstellen Sie eine Port-Gruppe:

1. Wählen Sie unter **Gruppen** die Option **Port-Gruppen** aus.
2. Klicken Sie auf **Port-Gruppe erstellen**.
   Der Assistent **Port-Gruppe erstellen** wird angezeigt.



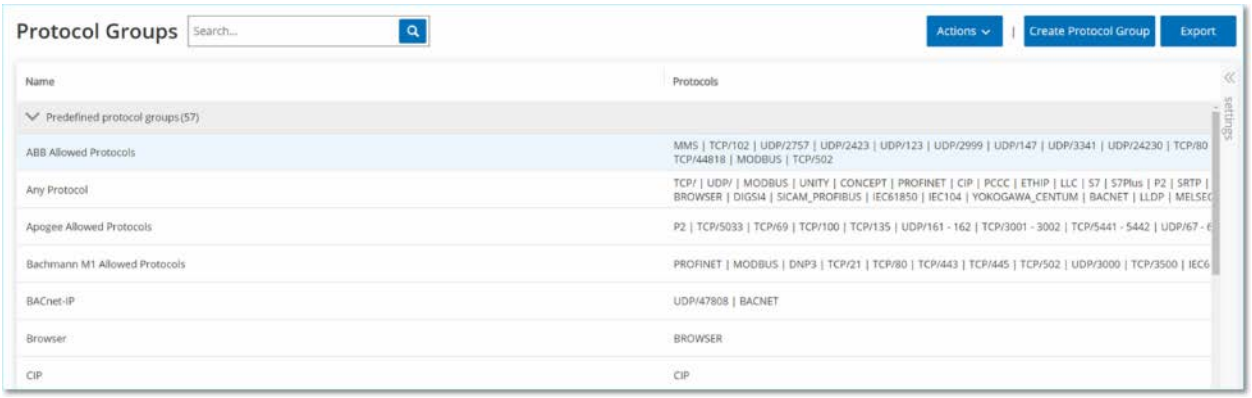
3. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
4. Geben Sie im Feld **TCP-Port** einen einzelnen Port oder eine Reihe von Ports ein, die in die Gruppe aufgenommen werden sollen.
5. Wenn Sie der Gruppe weitere Ports hinzufügen möchten, gehen Sie für jeden zusätzlichen Port wie folgt vor.
   a. Klicken Sie auf **+ Port hinzufügen**.
      Ein neues Port-Auswahlfeld wird angezeigt.
   b. Geben Sie im neuen Feld **Port-Nummer** einen einzelnen Port oder eine Reihe von Ports ein, die in die Gruppe aufgenommen werden sollen.
6. Klicken Sie auf **Erstellen**.
   Die neue Port-Gruppe wird erstellt und in der Liste der Port-Gruppen angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

Protokollgruppen

Protokollgruppen sind Gruppen von Protokollen, mit denen Konversationen zwischen Assets im Netzwerk geführt werden. Protokollgruppen werden als Richtlinienbedingung für Netzwerkrichtlinien verwendet und definieren, welche Protokolle, die zwischen bestimmten Assets verwendet werden, eine Richtlinie auslösen.

Tenable.ot enthält eine Reihe vordefinierter Protokollgruppen, die verwandte Protokolle umfassen. Diese Gruppen stehen zur Verwendung in Richtlinien zur Verfügung. Diese Gruppen können nicht bearbeitet oder gelöscht werden. Protokolle können danach gruppiert werden, welche Protokolle von einem bestimmten Anbieter zugelassen werden. Zu den von Schneider zugelassenen Protokollen gehören beispielsweise: TCP:80 (HTTP), TCP:21 (FTP), Modbus, Modbus_UMAS, Modbus_MODICON, TCP:44818 (CIP), UDP:69 (TFTP), UDP:161 (SNMP), UDP:162 (SNMP), UDP:44818, UDP:67-68 (DHCP). Sie können auch nach Protokolltyp (z. B. Modbus, PROFINET, CIP usw.) gruppiert werden. Sie können außerdem Ihre eigenen benutzerdefinierten Protokollgruppen erstellen.

Anzeigen von Protokollgruppen



Der Bildschirm **Protokollgruppen** zeigt alle Protokollgruppen an, die derzeit im System konfiguriert sind. Die Registerkarte *Vordefiniert* zeigt die in das System integrierten Gruppen an. Diese Gruppen können nicht bearbeitet oder gelöscht werden, sie können aber dupliziert werden. Die Registerkarte *Benutzerdefiniert* zeigt benutzerdefinierte Gruppen an, die vom Benutzer erstellt wurden. Diese Gruppen können bearbeitet, dupliziert oder gelöscht werden.

Die auf diesem Bildschirm angezeigten Informationen werden in der folgenden Tabelle beschrieben.

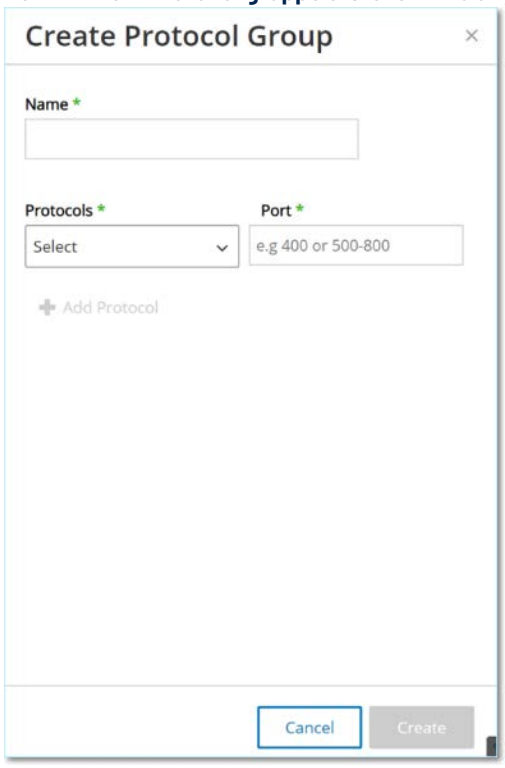
Parameter	Beschreibung
Name	Der Name, der zur Identifizierung der Gruppe dient.
Protokolle	Die Liste der Protokolle, die in der Gruppe enthalten sind. **Hinweis:** Wenn nicht genügend Platz vorhanden ist, um alle Mitglieder der Gruppe anzuzeigen, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > Mitglieder**.
In Richtlinien verwendet	Zeigt den Namen jeder Richtlinie an, die diese Protokollgruppe in ihrer Konfiguration verwendet. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Erstellen von Protokollgruppen

Sie können benutzerdefinierte Protokollgruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Durch die Gruppierung ähnlicher Protokolle ermöglichen Sie die Erstellung von Richtlinien, die festlegen, welche Protokolle verdächtig sind.

So erstellen Sie eine Protokollgruppe:

1. Wählen Sie unter **Gruppen** die Option **Protokollgruppen** aus.
2. Klicken Sie auf **Protokollgruppe erstellen**.
   Der Assistent **Protokollgruppe erstellen** wird angezeigt.

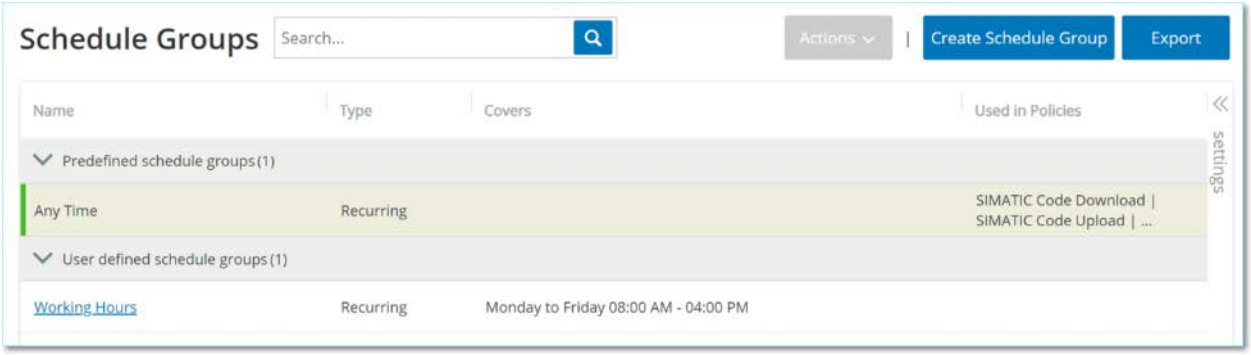


3. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
4. Wählen Sie im Feld **Protokolle** einen Protokolltyp aus dem Dropdown-Menü aus.
5. Wenn das ausgewählte Protokoll *TCP* oder *UDP* ist, geben Sie eine Port-Nummer oder einen Bereich von Ports in das Feld **Port** ein. Bei anderen Protokolltypen wird im Feld **Port** kein Wert eingetragen.
6. Wenn Sie der Gruppe weitere Protokolle hinzufügen möchten, gehen Sie für jedes zusätzliche Protokoll wie folgt vor.
   a. Klicken Sie auf **+ Protokoll hinzufügen**.
      Ein neues Feld zur **Protokollauswahl** wird angezeigt.
   b. Füllen Sie die neue Protokollauswahl wie in den Schritten 4 bis 5 beschrieben aus.
7. Klicken Sie auf **Erstellen**.
   Die neue Protokollgruppe wird erstellt und in der Liste der Protokollgruppen angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

Planungsgruppe

Eine Planungsgruppe definiert einen Zeitbereich oder eine Gruppe von Zeitbereichen, die bestimmte Merkmale aufweisen, die in diesem Zeitraum stattfindende Aktivitäten erwähnenswert machen. Beispielsweise wird erwartet, dass bestimmte Aktivitäten während der Arbeitszeit stattfinden, während andere Aktivitäten voraussichtlich während der Ruhezeiten stattfinden.

Anzeigen von Planungsgruppen



Der Bildschirm **Planungsgruppen** zeigt alle Planungsgruppen, die derzeit im System konfiguriert sind. Die Registerkarte *Vordefiniert* umfasst die in das System integrierten Gruppen. Diese Gruppen können nicht bearbeitet, dupliziert oder gelöscht werden. Die Registerkarte *Benutzerdefiniert* zeigt die benutzerdefinierten Gruppen, die vom Benutzer erstellt wurden. Diese Gruppen können bearbeitet, dupliziert oder gelöscht werden.

Die auf diesem Bildschirm angezeigten Informationen werden in der folgenden Tabelle beschrieben.

Parameter	Beschreibung
Name	Der Name, der zur Identifizierung der Gruppe dient.
Typ	Zeigt den Gruppentyp an. Optionen sind: • Funktion – Eine vordefinierte Planungsgruppe, die erstellt wurde, um eine bestimmte Funktion zu erfüllen. • Wiederkehrend – Ein Zeitplan, der sich täglich oder wöchentlich wiederholt. Beispielsweise kann ein Zeitplan der Arbeitszeiten als Zeitraum von Montag bis Freitag von 9:00 bis 17:00 Uhr definiert werden. • Intervall – Ein Zeitplan, der an einem bestimmten Datum oder in einem bestimmten Datumsbereich auftritt. Ein Zeitplan für die Renovierung einer Anlage könnte zum Beispiel durch den Zeitraum vom 1. Juni bis zum 15. August definiert werden.
Zeitplan	Eine Zusammenfassung der Planungseinstellungen. **Hinweis:** Wenn nicht genügend Platz vorhanden ist, um alle Mitglieder der Gruppe anzuzeigen, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > Mitglieder**.
In Richtlinien verwendet	Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Planungsgruppe in ihrer Konfiguration verwendet. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Erstellen von Planungsgruppen

Sie können benutzerdefinierte Planungsgruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Geben Sie einen Zeitbereich oder eine Gruppe von Zeitbereichen an, die bestimmte Merkmale aufweisen, die in diesem Zeitraum stattfindende Ereignisse zu auffälligen Ereignissen machen.

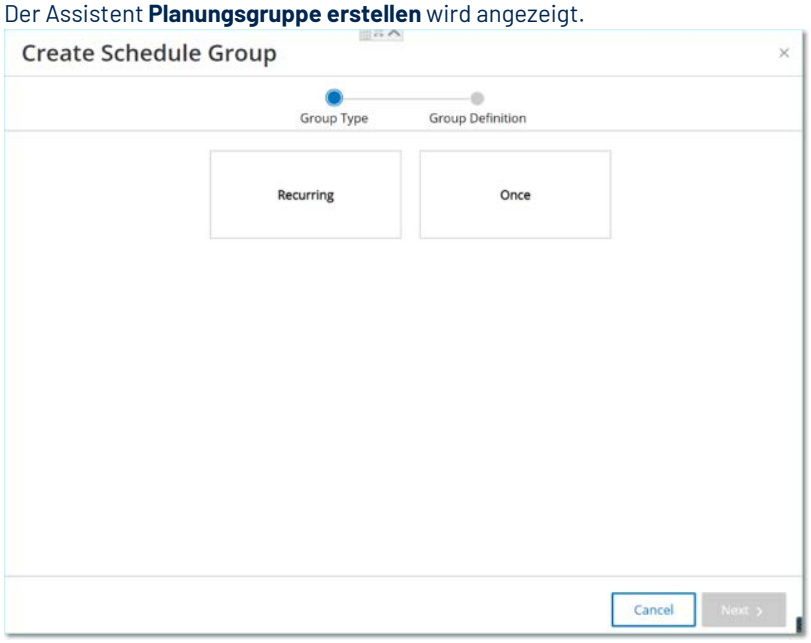
Es gibt zwei Arten von Planungsgruppen:

- **Wiederkehrend** – Zeitpläne, die sich wöchentlich wiederholen. Beispielsweise kann ein Zeitplan der Arbeitszeiten als Zeitraum von Montag bis Freitag von 9:00 bis 17:00 Uhr definiert werden.
- **Einmalig** – Zeitpläne, die an einem bestimmten Datum oder in einem bestimmten Datumsbereich auftreten. Ein Zeitplan für die Renovierung einer Anlage könnte zum Beispiel durch den Zeitraum vom 1. Juni bis zum 15. August definiert werden. Es gibt verschiedene Verfahren zum Erstellen der einzelnen Arten von Planungsgruppen.

Es gibt verschiedene Verfahren zum Erstellen der einzelnen Arten von Planungsgruppen.

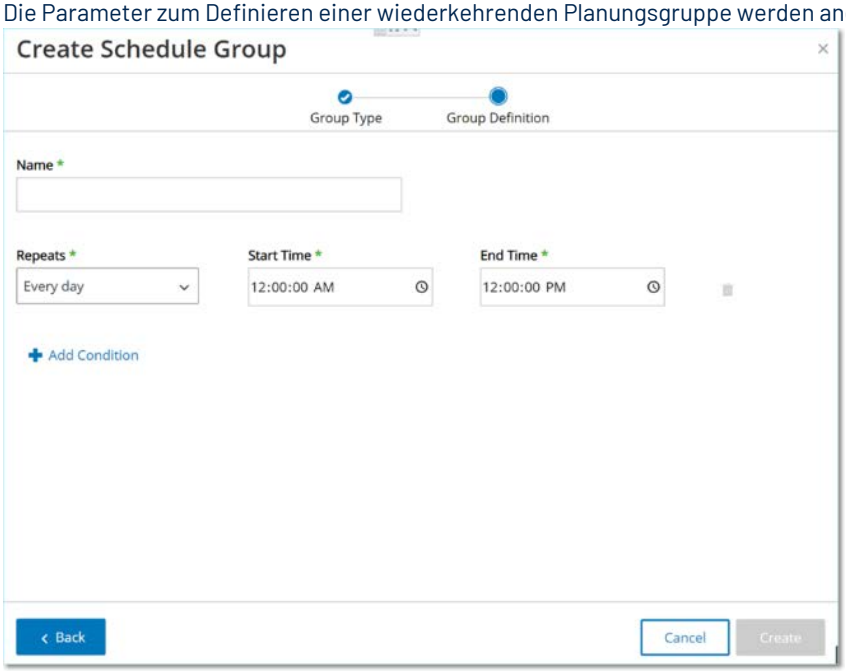
So erstellen Sie eine Planungsgruppe vom Typ „Wiederkehrend“:

1. Wählen Sie unter **Gruppen** die Option **Planungsgruppen** aus.
2. Klicken Sie auf **Planungsgruppe erstellen**.
3. Klicken Sie im Bildschirm **Planungsgruppe** auf **Planungsgruppe erstellen**.
   Der Assistent **Planungsgruppe erstellen** wird angezeigt.



4. Wählen Sie **Wiederkehrend** aus.

5. Klicken Sie auf **Weiter**.
   Die Parameter zum Definieren einer wiederkehrenden Planungsgruppe werden angezeigt.



6. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
7. Wählen Sie im Feld **Wird wiederholt** aus, welche Wochentage in die Planungsgruppe aufgenommen werden. Optionen sind: *Täglich*, *Montag bis Freitag* oder ein bestimmter Wochentag.

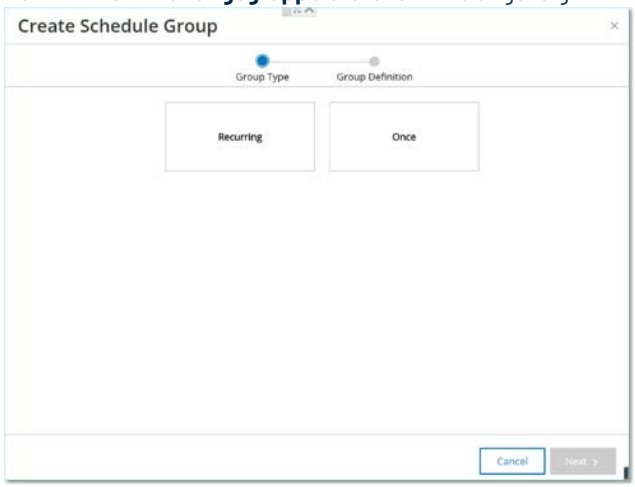
> Wenn Sie bestimmte Wochentage einbeziehen möchten, z. B. Montag und Mittwoch, müssen Sie für jeden Tag eine eigene Bedingung hinzufügen.

8. Geben Sie im Feld **Startzeit** die Tageszeit (HH:MM:SS AM/PM) für den Beginn des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
9. Geben Sie im Feld **Endzeit** die Tageszeit (HH:MM:SS AM/PM) für das Ende des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
10. Wenn Sie der Planungsgruppe weitere Bedingungen (z. B. weitere Zeitbereiche) hinzufügen möchten, gehen Sie für jede zusätzliche Bedingung wie folgt vor.
    a. Klicken Sie auf **+ Bedingung hinzufügen**.
       Eine neue Reihe von Feldern für die Zeitplanauswahl wird angezeigt.
    b. Füllen Sie die Zeitplanfelder wie oben in Schritt 5 bis 7 beschrieben aus.
11. Klicken Sie auf **Erstellen**.
    Die neue Planungsgruppe wird erstellt und in der Liste der Planungsgruppen angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

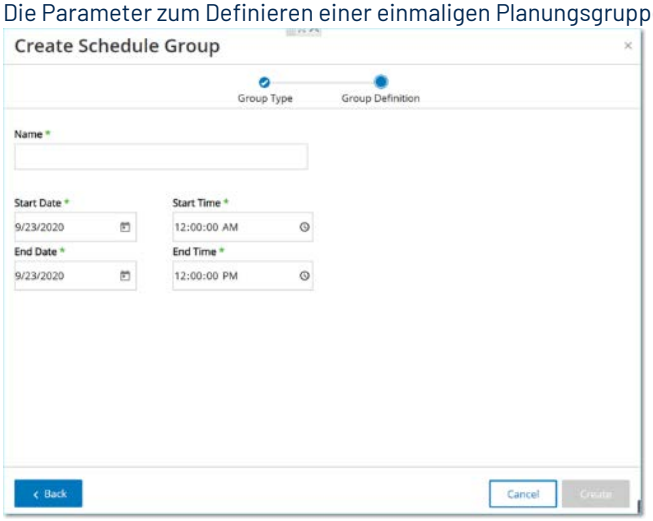
So erstellen Sie eine einmalige Planungsgruppe:

1. Wählen Sie unter **Gruppen** die Option **Planungsgruppen** aus.
2. Klicken Sie auf **Planungsgruppe erstellen**.

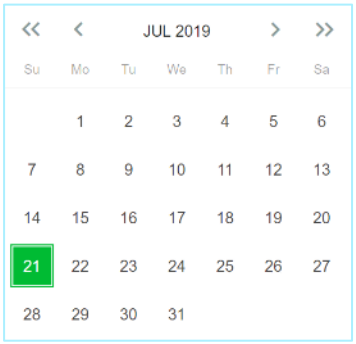
Der Assistent **Planungsgruppe erstellen** wird angezeigt.



3. Wählen Sie **Einmalig** aus.
4. Klicken Sie auf **Weiter**.
   Die Parameter zum Definieren einer einmaligen Planungsgruppe werden angezeigt.



5. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
6. Klicken Sie im Feld **Startdatum** auf das Kalendersymbol .
   Ein Kalenderfenster wird geöffnet.



7. Wählen Sie das Datum aus, an dem die Planungsgruppe beginnt. (Standard: das aktuelle Datum)
8. Geben Sie im Feld **Startzeit** die Tageszeit (HH:MM:SS AM/PM) für den Beginn des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
9. Klicken Sie im Feld **Enddatum** auf das Kalendersymbol .
   Ein Kalenderfenster wird geöffnet.
10. Wählen Sie das Datum aus, an dem die Planungsgruppe endet. (Standard: das aktuelle Datum)
11. Geben Sie im Feld **Endzeit** die Tageszeit (HH:MM:SS AM/PM) für das Ende des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.

12. Klicken Sie auf **Erstellen**.
    Die neue Planungsgruppe wird erstellt und in der Liste der Planungsgruppen angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

Tag-Gruppen

Tags sind Parameter in Controllern, die spezifische Betriebsdaten enthalten. Tag-Gruppen werden als Richtlinienbedingung für **Richtlinien für SCADA-Ereignisse** verwendet. Durch Gruppieren von Tags, die ähnliche Rollen spielen, können Sie Richtlinien erstellen, die verdächtige Änderungen an den angegebenen Parametern erkennen. Indem Sie beispielsweise Tags gruppieren, die die Ofentemperatur steuern, können Sie eine Richtlinie erstellen, die Temperaturänderungen erkennt, die für die Öfen schädlich sein könnten.

Anzeigen von Tag-Gruppen

Der Bildschirm „Tag-Gruppen" zeigt alle Tag-Gruppen, die derzeit im System konfiguriert sind.

Die auf diesem Bildschirm angezeigten Informationen werden in der folgenden Tabelle beschrieben.

Parameter	Beschreibung
Name	Der Name, der zur Identifizierung der Gruppe dient.
Typ	Der Datentyp für das Tag. Mögliche Werte sind: *Bool*, *Dint*, *Float*, *Int*, *Long*, *Short*, *Unknown* (für Tags eines Typs, den Tenable.ot nicht identifizieren konnte) oder *Any Type* (was Tags verschiedener Typen umfassen kann).
Controller	Der Controller, auf dem das Tag überwacht wird.
Tags	Zeigt jedes in der Gruppe enthaltene Tag sowie den Namen des Controllers an, in dem es sich befindet. **Hinweis:** Wenn in dieser Zeile kein Platz zum Anzeigen aller Tags vorhanden ist, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > Mitglieder**.
In Richtlinien verwendet	Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Planungsgruppe in ihrer Konfiguration verwendet. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen > Anzeigen > In Richtlinien verwendet**.

Das Verfahren zum Erstellen einer Port-Gruppe wird in dem folgenden Abschnitt beschrieben. Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe **Aktionen für Gruppen**.

Erstellen von Tag-Gruppen

Sie können benutzerdefinierte Tag-Gruppen zur Verwendung in der Richtlinienkonfiguration erstellen. Durch Gruppieren ähnlicher Tags können Sie Richtlinien erstellen, die für alle Tags in der Gruppe gelten. Wählen Sie die Tags ähnlichen Typs aus und geben Sie ihnen einen Namen, der das gemeinsame Element der Tags darstellt.

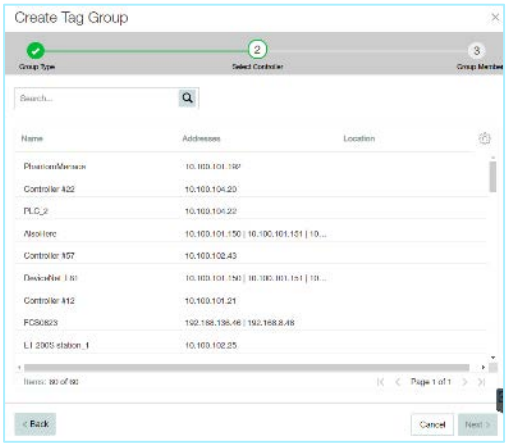
Sie können auch Gruppen erstellen, die Tags unterschiedlicher Typen enthalten, indem Sie die Option *Any Type* (Beliebiger Typ) auswählen In diesem Fall können Richtlinien, die auf diese Gruppe angewendet werden, nur Änderungen an *Beliebiger Wert* für die angegebenen Tags erkennen. Sie können jedoch nicht so eingestellt werden, dass sie bestimmte Werte erkennen.

Tag-Gruppen können bearbeitet, dupliziert oder gelöscht werden.

So erstellen Sie eine neue Tag-Gruppe:

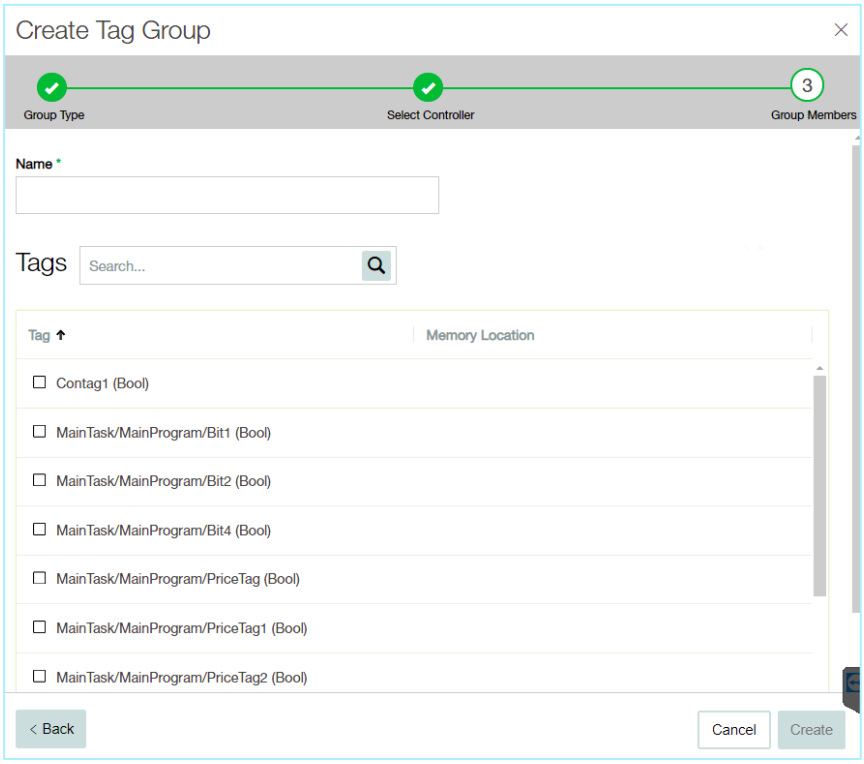
1. Wählen Sie unter **Gruppen** die Option **Tag-Gruppen** aus.
2. Klicken Sie auf **Tag-Gruppe erstellen**.
   Der Assistent **Tag-Gruppe erstellen** wird angezeigt.

3. Wählen Sie einen Tag-Typ aus. Optionen sind: *Bool*, *Dint*, *Float*, *Int*, *Long*, *Short* oder *Any Type* (was Tags verschiedener Typen umfassen kann).
4. Klicken Sie auf **Weiter**.
   Eine Liste der Controller in Ihrem Netzwerk wird angezeigt.



5. Wählen Sie einen Controller aus, für den Sie Tags in die Gruppe aufnehmen möchten.
6. Klicken Sie auf **Weiter**.

Eine Liste von Tags des angegebenen Typs auf dem angegebenen Controller wird angezeigt.



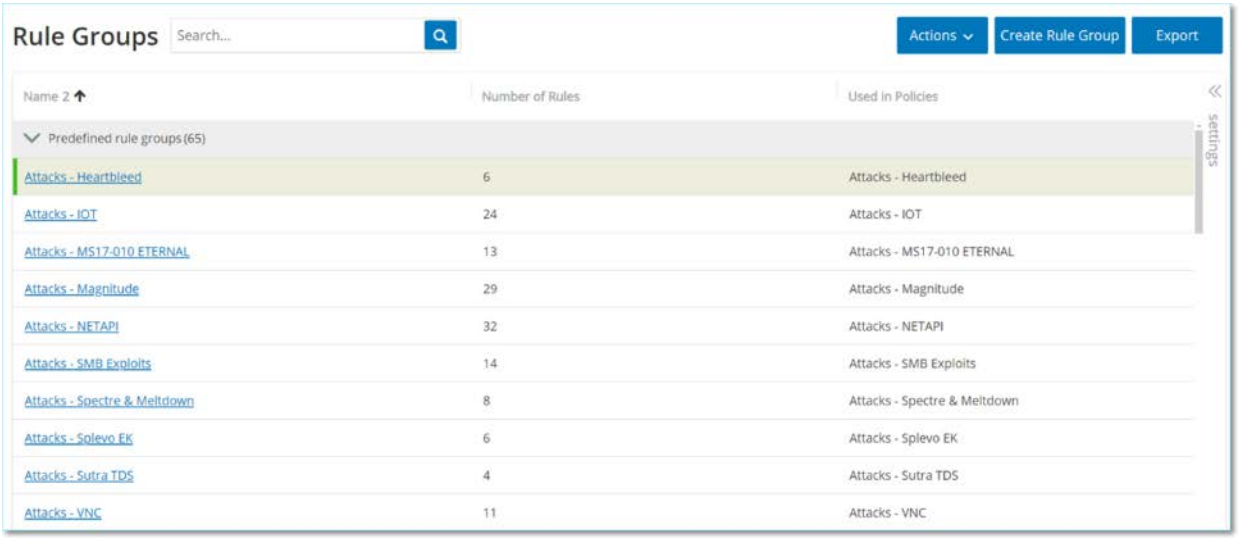
7. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
8. Aktivieren Sie das Kontrollkästchen neben jedem Tag, das Sie in die Gruppe aufnehmen möchten.
9. Klicken Sie auf **Erstellen**.
   Die neue Tag-Gruppe wird erstellt und in der Liste der Tag-Gruppen angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von SCADA-Ereignisrichtlinien verwenden.

Regelgruppen

Regelgruppen bestehen aus einer Gruppe verwandter Regeln, die durch ihre Suricata-Signatur-IDs (SIDs) identifiziert werden. Diese Gruppen werden als Richtlinienbedingung zum Definieren von Intrusion Detection-Richtlinien verwendet.

Tenable.ot bietet eine Reihe vordefinierter Gruppen verwandter Schwachstellen. Darüber hinaus können Sie einzelne Regeln aus unserem Schwachstellen-Repository auswählen und Ihre eigenen benutzerdefinierten Regelgruppen erstellen.

Anzeigen von Regelgruppen



Der Bildschirm **Regelgruppen** zeigt alle Regelgruppen, die derzeit im System konfiguriert sind. Die Registerkarte *Vordefiniert* umfasst die in das System integrierten Gruppen. Diese Gruppen können nicht bearbeitet, dupliziert oder gelöscht werden. Die Registerkarte *Benutzerdefiniert* zeigt die benutzerdefinierten Gruppen, die vom Benutzer erstellt wurden. Diese Gruppen können bearbeitet, dupliziert oder gelöscht werden.

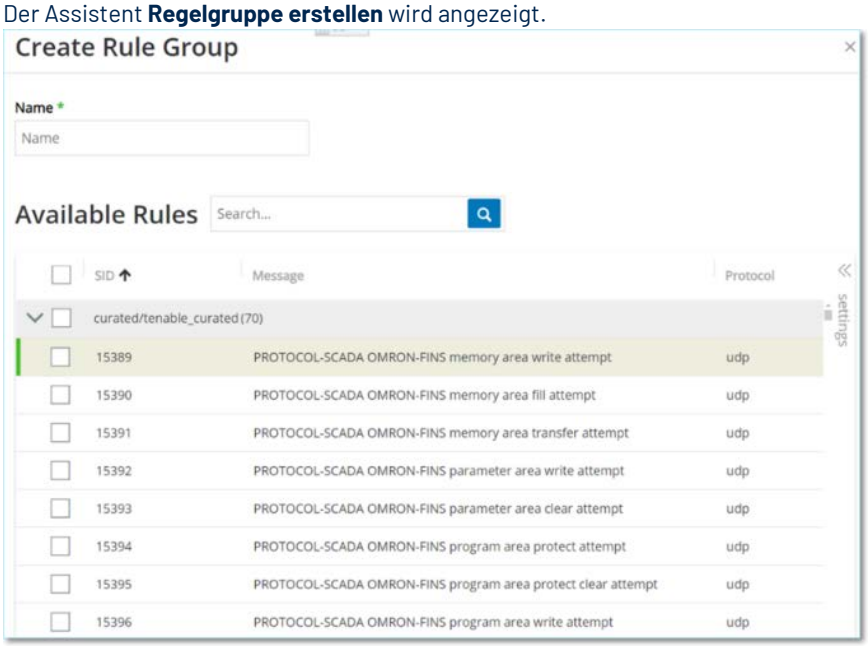
Die auf diesem Bildschirm angezeigten Informationen werden in der folgenden Tabelle beschrieben.

Parameter	Beschreibung
Name	Der Name, der zur Identifizierung der Gruppe dient.
Anzahl an Regeln	Die Anzahl der Regeln (SIDs), aus denen diese Regelgruppe besteht.
In Richtlinien verwendet	Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Regelgruppe in ihrer Konfiguration verwendet. **Hinweis:** Um weitere Details zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf die Registerkarte **Tabellenaktionen** > **Anzeigen** > **In Richtlinien verwendet**.

Erstellen von Regelgruppen

So erstellen Sie eine neue Regelgruppe:

1. Wählen Sie unter **Gruppen** die Option **Regelgruppen** aus.
2. Klicken Sie auf **Regelgruppe erstellen**.
   Der Assistent **Regelgruppe erstellen** wird angezeigt.



3. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
4. Aktivieren Sie im Abschnitt **Verfügbare Regeln** das Kontrollkästchen neben jeder Regel, die Sie in die Gruppe aufnehmen möchten.

> Verwenden Sie das Suchfeld, um die gewünschten Regeln zu finden.

5. Klicken Sie auf **Erstellen**.
   Die neue Regelgruppe wird erstellt und in der Liste der Regelgruppen angezeigt. Sie können diese Gruppe jetzt beim Konfigurieren von Intrusion Detection-Richtlinien verwenden.

Aktionen für Gruppen

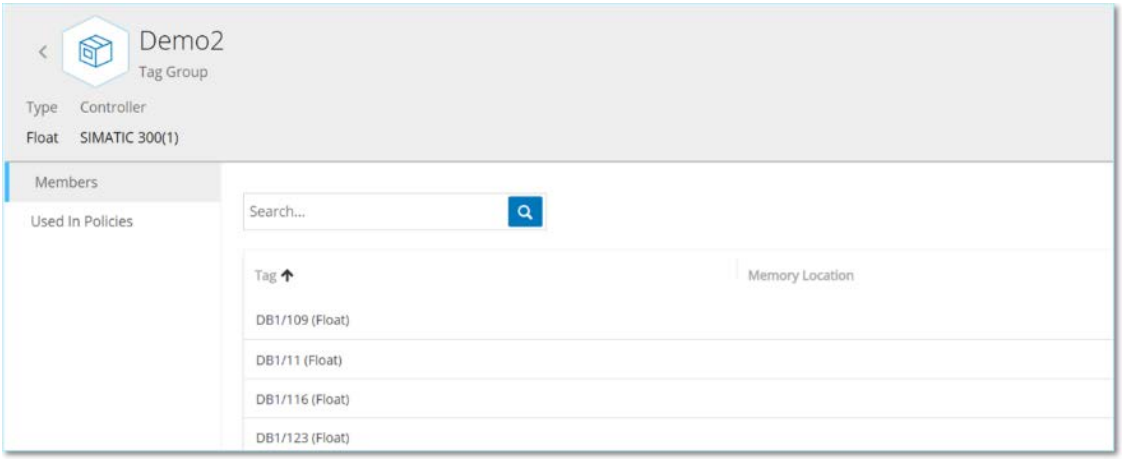
Wenn Sie eine Gruppe auswählen (auf einem der Gruppen-Bildschirme), können Sie im Menü „Aktionen" oben im Bildschirm die folgenden Aktionen ausführen:

- **Anzeigen** – Zeigt Details zur ausgewählten Gruppe an, z. B. welche Entitäten in der Gruppe enthalten sind und welche Richtlinien die Gruppe als Richtlinienbedingung verwenden.
- **Bearbeiten** – Hier können Sie Details der Gruppe bearbeiten.
- **Duplizieren** – Erstellen Sie eine neue Gruppe mit einer ähnlichen Konfiguration wie die angegebene Gruppe.
- **Löschen** – Löschen Sie die Gruppe aus dem System.

> Vordefinierte Gruppen können nicht bearbeitet oder gelöscht werden. Einige vordefinierte Gruppen können auch nicht dupliziert werden.
>
> Auf das Menü „Aktionen" kann auch zugegriffen werden, indem Sie mit der rechten Maustaste auf eine Gruppe klicken.

Anzeigen von Gruppendetails

Wenn Sie eine Gruppe auswählen und auf **Aktionen > Anzeigen** klicken, wird der Bildschirm *Gruppendetails* für die ausgewählte Gruppe angezeigt.



Der Bildschirm „Gruppendetails" enthält eine Kopfleiste, die den Namen und Typ der Gruppe anzeigt. Er hat außerdem zwei Registerkarten:

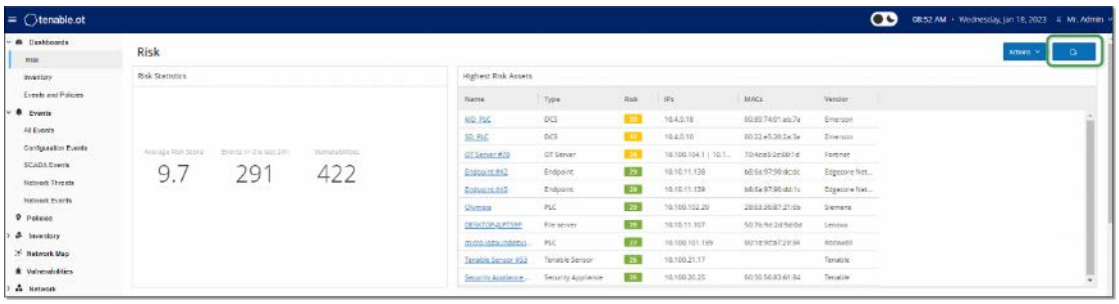
- **Mitglieder** – Zeigt eine Liste aller Mitglieder der Gruppe.

- **Verwendet in Richtlinien** – Zeigt eine Liste für jede Richtlinie, für die die angegebene Gruppe als Richtlinienbedingung verwendet wird. Die Richtlinienliste enthält einen Umschalter zum Aktivieren/Deaktivieren der Richtlinie. Die in den Richtlinienlisten angezeigten Informationen werden im Kapitel zum **EXPORTIEREN** des Dashboards

Über die Schaltfläche „Exportieren" des Dashboard-Bildschirms kann eine PDF-Datei exportiert werden, die für jedes Dashboard-Widget eine separate Seite enthält.

So exportieren Sie das Dashboard:

1. Klicken Sie in der oberen rechten Ecke des Dashboards auf die Schaltfläche **Exportieren** ( ).

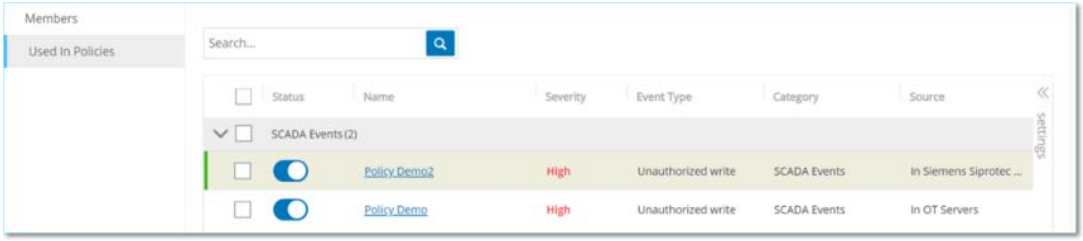


Die PDF-Datei wird automatisch in den Standardordner für Downloads heruntergeladen.

2. Achten Sie darauf, dass die Registerkarte „Dashboard“ in Ihrem Browser geöffnet bleibt, während die PDF-Datei heruntergeladen wird (2 bis 3 Sekunden).

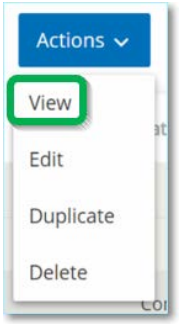
3. Navigieren Sie nach Abschluss des Downloads zu der gerade heruntergeladenen Datei, um sie anzuzeigen oder freizugeben.

- Richtlinien.



So zeigen Sie Details einer Gruppe an:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Wählen Sie die gewünschte Gruppe aus.
3. Klicken Sie auf **Aktionen** (oder klicken Sie mit der rechten Maustaste auf die Gruppe).
4. Wählen Sie im Dropdown-Menü **Anzeigen** aus.



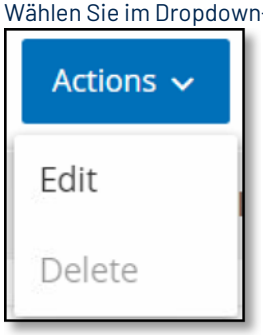
Der Bildschirm mit den Gruppendetails wird angezeigt.

Bearbeiten einer Gruppe

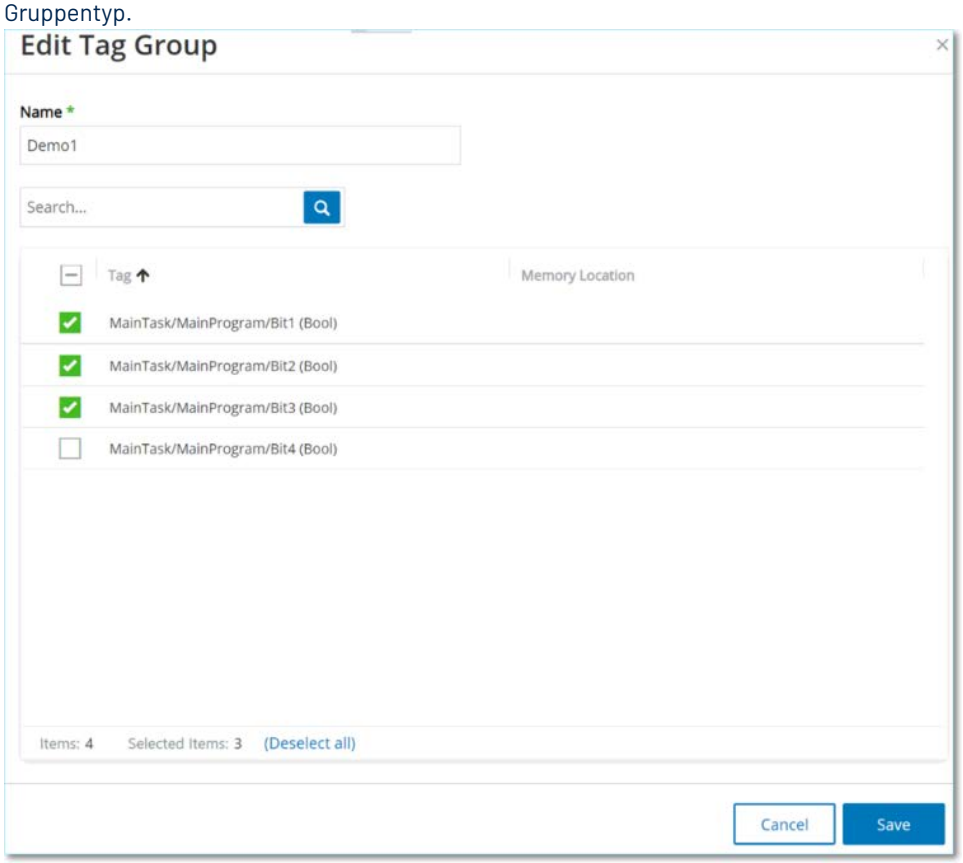
Sie können die Details einer bestehenden Gruppe bearbeiten.

So bearbeiten Sie Details einer Gruppe:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Wählen Sie die gewünschte Gruppe aus.
3. Klicken Sie auf **Aktionen** (oder klicken Sie mit der rechten Maustaste auf die Gruppe).
4. Wählen Sie im Dropdown-Menü **Bearbeiten** aus.



5. Das Fenster **Gruppe bearbeiten** wird angezeigt und zeigt die relevanten Parameter für den angegebenen Gruppentyp.



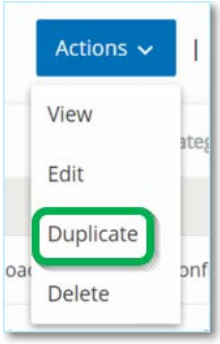
6. Nehmen Sie die gewünschten Änderungen vor.
7. Klicken Sie auf **Speichern**.
   Die Gruppe wird mit den neuen Einstellungen gespeichert.

Duplizieren einer Gruppe

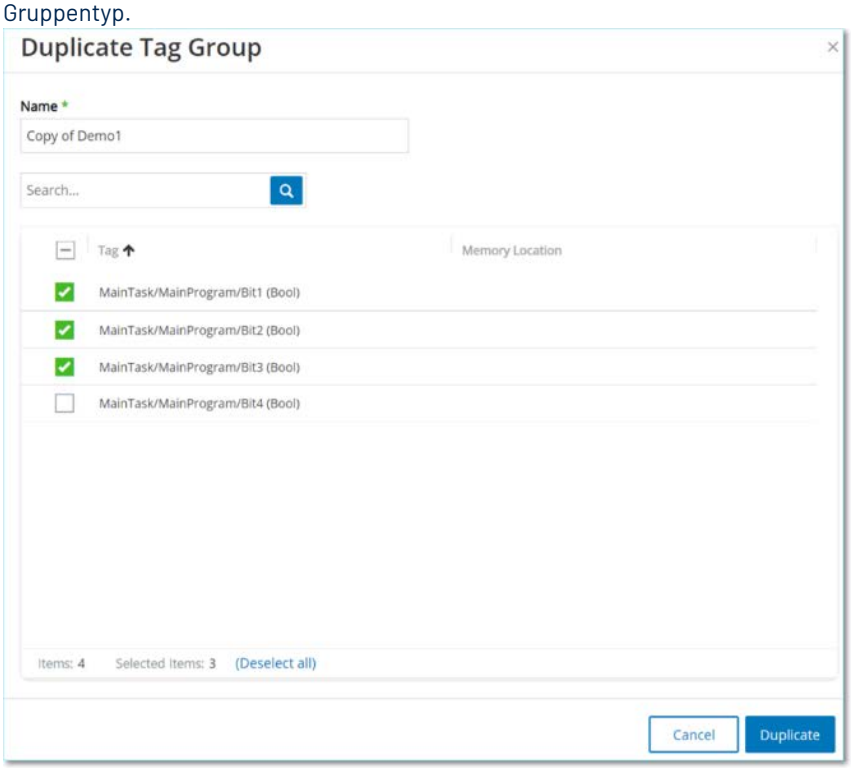
Wenn Sie eine neue Gruppe mit ähnlichen Einstellungen wie eine bestehende Gruppe erstellen möchten, können Sie die bestehende Gruppe „duplizieren". Wenn Sie eine Gruppe duplizieren, wird die neue Gruppe zusätzlich zur ursprünglichen Gruppe unter einem neuen Namen gespeichert.

So duplizieren Sie eine Gruppe:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Wählen Sie die vorhandene Gruppe aus, auf der die neue Gruppe basieren soll.
3. Klicken Sie auf **Aktionen** (oder klicken Sie mit der rechten Maustaste auf die Gruppe).
4. Wählen Sie im Dropdown-Menü **Duplizieren** aus.



5. Das Fenster **Gruppe duplizieren** wird angezeigt und zeigt die relevanten Parameter für den angegebenen Gruppentyp.



6. Geben Sie im Feld **Name** einen Namen für die neue Gruppe ein. (Standardmäßig heißt die neue Gruppe „Kopie von" dem ursprünglichen Gruppennamen.)
7. Nehmen Sie die gewünschten Änderungen an den Gruppeneinstellungen vor.
8. Klicken Sie auf **Duplizieren**.
   Die neue Gruppe wird zusätzlich zur bestehenden Gruppe mit den neuen Einstellungen gespeichert.

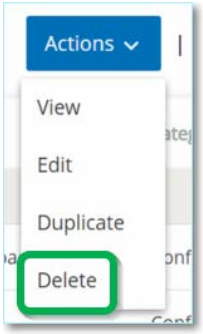
Löschen einer Gruppe

Sie können benutzerdefinierte Gruppen löschen. Vordefinierte Gruppen können nicht gelöscht werden. Falls eine benutzerdefinierte Gruppe als Richtlinienbedingung für eine oder mehrere Richtlinien verwendet wird, kann sie ebenfalls nicht gelöscht werden.

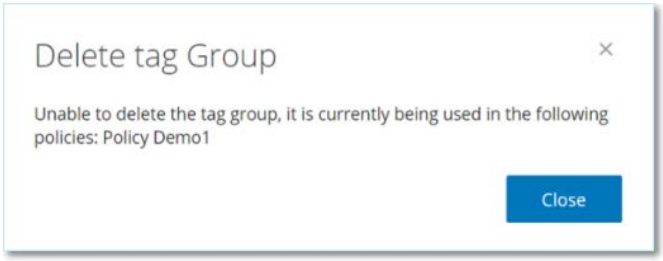
So löschen Sie eine Gruppe:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Wählen Sie die Gruppe aus, die Sie löschen möchten.

3. Klicken Sie auf **Aktionen** (oder klicken Sie mit der rechten Maustaste auf die Gruppe).
4. Wählen Sie im Dropdown-Menü **Löschen** aus.



5. Ein Bestätigungsfenster wird angezeigt.

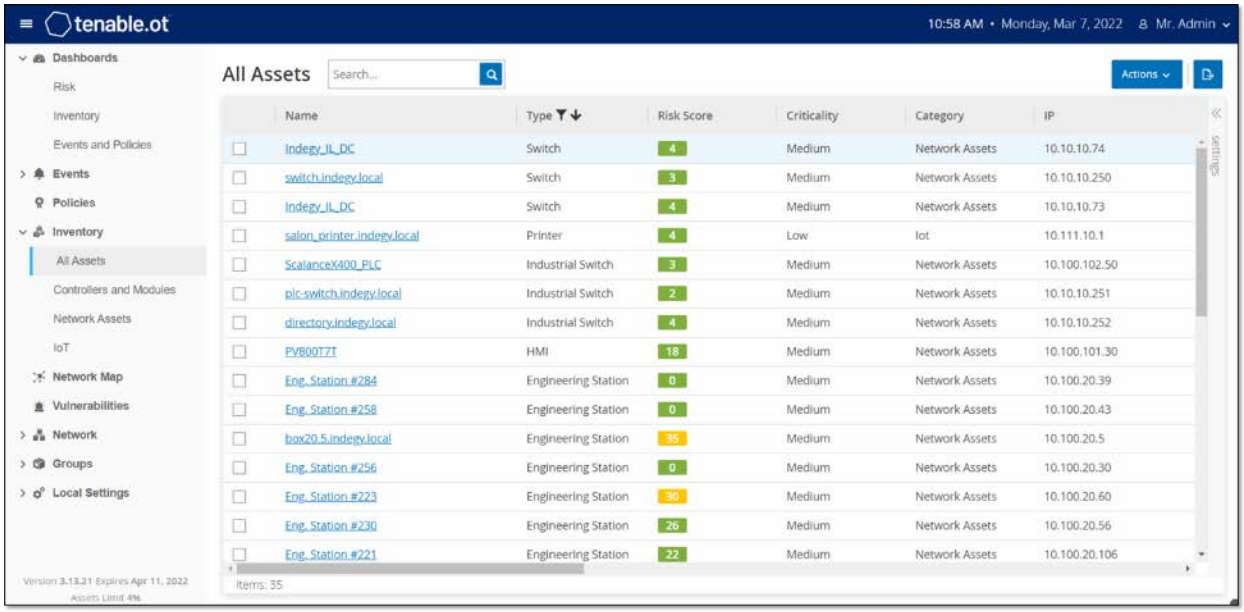


6. Klicken Sie auf **Löschen**.
   Die Gruppe wird dauerhaft aus dem System gelöscht.

INVENTAR

Die automatisierte Asset-Erfassung, -Klassifizierung und -Verwaltung von Tenable.ot bietet eine genaue, aktuelle Asset-Inventarisierung, indem alle Änderungen an Geräten kontinuierlich verfolgt werden. Dies vereinfacht die Aufrechterhaltung der betrieblichen Kontinuität, Zuverlässigkeit und Sicherheit. Es spielt außerdem eine wichtige Rolle bei der Planung von Wartungsprojekten, der Priorisierung von Upgrades, der Bereitstellung von Patches sowie bei der Vorfallsreaktion und Risikominderungsmaßnahmen.

Anzeigen von Assets



Alle Assets im Netzwerk werden auf den Inventar-Bildschirmen angezeigt. Zu jedem Asset werden detaillierte Daten angezeigt, was ein umfassendes Asset-Management sowie die Überwachung des Status jedes Assets und der damit verbundenen Ereignisse ermöglicht. Die in den Inventar-Bildschirmen angezeigten Daten werden mithilfe der Tenable.ot-Funktionen für Netzwerkerkennung und aktive Abfragen erfasst. Der Bildschirm **Alle** zeigt Daten für alle Asset-Typen. Darüber hinaus werden spezifische Teilmengen der Assets für jeden der folgenden Asset-Typen auf separaten Bildschirmen angezeigt: **Controller und Module**, **Netzwerk-Assets** und **IoT**.

Der Bildschirm *Netzwerk-Assets* enthält alle Arten von Assets, die nicht in den Bildschirmen *Controller und Module* oder *IoT* enthalten sind.

Für jeden Asset-Bildschirm (*Alle*, *Controller und Module*, *Netzwerk-Assets* und *IoT*) können Sie die Anzeigeeinstellungen benutzerdefiniert einstellen, indem Sie anpassen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Außerdem können Sie die Asset-Listen sortieren und filtern sowie eine Suche durchführen. Eine Erläuterung der Anpassungsfunktionen finden Sie unter **Arbeiten mit Listen**.

Die folgende Tabelle beschreibt die Parameter, die auf den Inventar-Bildschirmen angezeigt werden.

Mit einem „*“ gekennzeichnete Parameter werden nur im Bildschirm Controller angezeigt.

Parameter	Beschreibung
Name	Der Name des Assets im Netzwerk. Klicken Sie auf den Namen des Assets, um den Bildschirm „Asset-Details“ für dieses Asset anzuzeigen (siehe **Anzeigen von Asset-Details**).

Parameter	Beschreibung
IP	Die IP-Adresse des Assets. **Hinweis:** Ein Asset kann mehrere IP-Adressen haben. **Hinweis:** Als „Direkt" ausgewiesene IP-Adressen sind diejenigen, zu denen Tenable eine direkte Verbindung hergestellt hat. Wenn keine Beschriftung vorhanden ist, bedeutet dies, dass Tenable die IP ohne direkte Kommunikation gefunden hat. **Hinweis:** Assets können nach IP-Bereich gefiltert werden. Weitere Informationen zum Filtern finden Sie unter **Filtern**.
MAC	Die MAC-Adresse des Assets.
Netzwerksegment	Das Netzwerksegment, dem die IPs dieses Assets zugewiesen sind.
Typ	Der Typ des Assets, *Controller*, *E/A* oder *Kommunikation* usw. (siehe **Asset-Typen**).
Backplane*	Die Backplane-Einheit, mit der das Asset verbunden ist. Weitere Details zur Backplane-Konfiguration werden im Bildschirm „Asset-Details" angezeigt.
Slot*	Zeigt für Assets auf Backplanes die Nummer des Steckplatzes an, an dem das Asset angeschlossen ist.
Anbieter	Der Asset-Anbieter.
Familie*	Der vom Asset-Anbieter definierte Name der Produktfamilie.
Firmware	Die aktuell auf dem Asset installierte Firmware-Version.
Standort	Der Standort des Assets, wie vom Benutzer in den Asset-Details von Tenable.ot eingegeben. Siehe **Bearbeiten von Asset-Details**.
Zuletzt gesehen	Der Zeitpunkt, zu dem das Gerät zuletzt von Tenable.ot gesehen wurde. Dies ist das letzte Mal, dass das Gerät mit dem Netzwerk verbunden war oder eine Aktivität durchgeführt hat.
Betriebssystem	Das Betriebssystem, das auf dem Asset ausgeführt wird.
Modellname	Der Modellname des Assets.
Status*	Der Gerätestatus. Mögliche Werte: Backup – Der Controller wird als Backup für einen primären Controller ausgeführt. Fehler – Der Controller befindet sich im Fehlermodus. Keine Konfig. – Für den Controller wurde keine Konfiguration eingestellt. Läuft – Der Controller läuft. Angehalten – Der Controller läuft nicht. Unbekannt – Der Status ist unbekannt.
Beschreibung	Eine kurze Beschreibung des Assets, wie vom Benutzer in den Asset-Details von Tenable.ot konfiguriert. Siehe **Bearbeiten von Asset-Details**.
Risiko	Ein Maß für das mit diesem Asset verbundene Risiko auf einer Skala von 0 (kein Risiko) bis 100 (extrem hohes Risiko). Eine Erläuterung, wie der Risikowert berechnet wird, finden Sie unter **Risikobewertung**.

Parameter	Beschreibung
Kritikalität	Ein Maß für die Bedeutung dieses Assets für das ordnungsgemäße Funktionieren des Systems. Jedem Asset wird basierend auf dem Asset-Typ automatisch ein Wert zugewiesen. Sie können den Wert manuell anpassen.
Purdue-Level	Das Purdue-Level des Assets (0=Physischer Prozess, 1=Intelligente Geräte, 2=Steuerungssysteme, 3=Betriebssysteme der Produktion, 4=Business-Logistiksysteme).
Benutzerdefiniertes Feld	Sie können benutzerdefinierte Felder erstellen, um Ihre Assets mit relevanten Informationen zu kennzeichnen. Das benutzerdefinierte Feld kann ein Link zu einer externen Ressource sein.

Asset-Typen

Die folgende Tabelle beschreibt die verschiedenen Arten von Assets, die von Tenable.ot identifiziert wurden. Sie zeigt auch das Symbol, mit dem die einzelnen Asset-Typen jeweils in der Tenable.ot-Verwaltungskonsole dargestellt werden (z. B. im Bildschirm „Netzwerkübersicht“).

Kategorie	Standard-Kritikalitätsstufe/ Purdue-Level	Beschreibung	Untertypen	
Controller	Hoch/1	Ein industrielles Computer-Steuerungssystem, das den Zustand von Eingabegeräten kontinuierlich überwacht und Entscheidungen auf der Grundlage eines benutzerdefinierten Programms trifft, um den Zustand von Ausgabegeräten zu steuern. Diese Kategorie umfasst alle Arten von Controllern und ihre zugehörigen Komponenten.		Controller
				SPS
				DCS
				IED
				RTU
				BMS-Controller
				Roboter
				Kommunikationsmodul
				E/A-Modul
				CNC
				Stromversorgung
				Backplane-Modul

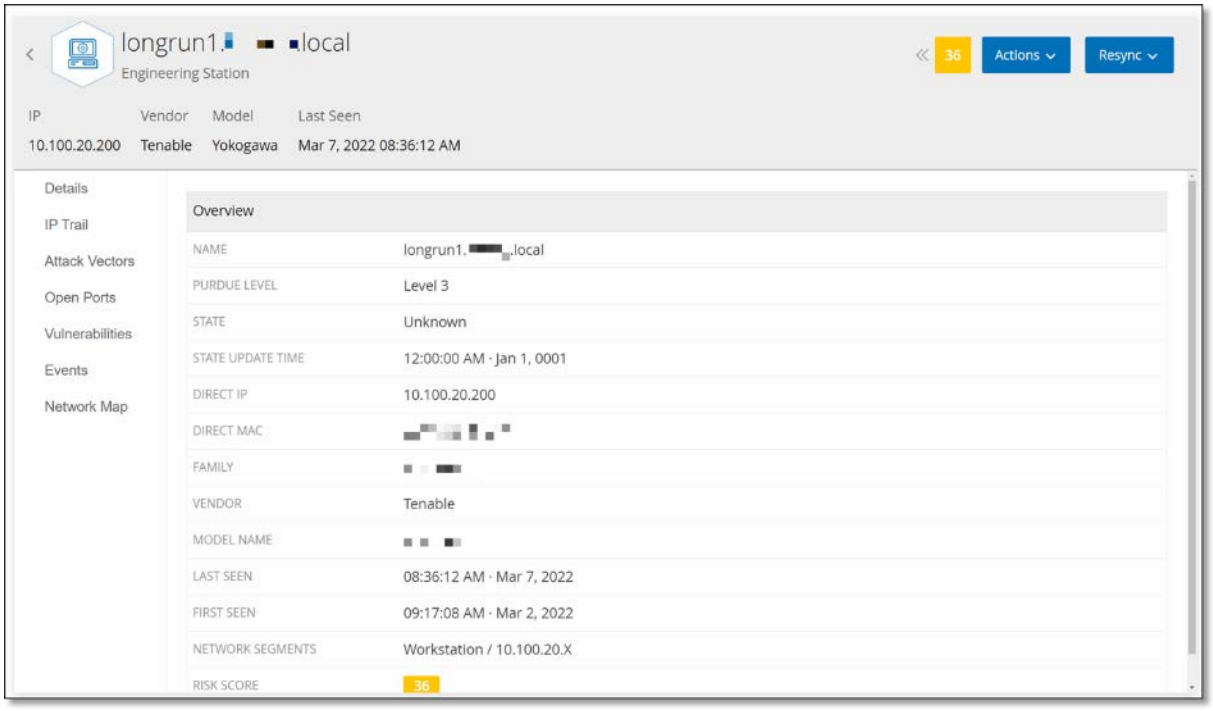
Kategorie	Standard-Kritikalitätsstufe/ Purdue-Level	Beschreibung	Untertypen	
Feldgeräte	Hoch/1	Ein industrielles Gerät (z. B. Sensor, Aktuator, Elektromotor), das Industrieprotokolle verwendet, um Informationen an ICS-Systeme zu senden.		Feldgerät
				Strommessgerät
				Remote-E/A
				Relais
				Wandler
				Industrieller Sensor
				Antrieb
				Aktuator
OT-Geräte	Mittel/2	Diese Kategorie umfasst alle Arten von OT-Geräten.		OT-Gerät
				Industrieller Router
				Industrieller Switch
				Industrielles Gateway
				Industrielles Netzwerkgerät
				Industrieller Drucker
OT-Server	Mittel/2	Ein Computer/Gerät, der/das für den Zugriff auf industrielle Daten verwendet wird. Diese Kategorie umfasst alle Arten von OT-Servern und ihre zugehörigen Komponenten.		OT-Server
				Historian
				HMI
				Datenlogger

Kategorie	Standard-Kritikalitätsstufe/ Purdue-Level	Beschreibung	Untertypen	
Netzwerkgeräte	Mittel/3	Ein Netzwerkgerät (z. B. ein Switch oder ein Router). Diese Kategorie umfasst alle Arten von Netzwerkgeräten und ihre zugehörigen Komponenten.		Netzwerkgerät
				Router
				Switch
				Serielle Ethernet-Brücke
				Gateway
				Hub
				Wireless Access Point
				Firewall
				Konverter
				Repeater
				Funksender
Workstations	Gering/3	Ein Computer, der mit dem Netzwerk verbunden ist und zur Steuerung der SPS verwendet wird. Diese Kategorie umfasst alle Arten von Workstations und ihre zugehörigen Komponenten.		Workstation
				OT-Workstation
				Engineering-Station
				Virtuelle Workstation
Server	Gering/3	Diese Kategorie umfasst verschiedene Arten von IT-Servern.		Server
				Dateiserver
				Webserver

Kategorie	Standard-Kritikalitätsstufe/ Purdue-Level	Beschreibung	Untertypen	
				Virtueller Server
				Sicherheits-Appliance
				Tenable ICP
				Tenable EM
				Tenable Sensor
				Domänencontroller
				IoT
IoTs	Gering/3	Diese Kategorie umfasst verschiedene Arten von miteinander verbundenen Geräten.		Kamera
				Panel
				Beamer
				VOIP-Gerät
				3D-Drucker
				Drucker
				USV
				IP-Telefon
				Intelligenter Sensor
				Barcodescanner
				Zugangskontrollsystem

Kategorie	Standard-Kritikalitätsstufe/ Purdue-Level	Beschreibung	Untertypen	
				Beleuchtungssteuerung
				HLK-Modul
				Intelligenter Hub
				Smart-TV
				Medizinisches Gerät
				Tablet
				Mobilgerät
				Speichergerät
Endgeräte	Gering/3	Eine nicht identifizierte IP-Adresse im Netzwerk.		Endgerät

Anzeigen von Asset-Details



Der Bildschirm **Asset-Details** zeigt umfassende Details zu allen Daten, die von Tenable.ot für das ausgewählte Asset erfasst wurden. Die Details werden in der Kopfleiste sowie in einer Reihe von Registerkarten und Unterabschnitten angezeigt. Einige Registerkarten und Unterabschnitte sind nur für bestimmte Asset-Typen relevant.

Auf den Bildschirm „Asset-Details" für ein bestimmtes Asset wird zugegriffen, indem Sie auf den Namen des Assets klicken, wo immer er als Link in der Verwaltungskonsole angezeigt wird (z. B. Inventar, Ereignisse, Netzwerk usw.), oder indem Sie im entsprechenden Bildschirm **Inventar** auf **Aktionen** > **Anzeigen** klicken.

Die folgenden Elemente sind im Bildschirm „Asset-Details" enthalten (für relevante Asset-Typen):

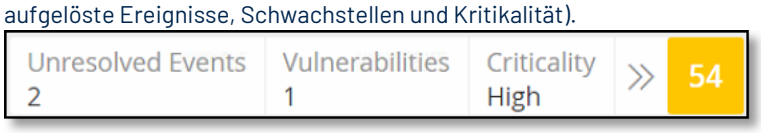
- **Kopfleistenbereich** – Zeigt einen Überblick über wichtige Informationen über das Asset und seinen aktuellen Zustand. Er enthält auch ein Menü *Aktionen*, mit dem Sie die Auflistung für dieses Asset bearbeiten können.
- **Details** – Zeigt detaillierte Informationen, die in Unterabschnitte mit spezifischen Daten unterteilt sind, die für verschiedene Asset-Typen relevant sind.
- **Coderevisionen** (nur für Controller) – Zeigt Informationen zu aktuellen sowie früheren Coderevisionen an, die von der „Snapshot"-Funktion von Tenable.ot ermittelt wurden. Dazu gehören Einzelheiten zu allen spezifischen Änderungen, die am Code vorgenommen wurden, d. h. die Abschnitte (Codeblöcke/Zeilen), die hinzugefügt, gelöscht oder geändert wurden.
- **IP-Trail** – Zeigt alle aktuellen und historischen IPs, die sich auf das Asset beziehen.
- **Angriffsvektoren** – Zeigt anfällige Angriffsvektoren, d. h. die Routen, die ein Angreifer verwenden kann, um Zugriff auf dieses Asset zu erlangen. Sie können einen Angriffsvektor automatisch generieren, um den kritischsten Angriffsvektor anzuzeigen, oder Sie können Angriffsvektoren aus bestimmten Assets manuell generieren.
- **Offene Ports** – Zeigt Informationen zu offenen Ports auf dem Asset an.
- **Schwachstellen –** Zeigt die Schwachstellen, die das System für das ausgewählte Asset identifiziert hat, wie z. B. veraltete Windows-Betriebssysteme, die Verwendung anfälliger Protokolle und offene Kommunikationsports, die bekanntermaßen riskant oder für bestimmte Gerätetypen nicht wesentlich sind, siehe **Schwachstellen**.
- **Ereignisse** – Eine Liste von Ereignissen im Netzwerk, die das Asset betreffen.

- **Netzwerkübersicht** – Zeigt eine grafische Visualisierung der Netzwerkverbindungen des Assets.
- **Geräte-Ports** (für Netzwerk-Switches) – Zeigt Informationen zu Ports auf dem Netzwerk-Switch an.

Kopfleistenbereich

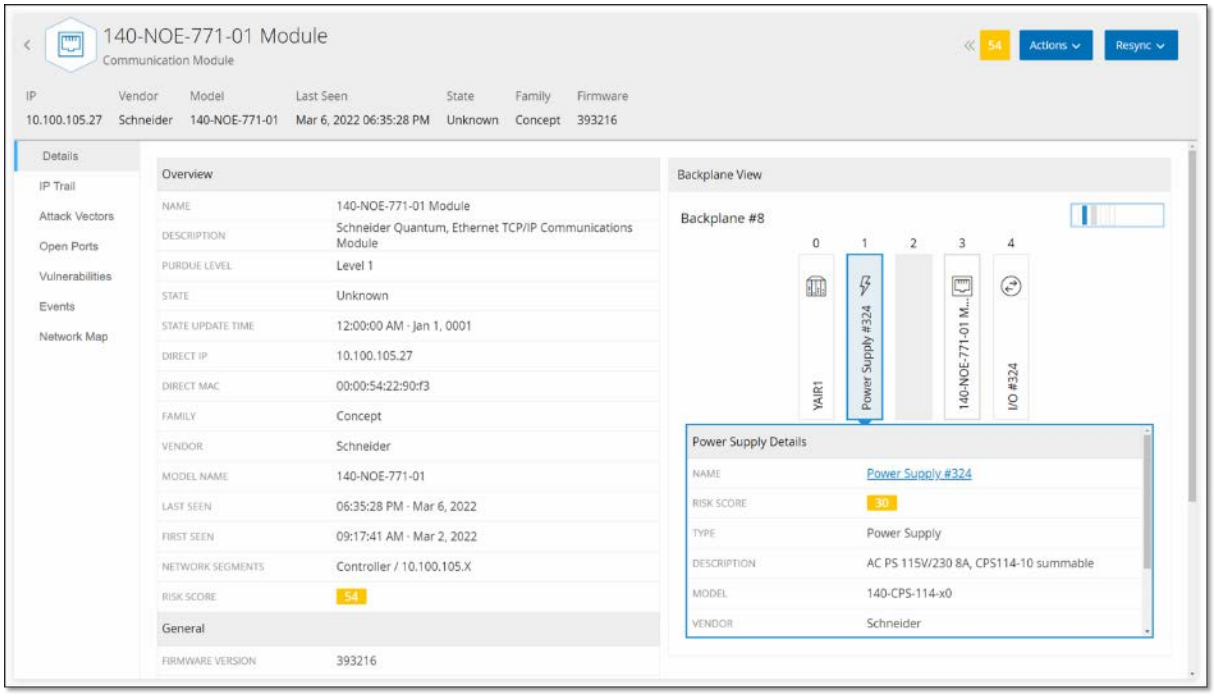
Der Kopfleistenbereich zeigt eine Übersicht über den aktuellen Status des Assets. Die Anzeige umfasst die folgenden Elemente:

- **Name** – Der Name des Assets.
- **Zurück (Link)** – Bringt Sie zurück zu dem Bildschirm, von dem aus Sie diesen Asset-Bildschirm aufgerufen haben.
- **Asset-Typ** – Zeigt das Symbol und den Namen des Asset-Typs an.
- **Asset-Übersicht** – Zeigt wichtige Informationen über das Asset, einschließlich IPs, Anbieter, Familie, Modell, Firmware und „Zuletzt gesehen" (Datum und Uhrzeit).
- **Risikowert-Widget –** Zeigt den Risikowert für das Asset an. Der Risikowert ist eine Bewertung (von 1 bis 100) des Grades der Bedrohung, die für das Asset besteht Eine Erläuterung, wie der Wert bestimmt wird, finden Sie unter **Risikobewertung**. Klicken Sie auf den Risikowert-Indikator, um ein erweitertes Widget mit einer Aufschlüsselung der Faktoren anzuzeigen, die zur Bewertung der Risikostufe beitragen (nicht aufgelöste Ereignisse, Schwachstellen und Kritikalität).

  Einige der Elemente sind Links zum entsprechenden Bildschirm, der Details zu diesem Element anzeigt.
- **Menü „Aktionen"** – Ermöglicht es Ihnen, die Asset-Details zu bearbeiten oder einen Nessus-Scan auszuführen.
- **Schaltfläche „Erneut synchronisieren"** – Klicken Sie auf diese Schaltfläche, um eine oder mehrere Abfragen, die für dieses Asset verfügbar sind, manuell auszuführen. Siehe **Durchführen einer erneuten Synchronisierung**.

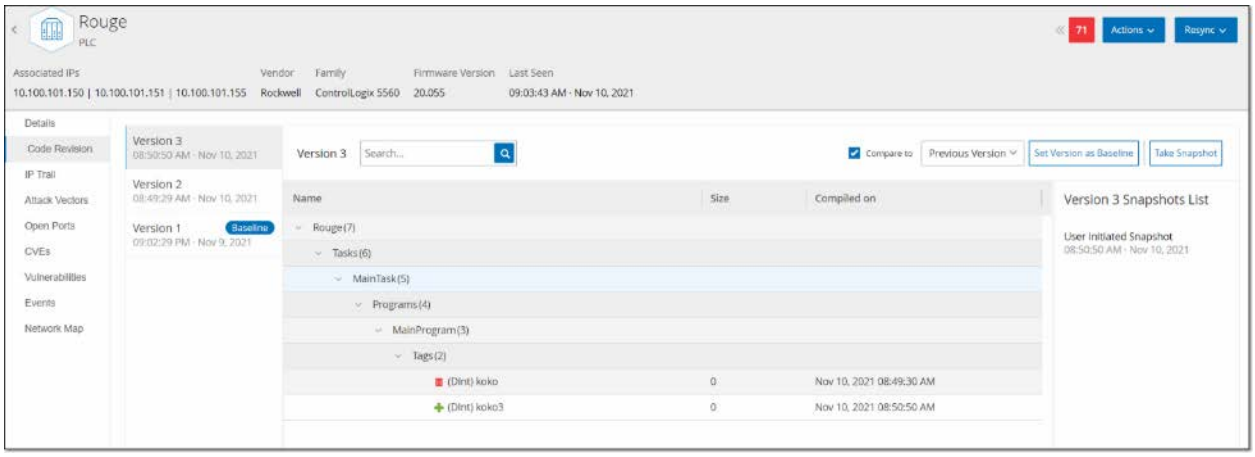
Registerkarte „Details“



Auf der Registerkarte **Details** werden zusätzliche Details zum ausgewählten Asset angezeigt. Die Informationen sind in Abschnitte unterteilt, die verschiedene Arten von System- und Konfigurationsdaten für das angegebene Asset zeigen. Es werden nur Abschnitte angezeigt, die für das angegebene Asset relevant sind. Nachfolgend finden Sie eine Liste aller Abschnittskategorien, die für verschiedene Asset-Typen angezeigt werden können: *Übersicht*, *Allgemein*, *Projekt*, *Speicher*, *Ethernet*, *Profinet*, *Betriebssystem*, *System*, *Hardware*, *Geräte und Laufwerke*, *USB-Geräte*, *Installierte Software*, *IEC -61850* und *Schnittstellenstatus*.

Für Assets, die mit einer Backplane verbunden sind, gibt es auch einen Abschnitt *Backplane-Ansicht*, der eine grafische Darstellung der Backplane-Konfiguration zeigt, einschließlich der Steckplatzposition jedes angeschlossenen Geräts. Wählen Sie ein Gerät aus, um seine Details im unteren Bereich anzuzeigen.

Coderevisionen



Die Registerkarte **Coderevision** (nur für Controller) zeigt die verschiedenen Versionen des Controller-Codes, die von Tenable.ot-„Snapshots“ erfasst wurden. Jede „Snapshot“-Version enthält Informationen über die Coderevision zum Zeitpunkt der Erstellung des Snapshot, einschließlich Details zu bestimmten Abschnitten (Codeblöcken/Zeilen) und

Tags. Immer wenn ein Snapshot nicht mit dem vorherigen Snapshot dieses Controllers identisch ist, wird eine neue *Version* der Coderevision erstellt. Sie können die einzelnen Versionen miteinander vergleichen, um zu sehen, welche Änderungen am Controller-Code vorgenommen wurden.

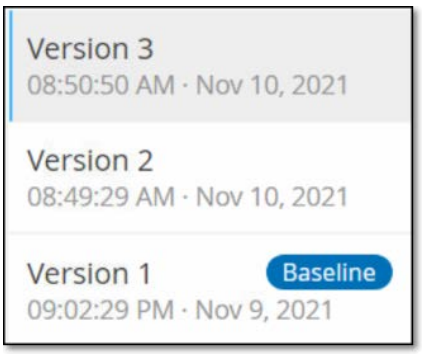
Ein Snapshot kann auf folgende Weise ausgelöst werden:

- **Routine** – Snapshots werden in regelmäßigen Abständen erstellt, wie vom Benutzer im Bildschirm „Systemeinstellungen" festgelegt.
- **Durch Aktivität** – Das System löst einen Snapshot aus, wenn eine bestimmte Code-Aktivität erkannt wird (z. B. ein Code-Download).
- **Durch Benutzer** – Der Benutzer kann einen Snapshot manuell auslösen, indem er auf die Schaltfläche **Snapshot erstellen** für ein bestimmtes Asset klickt.

Sie können eine Richtlinie für Snapshot-Konflikte konfigurieren, um Ergänzungen, Löschungen oder Änderungen am Code eines Controllers zu erkennen, siehe **Konfigurationsereignis – Typen von Controller-Validierungsereignissen**.

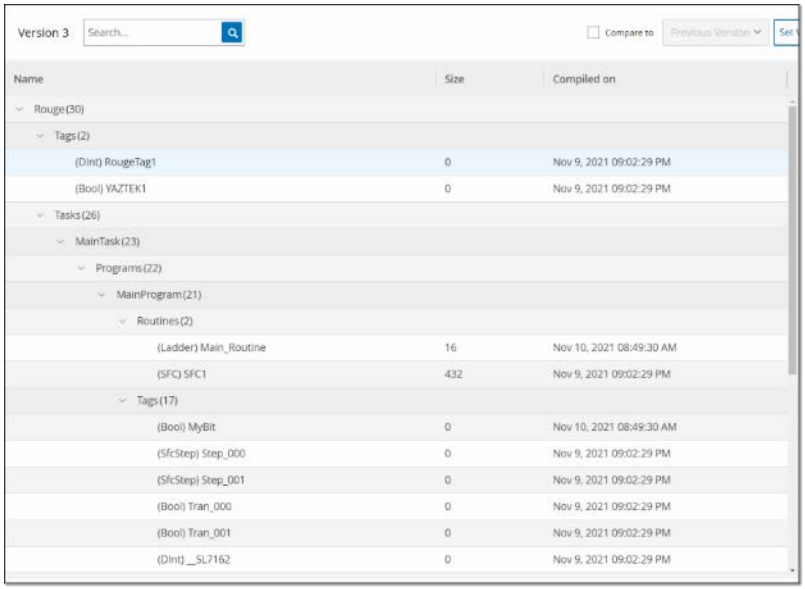
In den folgenden Abschnitten werden die verschiedenen Abschnitte der Coderevisionsanzeige sowie der Vergleich verschiedener „Snapshot"-Versionen beschrieben.

Bereich „Versionsauswahl"



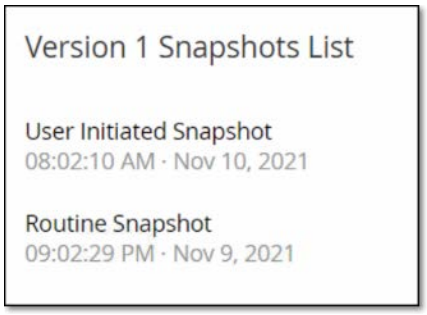
Dieser Bereich zeigt eine Liste aller verfügbaren Versionen der Coderevision für diesen Controller. Für jede Version wird die *Startzeit* angezeigt, zu der die Version nachweislich in Kraft war. Eine neue Version wird jedes Mal erstellt, wenn eine Änderung gegenüber dem vorherigen „Snapshot" erkannt wird. Das Tag „Baseline" gibt an, welche Version aktuell als Baseline-Version für Vergleichszwecke festgelegt ist. Wählen Sie eine Version aus, um ihre Coderevisionen im Bereich **Snapshot-Details** anzuzeigen.

Bereich „Snapshot-Details“



Der Detailbereich zeigt detaillierte Informationen zu den spezifischen Codeblöcken, Zeilen und Tags für die ausgewählte Snapshot-Version. Die Codeelemente werden in einer Baumstruktur mit Pfeilen zum Erweitern/Minimieren der angezeigten Details angezeigt. Für jedes Element werden der Name, die Größe und das Erstellungsdatum angezeigt. Sie können die ausgewählte Version mit der vorherigen Version oder mit der „Baseline“-Version vergleichen, um zu sehen, welche Änderungen vorgenommen wurden, siehe **Vergleichen von Snapshot-Versionen**.

Bereich „Versionsverlauf“



Dieser Bereich zeigt Details über den Snapshot, mit dem die ausgewählte Version erfasst wurde, einschließlich der Methode, mit der er initiiert wurde, sowie Datum und Uhrzeit der Erfassung.

Wenn zwischen den Snapshots keine Änderungen vorgenommen wurden, werden mehrere Snapshots zu einer einzigen Version zusammengefasst. Alle identischen Snapshots werden im Bereich für den Snapshot-Verlauf für die betreffende Version aufgelistet.

Vergleichen von Snapshot-Versionen

Sie können eine Snapshot-Version entweder mit der *vorherigen* Version oder mit der *Baseline-Version* vergleichen. Nachdem ein Vergleich ausgeführt wurde, zeigt der Bereich „Snapshot-Details“ die Änderungen an, die zwischen den beiden Snapshots am Code des Controllers vorgenommen wurden.

Änderungen werden wie folgt gekennzeichnet:

 Hinzugefügt – Neuer Code, der in der ausgewählten Version hinzugefügt wurde.

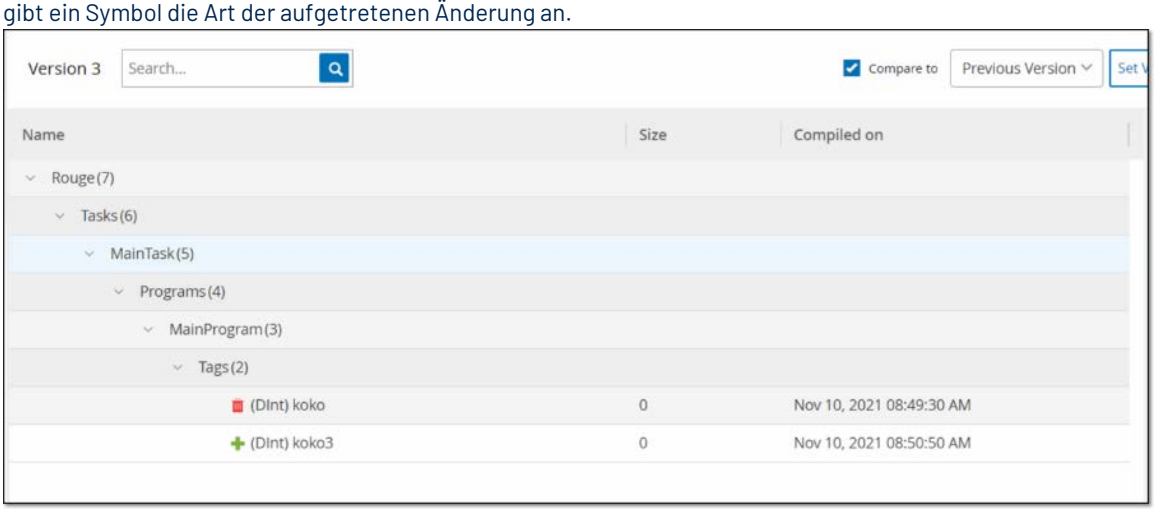
 Gelöscht – Code, der aus der ausgewählten Version gelöscht wurde.

 Bearbeitet – Code, der in der ausgewählten Version bearbeitet wurde.

So vergleichen Sie eine Snapshot-Version mit der vorherigen Version:

1. Wählen Sie im Bildschirm **Inventar** > **Controller** den gewünschten Controller aus.
2. Klicken Sie auf die Registerkarte **Coderevision**.
3. Wählen Sie im Bereich **Versionsauswahl** die Version aus, die Sie analysieren möchten.
4. Wählen Sie oben im Bereich **Snapshot-Details** im Vergleichsfeld **Vorherige Version** aus dem Dropdown-Menü aus.

5. Klicken Sie auf das Kontrollkästchen **Vergleichen mit**.
   Der Bereich „Snapshot-Details“ zeigt alle Unterschiede zwischen den beiden Versionen. Für jede Änderung gibt ein Symbol die Art der aufgetretenen Änderung an.



So vergleichen Sie eine Snapshot-Version mit einer früheren Version (nicht der vorherigen Version):

1. Wählen Sie im Bildschirm **Inventar** > **Controller** den gewünschten Controller aus.
2. Klicken Sie auf die Registerkarte **Coderevision**.
3. Wählen Sie im Bereich **Versionsauswahl** die Version aus, die Sie als Baseline für den Vergleich verwenden möchten.
4. Klicken Sie oben im Bereich **Snapshot-Details** auf **Version als Baseline festlegen**.
   Das **Baseline**-Tag wird für die ausgewählte Version angezeigt, was darauf hinweist, dass sie als Baseline-Version festgelegt ist.

> Die Einstellung einer Version als Baseline wirkt sich nur auf Vergleiche aus, die mithilfe dieses Bildschirms durchgeführt werden. Sie wirkt sich nicht auf Richtlinien aus, die auf *Snapshot-Konflikt* prüfen.

5. Wählen Sie im Bereich **Versionsauswahl** die Version aus, die Sie mit der Baseline vergleichen möchten.
6. Klicken Sie auf das Kontrollkästchen **Vergleichen mit**.
7. Wählen Sie im Feld neben dem Kontrollkästchen „Vergleichen mit“ die Option **Baseline-Version** aus dem Dropdown-Menü aus.
   Der Bereich „Snapshot-Details“ zeigt alle Unterschiede zwischen den beiden Versionen. Für jede Änderung gibt ein Symbol die Art der aufgetretenen Änderung an.

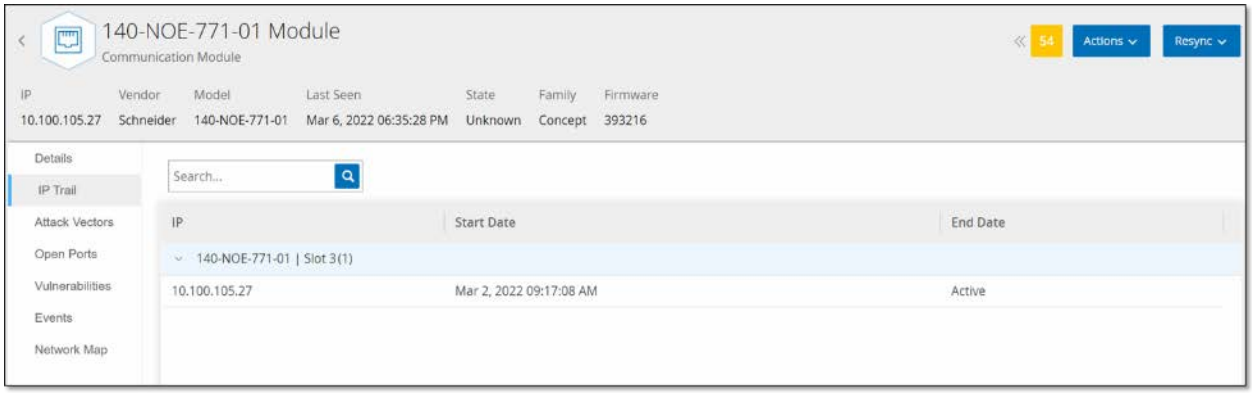
Erstellen von Snapshots

Ein Snapshot kann manuell vom Benutzer initiiert werden. Beispielsweise wird empfohlen, vor und nach der Wartung eines Controllers durch einen Techniker einen Snapshot zu erstellen.

So erstellen Sie einen Snapshot eines Controllers:

1. Wählen Sie im Bildschirm **Inventar** > **Controller** den gewünschten Controller aus.
2. Klicken Sie auf die Registerkarte **Coderevision**.
3. Klicken Sie in der oberen rechten Ecke des Bereichs **Snapshot-Details** auf **Snapshot erstellen**.
   Der vom Benutzer initiierte Snapshot wird erstellt.
4. Wenn keine Änderungen festgestellt werden, wird ein neuer vom Benutzer identifizierter Snapshot für die neueste Version zum Bereich „Revisionsverlauf“ hinzugefügt. Wenn Änderungen festgestellt werden, wird eine neue Version erstellt, die die Änderungen der Coderevision zeigt.

IP-Trail



Die Registerkarte **IP-Trail** zeigt alle IPs, die für dieses Asset relevant sind. Die Spalte „Netzwerkkarte" zeigt eine Liste der Netzwerkkarten, die von diesem Asset verwendet werden. Klicken Sie auf den Pfeil neben einer Netzwerkkarte, um die Liste zu erweitern und die IPs aller Assets anzuzeigen, die mit der gemeinsam genutzten Backplane verbunden sind.

Die Listen enthalten das Start- und Enddatum der Nutzung der IP-Adresse. Die Optionen für das Enddatum sind:

- **Aktiv** – Die IP-Adresse wird derzeit für dieses Asset verwendet.
- **{Datum/Uhrzeit}** – Das letzte Datum und die letzte Uhrzeit, zu der die IP-Adresse für dieses Asset aktiv war (wenn sie innerhalb der letzten 30 Tage aktiv war).
- **{Datum/Uhrzeit} (Inaktiv)** – Das letzte Datum und die letzte Uhrzeit, zu der die IP-Adresse für dieses Asset aktiv war (wenn sie mindestens 30 Tage lang inaktiv war).
- **Inaktiv** – Die IP-Adresse wird von einem anderen Asset verwendet.

Angriffsvektoren

Ein Angreifer kann ein kritisches Asset kompromittieren, indem er einen verwundbaren „Schwachpunkt" im Netzwerk ausnutzt, um Zugang zu dem kritischen Asset zu erhalten. Das kritische Asset ist das Ziel des Angriffs und der *Angriffsvektor* ist die Route, die der Angreifer nutzt, um sich Zugriff auf das Asset zu verschaffen.

Wie wird ein Angriffsvektor bestimmt?

Sobald das Ziel-Asset festgelegt ist, berechnet das System alle potenziellen Angriffsvektoren, die den Zugriff auf dieses Asset ermöglichen könnten, und identifiziert den Pfad, der das höchste Risikopotenzial für die Kompromittierung dieses Assets aufweist. Bei der Berechnung werden mehrere Parameter berücksichtigt und ein risikobasierter Ansatz verwendet, um den kritischsten Angriffsvektor zu bestimmen. Zu den verwendeten Parametern gehören:

- Asset-Risikostufe
- Länge des Angriffspfads
- Methode der Kommunikation zwischen Assets
- Externe Kommunikation (Internet/Unternehmensnetz) vs. interne Kommunikation

Empfohlene Schritte zur Risikominderung

Um das Risiko eines potenziellen Angriffs über den ausgewählten Vektor zu minimieren, werden u. a. folgende Schritte zur Risikominderung empfohlen:

- Verringerung der verbundenen und individuellen Risikowerte der Assets, die in dem Angriffsvektor enthalten sind.
- Minimierung oder Entfernung des Zugangs zu externen Netzwerken (Internet oder Unternehmensnetzwerke).
- Prüfung der Kommunikationswege entlang der Kette und Validierung ihrer Relevanz für den Prozess. Wenn sie nicht unbedingt notwendig sind, sollten sie entfernt werden (z. B. Schließen von Ports oder Entfernen von Diensten), um den potenziellen Angriffspfad zu beseitigen.

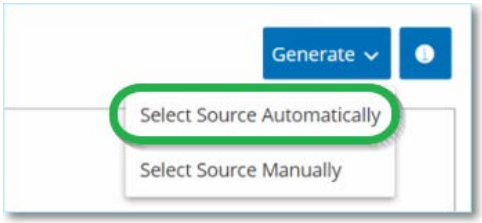
Generieren von Angriffsvektoren

Angriffsvektoren müssen für jedes relevante Ziel-Asset manuell generiert werden. Dies erfolgt auf der Registerkarte „Angriffsvektoren" für das gewünschte Ziel-Asset. Es gibt zwei Methoden zum Generieren von Angriffsvektoren:

- **Automatisch** – Tenable.ot bewertet alle potenziellen Angriffsvektoren und identifiziert den anfälligsten Pfad.
- **Manuell** – Sie geben ein bestimmtes Quell-Asset an und Tenable.ot zeigt Ihnen den potenziellen Pfad (sofern vorhanden), der für den Zugriff auf Ihr Ziel-Asset verwendet werden kann.

So generieren Sie einen automatischen Angriffsvektor:

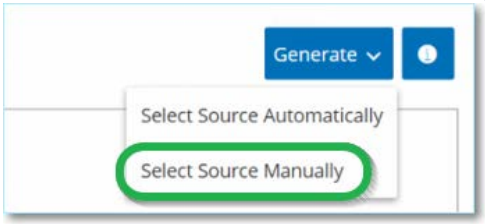
1. Navigieren Sie zur Seite **Asset-Details** für das gewünschte Ziel-Asset und klicken Sie auf die Registerkarte **Angriffsvektor**.
2. Klicken Sie auf **Generieren** und dann in der Dropdown-Liste auf **Quelle automatisch auswählen**.



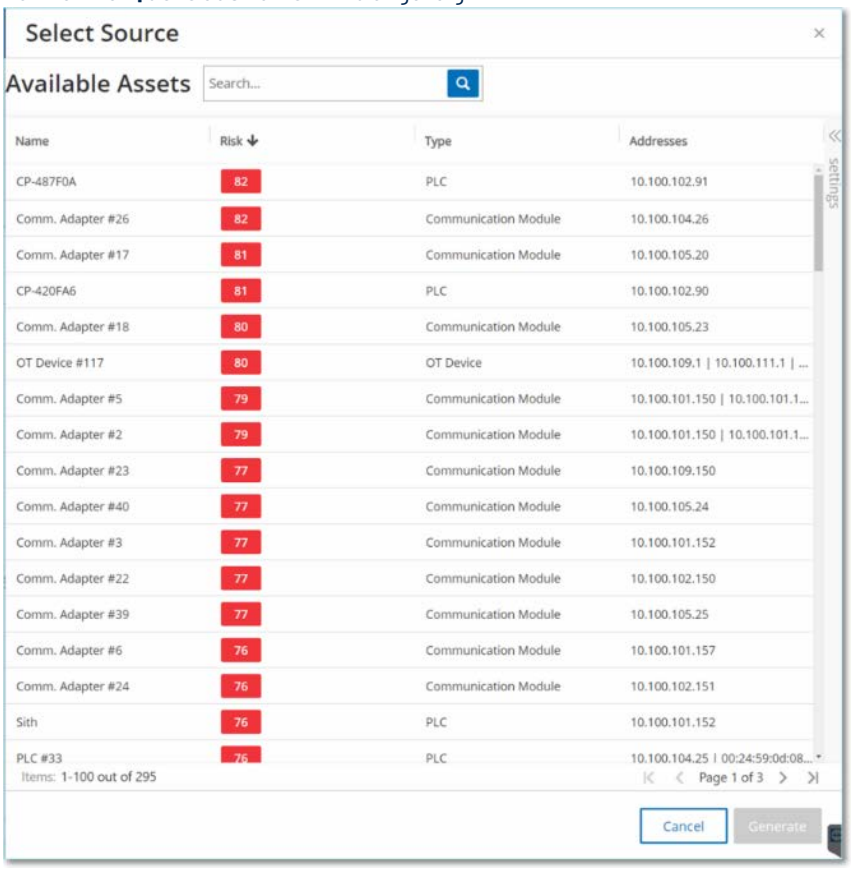
Der Angriffsvektor wird automatisch generiert und auf der Registerkarte **Angriffsvektor** angezeigt.

So generieren Sie einen manuellen Angriffsvektor:

1. Navigieren Sie zur Seite **Asset-Details** für das gewünschte Ziel-Asset und klicken Sie auf die Registerkarte **Angriffsvektor**.
2. Klicken Sie auf **Generieren** und dann in der Dropdown-Liste auf **Quelle manuell auswählen**.



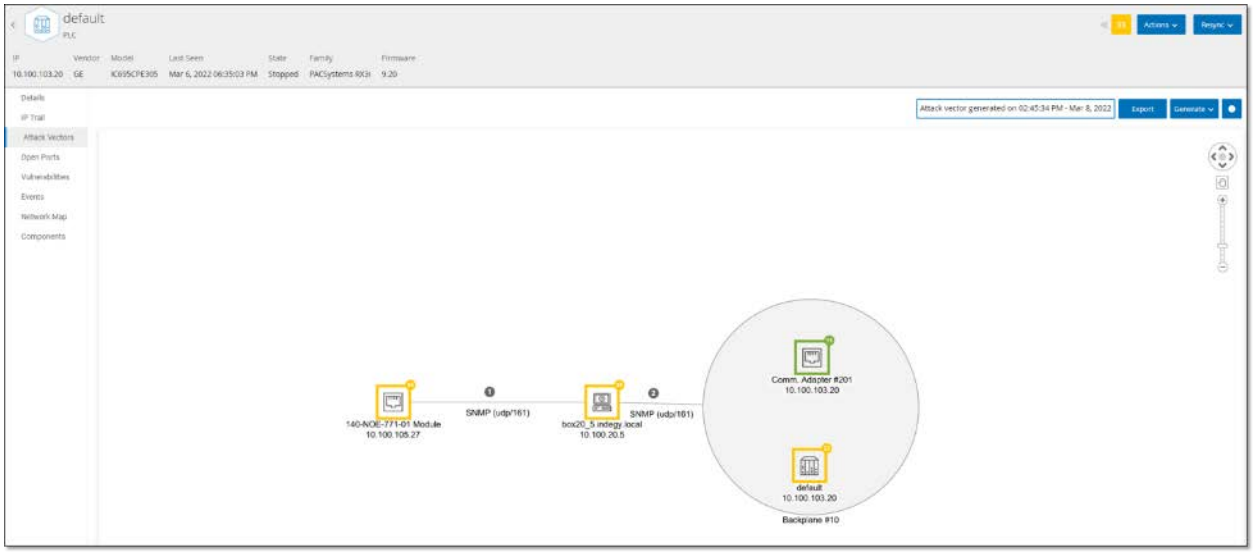
Das Fenster **Quelle auswählen** wird angezeigt.



Standardmäßig werden die Quell-Assets nach Risikowert sortiert. Sie können die Anzeigeeinstellungen anpassen oder nach dem gewünschten Asset suchen.

3. Wählen Sie das gewünschte Quell-Asset aus.
4. Klicken Sie auf **Generieren**.
   Der Angriffsvektor wird generiert und auf der Registerkarte **Angriffsvektor** angezeigt.

Anzeigen von Angriffsvektoren

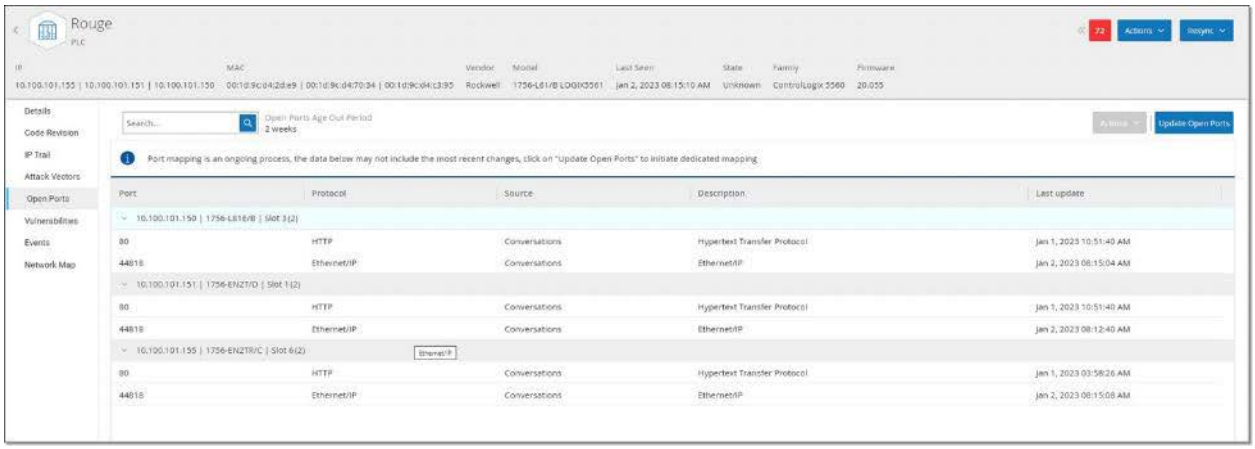


Die Registerkarte **Angriffsvektoren** zeigt ein Diagramm des zuletzt generierten Angriffsvektors für das angegebene Ziel-Asset. Das Feld neben der Schaltfläche „Generieren" zeigt Datum und Uhrzeit der Generierung des angezeigten Angriffsvektors an. Das Angriffsvektor-Diagramm umfasst die folgenden Elemente:

- Für jedes Asset, das im Angriffsvektor enthalten ist, werden die Risikostufe und die IP-Adressen angezeigt. Klicken Sie auf ein Asset-Symbol, um weitere Details zu seinen Risikofaktoren anzuzeigen.
- Für jede Netzwerkverbindung wird das Kommunikationsprotokoll angezeigt.
- Bei Assets, die eine Backplane gemeinsam nutzen, sind die Assets von einem Kreis umgeben.

Klicken Sie auf die Hilfe-Schaltfläche in der oberen rechten Ecke der Registerkarte „Angriffsvektoren", um eine Erklärung der Angriffsvektor-Funktion zu erhalten.

Offene Ports



Die Registerkarte **Offene Ports** zeigt eine Liste der offenen Ports auf diesem Asset. Für jeden offenen Port werden Details zum verwendeten Protokoll, eine Beschreibung seiner Funktion, Datum und Uhrzeit der letzten Aktualisierung der Daten sowie die Informationsquelle (aktive Abfragen, Port-Zuordnung, Konversationen, NNM oder Nessus-Scans) angegeben, die angezeigt hat, dass der Port offen ist. Für jede IP-Adresse, die dem Asset zur Verfügung steht, wird eine separate Liste der offenen Ports angezeigt (einschließlich der Ports, auf die über eine gemeinsam genutzte Backplane zugegriffen wird). Klicken Sie auf den Pfeil neben einer IP-Adresse, um die Liste zu erweitern und ihre offenen Ports anzuzeigen.

Es gibt einen automatischen **Zeitraum, nach dem offene Ports als veraltet gelten**, nach dessen Ablauf ein Eintrag eines offenen Ports automatisch aus der Liste gelöscht wird, wenn kein weiterer Hinweis darauf eingegangen ist, dass der Port noch offen ist. Der Standardzeitraum beträgt zwei Wochen. Informationen zur Anpassung der Länge des Zeitraums, nach dem offene Ports als veraltet gelten, finden Sie unter **Geräte**.

Die Parameter zum Scannen offener Ports werden auf der Registerkarte **Lokale Einstellungen** konfiguriert, siehe **Alle Controller-Abfragen**. Sie können auch eine manuelle Abfrage des ausgewählten Assets ausführen, um die Liste der offenen Ports zu aktualisieren.

So aktualisieren Sie die Liste der offenen Ports manuell:

1. Wählen Sie im Bildschirm **Inventar > Controller/Netzwerk-Assets** das gewünschte Asset aus. Der Bildschirm **Asset-Details** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Offene Ports**.
3. Klicken Sie in der oberen rechten Ecke des Bereichs „Offene Ports"auf **Offene Ports aktualisieren**. Es wird ein neuer Scan ausgeführt, der die für diesen Controller angezeigten offenen Ports aktualisiert.

Zusätzliche Aktionen auf der Registerkarte „Offene Ports“

Auf der Registerkarte „Offene Ports“ für ein bestimmtes Asset können Sie die folgenden weiteren Aktionen für einen bestimmten offenen Port durchführen.

- Scannen – Führen Sie einen Scan des ausgewählten Ports durch.
- Anzeigen – Zeigt zusätzliche Gerätedetails und Diagnosen durch Zugriff auf die Webschnittstelle des Geräts.

So führen Sie einen Scan auf einem bestimmten Port aus:

1. Wählen Sie im Bildschirm **Inventar > Controller/Netzwerk-Assets** das gewünschte Asset aus.
   Der Bildschirm **Asset-Details** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Offene Ports**.
3. Wählen Sie einen bestimmten Port aus.
4. Klicken Sie auf das Menü **Aktionen**.
5. Wählen Sie im Dropdown-Menü **Scannen** aus.
   Tenable.ot führt einen Scan auf dem ausgewählten Port durch.

So zeigen Sie das Portal für das Asset an:

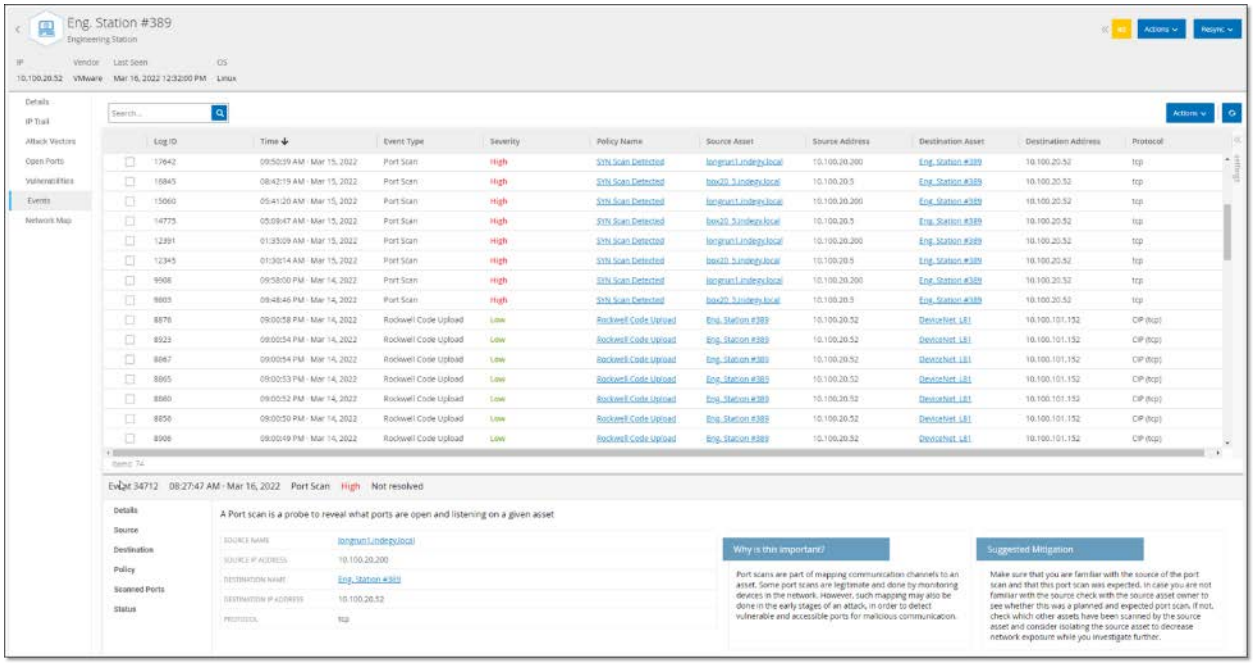
Diese Option ist nur verfügbar, wenn Port 80 (für den Webzugriff verwendet) einer der offenen Ports ist.

1. Wählen Sie im Bildschirm **Inventar > Controller/Netzwerk-Assets** das gewünschte Asset aus.
   Der Bildschirm **Asset-Details** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Offene Ports**.
3. Wählen Sie einen bestimmten Port aus.
4. Klicken Sie auf das Menü **Aktionen**.
5. Wählen Sie im Dropdown-Menü **Anzeigen** aus.
   Eine neue Browser-Registerkarte wird geöffnet, die das Asset-Portal für dieses Asset anzeigt.

Schwachstellen

Auf der Registerkarte **Schwachstellen** wird eine Liste aller Schwachstellen angezeigt, die das angegebene Asset betreffen und die von Tenable.ot Plugins erkannt wurden. Das System identifiziert Schwachstellen wie z. B. veraltete Windows-Betriebssysteme, die Verwendung anfälliger Protokolle und offene Kommunikationsports, die bekanntermaßen riskant oder für bestimmte Gerätetypen nicht unbedingt erforderlich sind. Jede Auflistung enthält Details über die Art der Bedrohung und ihren Schweregrad. Die auf dieser Registerkarte angezeigten Informationen sind **identisch mit den Informationen, die im Bildschirm „Risiko > Schwachstellen“ angezeigt werden**, mit dem Unterschied, dass hier nur Schwachstellen angezeigt werden, die für das angegebene Asset relevant sind. Eine Erläuterung der Informationen zu Schwachstellen finden Sie unter **Schwachstellen.**

Ereignisse



Auf der Registerkarte **Ereignisse** wird eine detaillierte Liste von Ereignissen im Netzwerk angezeigt, die das Asset betreffen und die von Tenable.ot Plugins erkannt wurden. Sie können die Anzeigeeinstellungen anpassen, indem Sie festlegen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Die Ereignisse können nach verschiedenen Kategorien gruppiert werden (z. B. Ereignistyp, Schweregrad, Richtlinienname). Sie können die Ereignislisten auch sortieren und filtern sowie nach Text suchen. Eine Erläuterung der Anpassungsfunktionen finden Sie unter **Arbeiten mit Listen**.

Unten im Bildschirm werden auf verschiedenen Registerkarten detaillierte Informationen zum ausgewählten Ereignis angezeigt. Es werden nur Registerkarten angezeigt, die für den Ereignistyp des ausgewählten Ereignisses relevant sind. Weitere Informationen zu Ereignissen finden Sie unter **Ereignisse**.

Oben im Bereichs befindet sich eine Schaltfläche **Aktionen**, mit der Sie die folgende Aktion für die ausgewählten Ereignisse ausführen können:

- Auflösen – Markieren Sie dieses Ereignis als „Aufgelöst“.
- PCAP herunterladen – Laden Sie die PCAP-Datei für dieses Ereignis herunter.
- Ausschließen – Erstellen Sie einen Richtlinienausschluss für dieses Ereignis.

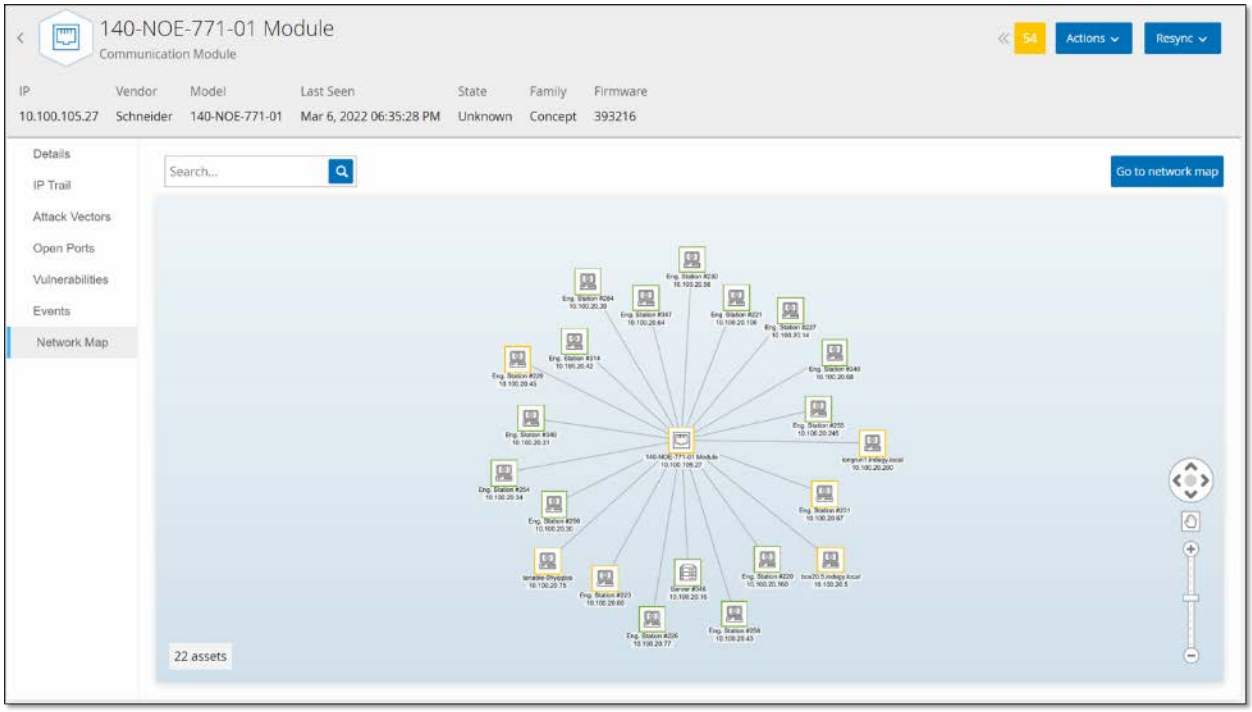
Detaillierte Informationen zu diesen Aktionen finden Sie im Kapitel **Ereignisse**.

Die für die einzelnen Ereignislisten angezeigten Informationen werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Protokoll-ID	Die vom System generierte ID, um auf das Ereignis zu verweisen.
Uhrzeit	Das Datum und die Uhrzeit des Ereignisses.

Ereignistyp	Beschreibt die Art der Aktivität, die das Ereignis ausgelöst hat. Ereignisse werden von Richtlinien generiert, die im System eingerichtet sind. Eine Erläuterung der verschiedenen Arten von Richtlinien finden Sie unter **Richtlinientypen**.
Schweregrad	Zeigt den Schweregrad des Ereignisses an. Nachfolgend finden Sie eine Erläuterung zu den möglichen Werten: Kein – Kein Grund zur Besorgnis. **Info** – Kein unmittelbarer Grund zur Sorge. Sollte bei Gelegenheit geprüft werden. **Warnung** – Moderate Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte behandelt werden, wenn es passt. **Kritisch** – Schwerwiegende Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte sofort behandelt werden.
Richtlinienname	Der Name der Richtlinie, die das Ereignis generiert hat. Der Name ist ein Link zur Richtlinienliste.
Quell-Asset	Der Name des Assets, das das Ereignis initiiert hat. Dieses Feld ist ein Link zur Asset-Liste.
Quelladresse	Die IP- oder MAC-Adresse des Assets, das das Ereignis initiiert hat.
Ziel-Asset	Der Name des Assets, das von dem Ereignis betroffen war. Dieses Feld ist ein Link zur Asset-Liste.
Zieladresse	Die IP- oder MAC-Adresse des Assets, das von dem Ereignis betroffen war.
Protokoll	Sofern relevant, wird hier das Protokoll angezeigt, das für die Konversation verwendet wurde, die dieses Ereignis ausgelöst hat.
Ereigniskategorie	Zeigt die allgemeine Kategorie des Ereignisses an. **Hinweis:** Im Bildschirm „Alle Ereignisse" werden Ereignisse aller Art angezeigt. Auf jedem der spezifischen Ereignisbildschirme werden nur Ereignisse der angegebenen Kategorie angezeigt. Im Folgenden finden Sie eine kurze Erläuterung der Ereigniskategorien (für eine ausführlichere Erläuterung siehe **Richtlinienkategorien**): • Konfigurationsereignisse – Dies umfasst zwei Unterkategorien. • Controller-Validierungsereignisse – Diese Richtlinien erkennen Änderungen, die in den Controllern im Netzwerk stattfinden. • Controller-Aktivitätsereignisse – Aktivitätsrichtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden (d. h. die „Befehle", die zwischen Assets im Netzwerk implementiert werden). • SCADA-Ereignisse – Richtlinien, die Änderungen identifizieren, die an der Datenebene von Controllern vorgenommen wurden. • Netzwerkbedrohungsereignisse – Diese Richtlinien identifizieren Netzwerk-Traffic, der auf Bedrohungen durch Eindringlinge hinweist. • Netzwerkereignisse – Richtlinien, die sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets beziehen.
Status	Zeigt an, ob das Ereignis als aufgelöst markiert wurde oder nicht.
Aufgelöst von	Zeigt für aufgelöste Ereignisse an, welcher Benutzer das Ereignis als aufgelöst markiert hat.
Aufgelöst am	Zeigt für aufgelöste Ereignisse an, wann das Ereignis als aufgelöst markiert wurde.
Kommentar	Zeigt alle Kommentare an, die hinzugefügt wurden, als das Ereignis aufgelöst wurde.

Netzwerkübersicht



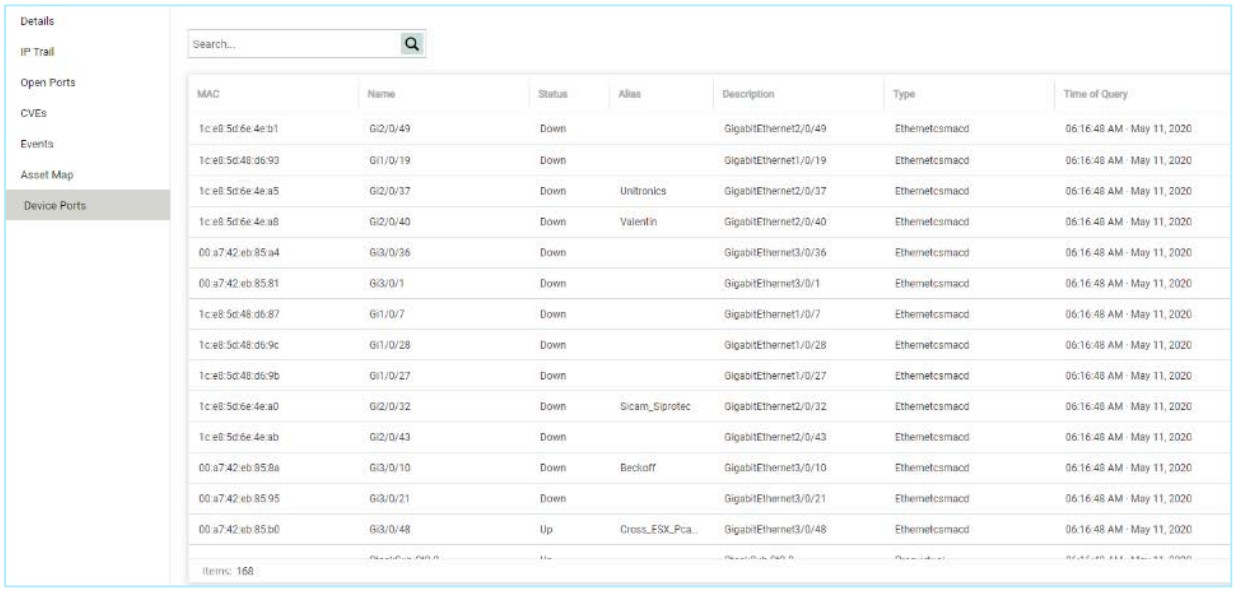
Die Registerkarte **Netzwerkübersicht** zeigt eine grafische Visualisierung der Netzwerkverbindungen des Assets. Diese Ansicht zeigt alle Verbindungen, die das ausgewählte Asset in den letzten 30 Tagen hergestellt hat.

Die auf dieser Registerkarte angezeigten Informationen ähneln den im Bildschirm **Netzwerkübersicht** angezeigten Informationen, sind jedoch auf Verbindungen beschränkt, die dieses spezifische Asset betreffen. Außerdem zeigt dieser Bildschirm Verbindungen zu einzelnen Assets und nicht zu Asset-Gruppen, wie im Hauptbildschirm „Netzwerkübersicht" dargestellt. Eine Erläuterung der auf dieser Registerkarte angezeigten Informationen finden Sie unter **NETZWERKÜBERSICHT**.

Um die Netzwerkübersicht für alle Assets anzuzeigen, klicken Sie auf die Schaltfläche **Zur Netzwerkübersicht**. Wenn Sie auf diese Schaltfläche klicken, wird die Netzwerkübersicht dynamisch vergrößert und zeigt dieses Asset und seine Verbindungen zu anderen Asset-Gruppen.

Durch Klicken auf eines der verbundenen Assets in der Übersicht klicken, werden Details zu diesem Asset angezeigt, und wenn Sie auf den Link im Namen des Assets klicken, gelangen Sie zum Detailbildschirm des ausgewählten Assets.

Geräte-Ports



Die Registerkarte **Geräte-Ports** wird für Netzwerk-Switches angezeigt. Sie zeigt detaillierte Informationen zu den Ports auf dem Netzwerk-Switch. Diese Daten werden mithilfe von SNMP-Abfragen an den Switch gesammelt. Für jeden Port werden die folgenden Informationen angezeigt: *MAC*-Adresse, *Name*, *Verbindungsstatus* (aktiv oder inaktiv), *Alias* und *Beschreibung*.

Diese Registerkarte ist nur verfügbar, wenn sie für Ihr Konto aktiviert wurde. Um diese Funktion zu aktivieren, wenden Sie sich an Ihren zuständigen Support-Mitarbeiter.

Bearbeiten von Asset-Details

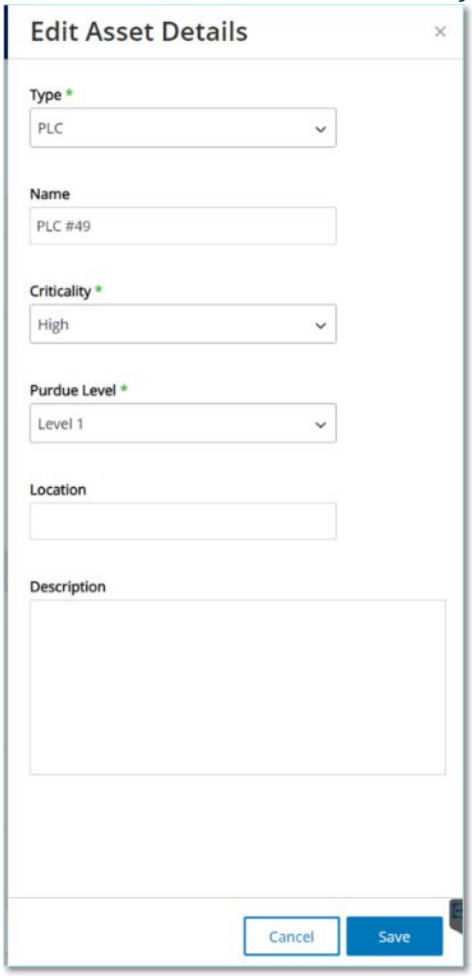
Tenable.ot identifiziert Typ und Name des Assets automatisch anhand seiner internen Daten und seiner Aktivität im Netzwerk. Wenn das System diese Informationen nicht erfassen konnte oder Sie der Meinung sind, dass die automatische Identifizierung nicht korrekt ist, können Sie diese Parameter entweder direkt über die Benutzeroberfläche oder durch Hochladen einer CSV-Datei bearbeiten. Sie können auch eine allgemeine Beschreibung des Assets und eine Beschreibung des Standorts der Einheit hinzufügen.

Bearbeiten von Asset-Details über die Benutzeroberfläche

So bearbeiten Sie Asset-Details für ein einzelnes Asset:

1. Klicken Sie unter **Inventar** auf **Controller** oder **Netzwerk-Assets**.
2. Wählen Sie das gewünschte Asset aus.
3. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen**.

4. Wählen Sie im Dropdown-Menü **Bearbeiten** aus.
   Das Fenster **Asset-Details bearbeiten** wird geöffnet.



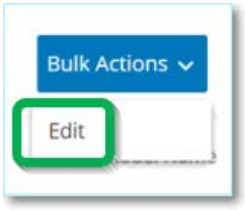
5. Wählen Sie im Feld **Typ** den Asset-Typ aus der Dropdown-Liste aus.
6. Geben Sie im Feld **Name** einen Namen ein, mit dem das Asset in der Benutzeroberfläche von Tenable.ot identifiziert wird.
7. Geben Sie im Feld **Kritikalität** die Kritikalität dieses Assets für das System ein.
8. Geben Sie im Feld **Purdue-Level** das Purdue Level basierend auf dem Asset-Typ ein.
9. Geben Sie im Feld **Backplane** (für Controller) den Namen der Backplane ein, auf der das Asset installiert ist.
10. Geben Sie im Feld **Standort** eine Beschreibung des Standorts des Assets ein. Dies ist ein optionales Feld. Die Daten werden in der Assets-Tabelle sowie im Bildschirm „Asset-Details“ für dieses Asset angezeigt.
11. Geben Sie im Feld **Beschreibung** eine Beschreibung des Assets ein. Dies ist ein optionales Feld. Die Daten werden im Bildschirm „Asset-Details“ für dieses Asset angezeigt.
12. Klicken Sie auf **Speichern**.
    Die bearbeiteten Details werden für dieses Asset gespeichert.

So bearbeiten Sie mehrere Assets (Massenprozess):

1. Klicken Sie unter **Inventar** auf **Controller** oder **Netzwerk-Assets**.
2. Aktivieren Sie das Kontrollkästchen neben den gewünschten Assets.

> Alternativ können Sie mehrere Assets auswählen, indem Sie die **Umschalttaste** gedrückt halten, während Sie auf jedes der gewünschten Assets klicken.

3. Klicken Sie auf das Menü **Massenaktionen** und wählen Sie **Bearbeiten** aus der Dropdown-Liste aus.



Der Bildschirm **Massenbearbeitung** wird mit den für die Massenbearbeitung verfügbaren Parametern angezeigt.

4. Aktivieren Sie das Kontrollkästchen neben jedem Parameter, den Sie bearbeiten möchten (*Typ*, *Kritikalität*, *Purdue-Level*, *Netzwerksegmente*, *Standort* und *Beschreibung*).

> Filtern Sie bei der Massenbearbeitung von Netzwerksegmenten zuerst Ihre Assets nach Typ aus und dann die Assets, die Sie per Massenvorgang bearbeiten möchten. Assets mit mehreren IP-Adressen können nicht in eine Massenbearbeitung für Netzwerksegmente aufgenommen werden. Sie müssen jedes Asset manuell bearbeiten.

5. Stellen Sie jeden Parameter wie gewünscht ein.

> Durch die in die Felder für die Massenbearbeitung eingegebenen Informationen werden alle aktuellen Inhalte für das ausgewählte Asset überschrieben. Wenn Sie das Kontrollkästchen neben einem Parameter aktivieren, aber keine Auswahl treffen, werden die aktuellen Werte für diesen Parameter gelöscht.

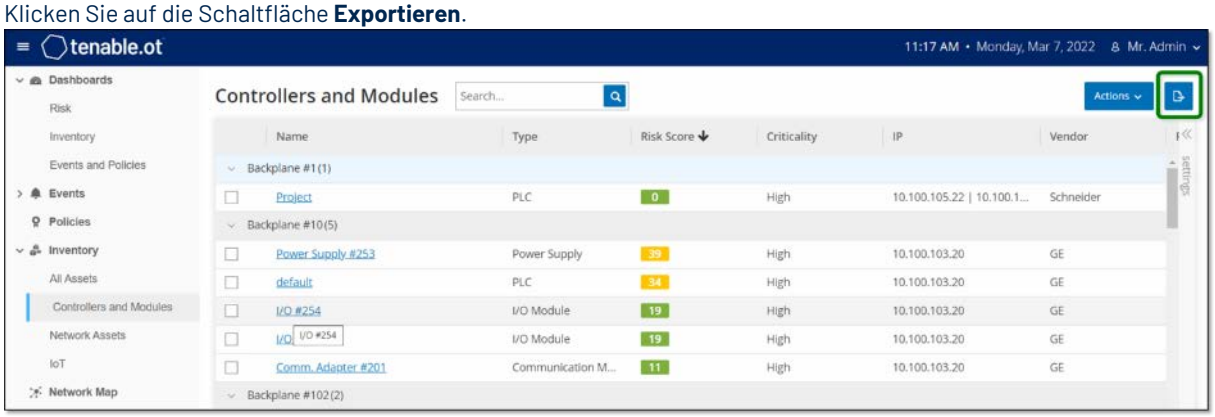
6. Klicken Sie auf **Speichern**.
   Die Assets werden mit der neuen Konfiguration gespeichert.

Bearbeiten von Asset-Details durch Hochladen einer CSV-Datei

Mit dieser Methode zum Bearbeiten von Asset-Details können Sie eine große Anzahl von Assets über eine CSV-Datei bearbeiten, anstatt sie manuell in der Benutzeroberfläche zu bearbeiten. Die folgenden Details können mit dieser Methode bearbeitet werden: *Typ*, *Name*, *Kritikalität*, *Purdue-Level*, *Standort*, *Beschreibung* und benutzerdefinierte Felder.

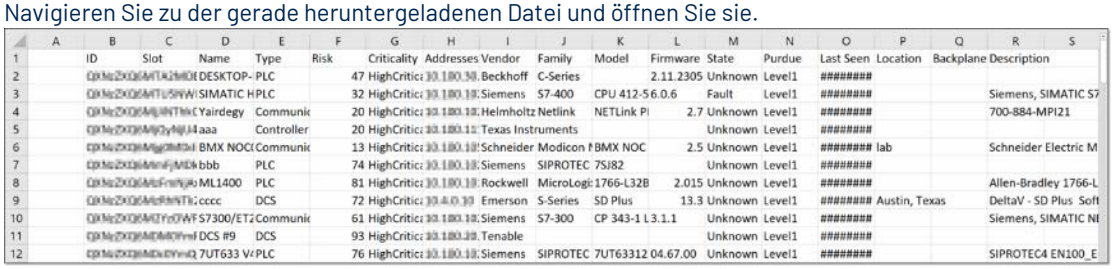
So bearbeiten Sie Asset-Details über eine CSV-Datei:

1. Klicken Sie unter **Inventar** auf **Alle Assets**, **Controller** und **Module** oder **Netzwerk-Assets**.
2. Klicken Sie auf die Schaltfläche **Exportieren**.



Eine CSV-Datei des Inventars wird heruntergeladen.

3. Navigieren Sie zu der gerade heruntergeladenen Datei und öffnen Sie sie.



	ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description
2			DESKTOP-	PLC		47 HighCritic		Beckhoff	C-Series		2.11.2305	Unknown	Level1	########			
3			SIMATIC H	PLC		32 HighCritic		Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	########			Siemens, SIMATIC S7
4			Yairdegy	Communic		20 HighCritic		Helmholtz	Netlink	NETLink PI	2.7	Unknown	Level1	########			700-884-MPI21
5			aaa	Controller		20 HighCritic		Texas Instruments				Unknown	Level1	########			
6			BMX NOC(	Communic		13 HighCritic		Schneider	Modicon M	BMX NOC	2.5	Unknown	Level1	########	lab		Schneider Electric M
7			bbb	PLC		74 HighCritic		Siemens	SIPROTEC	7SJ82		Unknown	Level1	########			
8			ML1400	PLC		81 HighCritic		Rockwell	MicroLogi	1766-L32B	2.015	Unknown	Level1	########			Allen-Bradley 1766-L
9			cccc	DCS		72 HighCritic		Emerson	S-Series	SD Plus	13.3	Unknown	Level1	########	Austin, Texas		DeltaV - SD Plus Soft
10			S7300/ET2	Communic		61 HighCritic		Siemens	S7-300	CP 343-1	3.1.1	Unknown	Level1	########			Siemens, SIMATIC NI
11			DCS #9	DCS		93 HighCritic		Tenable				Unknown	Level1	########			
12			7UT633 V4	PLC		76 HighCritic		Siemens	SIPROTEC	7UT6331	2 04.67.00	Unknown	Level1	########			SIPROTEC4 EN100_E

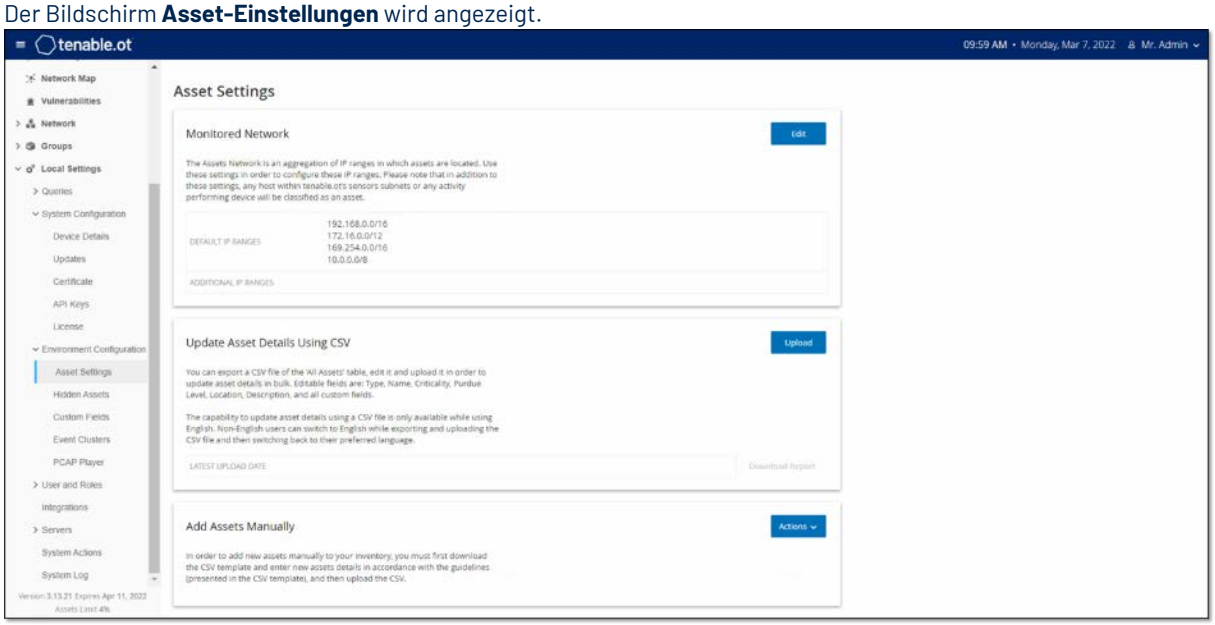
4. Bearbeiten Sie die zulässigen Parameter, indem Sie den Inhalt der Zellen ändern. (Zulässige Parameter: *Typ, Name, Kritikalität, Purdue-Level, Standort, Beschreibung und* benutzerdefinierte Felder.)

> Sie müssen gültige Daten für Parameter eingeben, die bestimmte Optionen erfordern (z. B. Typ, Kritikalität, Purdue-Level). Andernfalls kann das jeweilige Asset nicht aktualisiert werden.

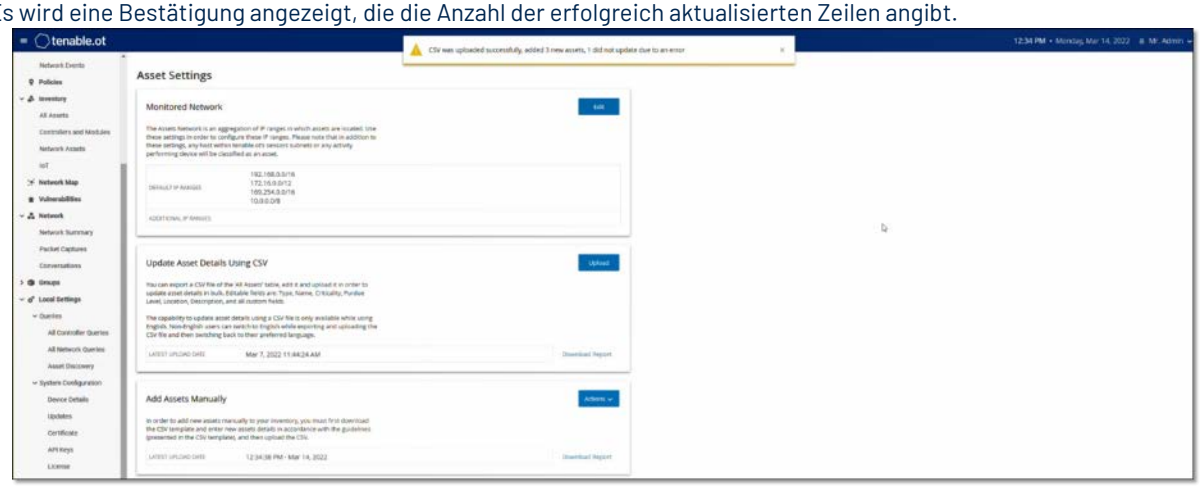
5. Speichern Sie die Datei als CSV-Dateityp.

> Nur die von Ihnen geänderten Assets werden im System aktualisiert. Assets, die nicht in der CSV-Datei enthalten sind, oder Zeilen, die Sie nicht geändert haben, bleiben im System unverändert. Es ist nicht möglich, Assets mit dieser Methode zu löschen.

6. Gehen Sie unter **Lokale Einstellungen** zu **Umgebungskonfiguration** > **Asset-Einstellungen**.
   Der Bildschirm **Asset-Einstellungen** wird angezeigt.



7. Klicken Sie im Abschnitt **Asset-Details per CSV aktualisieren** auf **Hochladen**.
8. Folgen Sie den Navigationsanweisungen Ihres Geräts, um die soeben gespeicherte CSV-Datei hochzuladen.
   Es wird eine Bestätigung angezeigt, die die Anzahl der erfolgreich aktualisierten Zeilen angibt.



   Das Feld **Datum des letzten Uploads** im Abschnitt „Asset-Details per CSV aktualisieren“ wird aktualisiert.
9. Wenn Sie weitere Informationen zu den Ergebnissen des Uploads sehen möchten, klicken Sie im Abschnitt **Asset-Details per CSV aktualisieren** auf **Bericht herunterladen**.
   Es wird eine CSV-Datei heruntergeladen, die angibt, welche Asset-IDs erfolgreich aktualisiert wurden und welche fehlgeschlagen sind.

Ausblenden von Assets

Sie können ein oder mehrere Assets aus der Asset-Inventarisierung ausblenden. Ein ausgeblendetes Asset wird nicht im Inventar angezeigt und aus Gruppen entfernt. Für das ausgeblendete Asset werden jedoch weiterhin Ereignisse und Netzwerkaktivitäten angezeigt.

Ein ausgeblendetes Asset kann über den Bildschirm **Lokale Einstellungen** > **Assets** > **Ausgeblendete Assets** wiederhergestellt werden, siehe **Lokale Einstellungen**.

So blenden Sie ein oder mehrere Assets aus:

1. Klicken Sie unter **Inventar** auf **Controller** oder **Netzwerk-Assets**.
2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Assets, die Sie entfernen möchten.
3. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen**.
4. Wählen Sie im Dropdown-Menü **Asset ausblenden** aus.
   Das Fenster **Ausgeblendete Assets** wird geöffnet.
5. Im Feld **Kommentare** können Sie Freitextkommentare zu den Assets hinzufügen. (Optional)

> Kommentare werden in der Liste der entfernten Assets im Bildschirm **Lokale Einstellungen** > **Assets** > **Ausgeblendete Assets** angezeigt.

6. Klicken Sie auf **Ausblenden**.
   Die Assets werden aus dem Inventar und den Gruppen ausgeblendet.

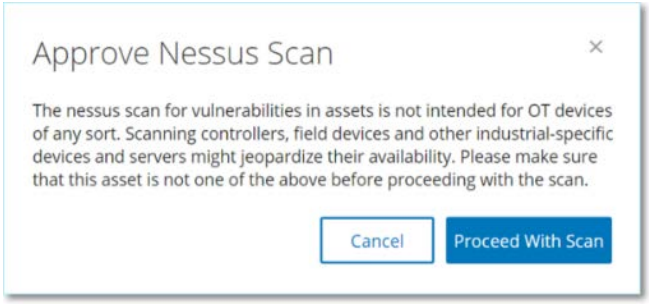
Durchführen eines Asset-spezifischen Nessus-Scans

Nessus ist ein Tenable-Tool, das IT-Geräte scannt, um Schwachstellen zu erkennen. Mit Tenable.ot können Sie den Nessus „Basic Network Scan" für spezifische IT Assets in Ihrem OT-Netzwerk durchführen. Dies ist ein aktiver Scan des gesamten Systems, der zusätzliche Informationen über Schwachstellen auf den Servern und Netzwerkgeräten sammelt. Dieser Scan verwendet die WMI- und SNMP-Zugangsdaten, wenn diese vom Benutzer bereitgestellt wurden. Diese Aktion ist nur für relevante PC-basierte Maschinen verfügbar. Die Ergebnisse des Scans werden im Bildschirm **Schwachstellen** angezeigt. Sie können auch benutzerdefinierte Scans erstellen, um einen bestimmten Satz von Nessus-Plugins für einen bestimmten Satz von Netzwerkressourcen auszuführen, siehe **Nessus-Plugin-Scans**.

> Nessus ist ein invasives Tool, das am besten in IT-Umgebungen funktioniert. Es wird nicht für die Verwendung auf OT-Geräten empfohlen, da es deren normalen Betrieb beeinträchtigen kann.

So führen Sie einen Nessus-Scan manuell aus:

1. Klicken Sie unter **Inventar** auf **Netzwerk-Assets**.
2. Wählen Sie das gewünschte Asset aus.
3. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen**.
4. Wählen Sie im Dropdown-Menü **Nessus-Scan** aus.
   Das Bestätigungsfenster **Nessus-Scan genehmigen** wird angezeigt.



5. Klicken Sie auf **Mit Scan fortfahren**.
   Der Nessus-Scan wird ausgeführt.

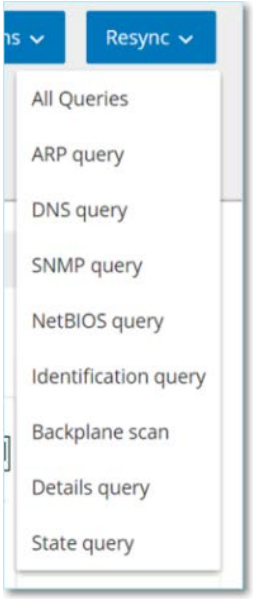
Durchführen einer erneuten Synchronisierung

Die Funktion „Erneut synchronisieren" initiiert eine oder mehrere Abfragen an das Netzwerk und den Controller, um aktuelle Informationen für dieses Asset zu erfassen. Sie können alle verfügbaren Abfragen ausführen oder bestimmte Abfragen auswählen, die ausgeführt werden sollen. Die folgenden Abfragen sind für die Funktion „Erneut synchronisieren" verfügbar:

- **Backplane-Scan** – Erfasst Module und ihre Spezifikationen innerhalb einer Backplane.
- **DNS-Scanning** – Sucht nach den DNS-Namen der Assets im Netzwerk.
- **Detailabfrage** – Ruft die Details zur Hardware und Firmware des Controllers ab. Das Ergebnis wird im Feld **Firmware** angezeigt, das sich im Bildschirm **Assets > Controller** befindet.
- **Identifizierungsabfrage** – Verwendet mehrere Protokolle, um zu versuchen, das Asset zu identifizieren.
- **NetBIOS-Abfrage** – Sendet ein NetBIOS-Unicast-Paket, mit dem Windows-Computer im Netzwerk klassifiziert und ermittelt werden.
- **SNMP-Abfrage** (für SNMP-fähige Assets) – Ruft Konfigurationsdetails für SNMP-fähige Assets ab.
- **Status** – Erkennt den aktuellen Status des Assets (d. h. „Wird ausgeführt", „Gestoppt", „Fehler", „Keine Konfig." und „Test").
- **ARP** – Ruft die MAC-Adresse neuer IP-Adressen ab, die im Netzwerk erkannt wurden. Das Ergebnis wird im Feld **MAC** angezeigt, das sich im Bildschirm **Details > Übersicht** befindet.

So führen Sie die erneute Synchronisierung von Asset-Daten aus:

1. Klicken Sie im Bildschirm **Asset-Details** für das gewünschte Asset auf die Schaltfläche **Erneut synchronisieren** im Kopfbereich.
2. Eine Dropdown-Liste mit Abfragen wird angezeigt.



3. Klicken Sie auf die Abfrage, die Sie ausführen möchten, ODER klicken Sie auf *Alle Abfragen*, um alle verfügbaren Abfragen auszuführen.
4. Während die einzelnen Abfragen ausgeführt werden, zeigt eine Popup-Benachrichtigung den Status der Abfrage an.

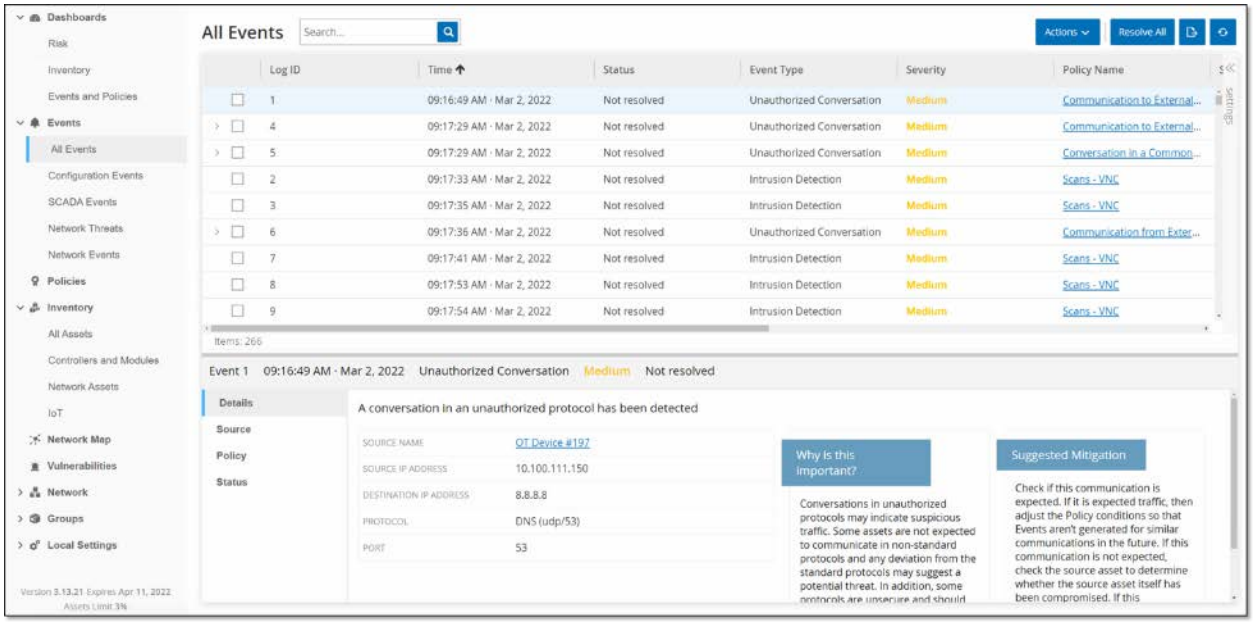
Für jede erfolgreich ausgeführte Abfrage werden die Systemdaten für dieses Asset basierend auf den neuen Daten aktualisiert.

EREIGNISSE

Ereignisse sind Benachrichtigungen, die im System generiert wurden, um auf potenziell schädliche Aktivitäten im Netzwerk aufmerksam zu machen. Ereignisse werden von Richtlinien generiert, die im System in einer der folgenden Kategorien eingerichtet sind: *Konfigurationsereignisse*, *SCADA-Ereignisse*, *Netzwerkbedrohungen* oder *Netzwerkereignisse*. Jeder Richtlinie wird ein Schweregrad zugewiesen, der den Schweregrad des Ereignisses angibt.

Sobald eine Richtlinie aktiviert wurde, löst jedes Ereignis im System, das den Richtlinienbedingungen entspricht, ein Ereignisprotokoll aus. Mehrere Ereignisse mit denselben Merkmalen werden in einem einzigen Cluster zusammengefasst.

Anzeigen von Ereignissen



Alle Ereignisse, die im System aufgetreten sind, werden im Bildschirm **Alle Ereignisse** angezeigt. Spezifische Teilmengen der Ereignisse werden auf separaten Bildschirmen für jede der folgenden Ereigniskategorien angezeigt: **Konfigurationsereignisse**, **SCADA-Ereignisse**, **Netzwerkbedrohungen** und **Netzwerkereignisse**.

Oben im Bildschirm wird ein Eintrag für jedes Ereignis angezeigt. Für jeden Ereignisbildschirm (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen und Netzwerkereignisse) können Sie die Anzeigeeinstellungen anpassen, indem Sie anpassen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Die Ereignisse können nach verschiedenen Kategorien gruppiert werden (z. B. Ereignistyp, Schweregrad, Richtlinienname). Sie können die Ereignislisten auch sortieren und filtern sowie nach Text suchen. Eine Erläuterung der Anpassungsfunktionen finden Sie unter **Arbeiten mit Listen**.

In der Kopfleiste befindet sich eine Schaltfläche **Aktionen**, mit der Sie die folgende Aktion für die ausgewählten Ereignisse ausführen können:

- Auflösen – Markieren Sie dieses Ereignis als „Aufgelöst".
- PCAP herunterladen – Laden Sie die PCAP-Datei für dieses Ereignis herunter.
- Ausschließen – Erstellen Sie einen Richtlinienausschluss für dieses Ereignis.

Detaillierte Informationen zu diesen Aktionen finden Sie in den folgenden Abschnitten.

Unten im Bildschirm werden auf verschiedenen Registerkarten detaillierte Informationen zum ausgewählten Ereignis angezeigt. Es werden nur Registerkarten angezeigt, die für den Ereignistyp des ausgewählten Ereignisses relevant sind. Die folgenden Registerkarten werden für verschiedene Arten von Ereignissen angezeigt: *Details*, *Code*, *Quelle*, *Ziel*, *Richtlinie*, *gescannte Ports* und *Status*.

Sie können die Bereichstrennlinie nach oben oder unten ziehen, um die Anzeige des unteren Bereichs zu vergrößern/verkleinern.

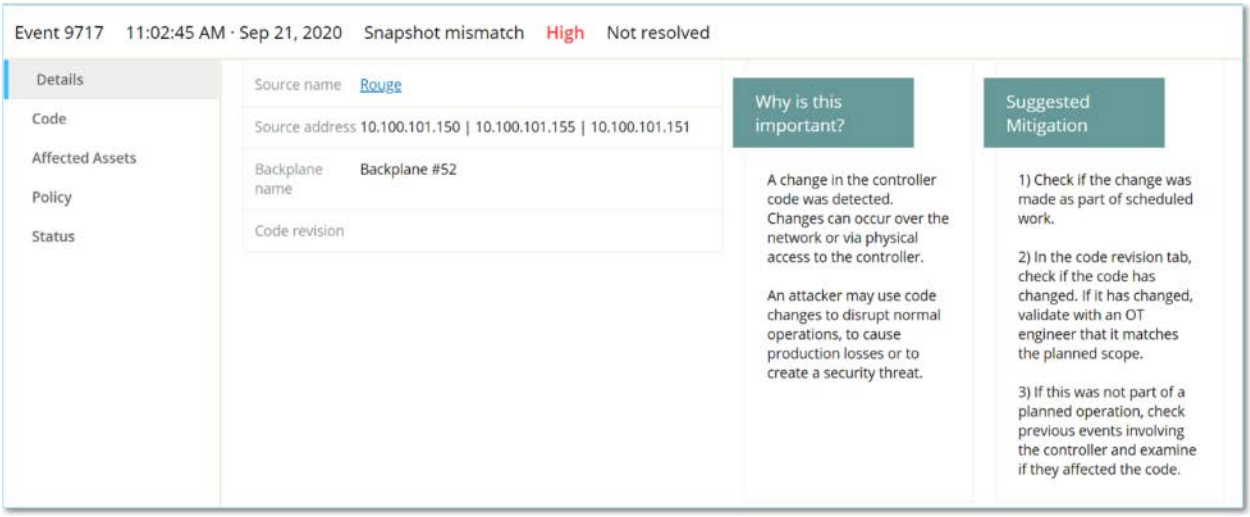
Sie können die mit jedem Ereignis verknüpfte Paketerfassungsdatei herunterladen, siehe **Herunterladen von Dateien**.

Die für die einzelnen Ereignislisten angezeigten Informationen werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Name	Der Name des Geräts im Netzwerk. Klicken Sie auf den Namen des Assets, um den Bildschirm „Asset-Details" für dieses Asset anzuzeigen (siehe **Anzeigen von Asset-Details**).
Adressen	Die IP- und/oder MAC-Adresse des Assets. **Hinweis:** Ein Asset kann mehrere IP-Adressen haben.
Typ	Der Asset-Typ. Eine Erläuterung der verschiedenen Asset-Typen finden Sie unter **Asset-Typen**.
Backplane	Die Backplane-Einheit, mit der der Controller verbunden ist. Weitere Details zur Backplane-Konfiguration werden im Bildschirm „Asset-Details" angezeigt.
Slot	Bei Controllern, die sich auf Backplanes befinden, wird die Nummer des Steckplatzes angezeigt, an den der Controller angeschlossen ist.
Anbieter	Der Asset-Anbieter.
Familie	Der vom Controller-Anbieter definierte Name der Produktfamilie.
Firmware	Die aktuell auf dem Controller installierte Firmware-Version.
Standort	Der Standort des Assets, wie er vom Benutzer in den Asset-Details in Tenable.ot eingegeben wurde. Siehe **Bearbeiten von Asset-Details**.
Zuletzt gesehen	Der Zeitpunkt, zu dem das Gerät zuletzt von Tenable.ot gesehen wurde. Dies ist das letzte Mal, dass das Gerät mit dem Netzwerk verbunden war oder eine Aktivität durchgeführt hat.
Betriebssystem	Das Betriebssystem, das auf dem Asset ausgeführt wird.
Protokoll-ID	Die vom System generierte ID, um auf das Ereignis zu verweisen.
Uhrzeit	Das Datum und die Uhrzeit des Ereignisses.
Ereignistyp	Beschreibt die Art der Aktivität, die das Ereignis ausgelöst hat. Ereignisse werden von Richtlinien generiert, die im System eingerichtet sind. Eine Erläuterung der verschiedenen Arten von Richtlinien finden Sie unter **Richtlinientypen**.

Parameter	Beschreibung
Schweregrad	Zeigt den Schweregrad des Ereignisses an. Nachfolgend finden Sie eine Erläuterung zu den möglichen Werten: Kein – Kein Grund zur Besorgnis. **Info** – Kein unmittelbarer Grund zur Sorge. Sollte bei Gelegenheit geprüft werden. **Warnung** – Moderate Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte behandelt werden, wenn es passt. **Kritisch** – Schwerwiegende Bedenken, dass potenziell schädliche Aktivitäten stattgefunden haben. Sollte sofort behandelt werden.
Richtlinienname	Der Name der Richtlinie, die das Ereignis generiert hat. Der Name ist ein Link zur Richtlinienliste.
Quell-Asset	Der Name des Assets, das das Ereignis initiiert hat. Dieses Feld ist ein Link zur Asset-Liste.
Quelladresse	Die IP- oder MAC-Adresse des Assets, das das Ereignis initiiert hat.
Ziel-Asset	Der Name des Assets, das von dem Ereignis betroffen war. Dieses Feld ist ein Link zur Asset-Liste.
Zieladresse	Die IP- oder MAC-Adresse des Assets, das von dem Ereignis betroffen war.
Protokoll	Sofern relevant, wird hier das Protokoll angezeigt, das für die Konversation verwendet wurde, die dieses Ereignis ausgelöst hat.
Ereigniskategorie	Zeigt die allgemeine Kategorie des Ereignisses an. **Hinweis:** Im Bildschirm „Alle Ereignisse" werden Ereignisse aller Art angezeigt. Auf jedem der spezifischen Ereignisbildschirme werden nur Ereignisse der angegebenen Kategorie angezeigt. Im Folgenden finden Sie eine kurze Erläuterung der Ereigniskategorien (für eine ausführlichere Erläuterung siehe **Richtlinienkategorien**): • Konfigurationsereignisse – Dies umfasst zwei Unterkategorien. • Controller-Validierungsereignisse – Diese Richtlinien erkennen Änderungen, die in den Controllern im Netzwerk stattfinden. • Controller-Aktivitätsereignisse – Aktivitätsrichtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden (d. h. die „Befehle", die zwischen Assets im Netzwerk implementiert werden). • SCADA-Ereignisse – Richtlinien, die Änderungen identifizieren, die an der Datenebene von Controllern vorgenommen wurden. • Netzwerkbedrohungsereignisse – Diese Richtlinien identifizieren Netzwerk-Traffic, der auf Bedrohungen durch Eindringlinge hinweist. • Netzwerkereignisse – Richtlinien, die sich auf die Assets im Netzwerk und die Kommunikationsströme zwischen Assets beziehen.
Status	Zeigt an, ob das Ereignis als aufgelöst markiert wurde oder nicht.
Aufgelöst von	Zeigt für aufgelöste Ereignisse an, welcher Benutzer das Ereignis als aufgelöst markiert hat.
Aufgelöst am	Zeigt für aufgelöste Ereignisse an, wann das Ereignis als aufgelöst markiert wurde.
Kommentar	Zeigt alle Kommentare an, die hinzugefügt wurden, als das Ereignis aufgelöst wurde.

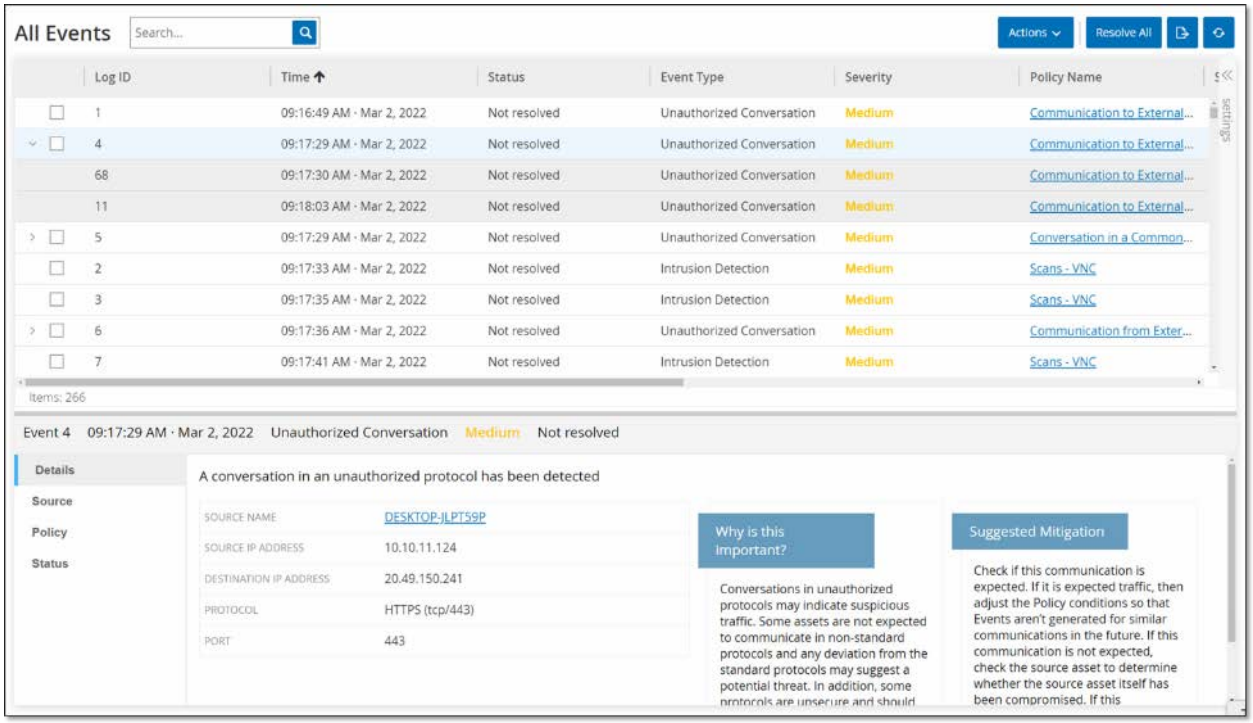
Anzeigen von Ereignisdetails



Unten im Bildschirm „Ereignisse" werden zusätzliche Details zum ausgewählten Ereignis angezeigt. Die Informationen sind in Registerkarten unterteilt. Es werden nur Registerkarten angezeigt, die für das ausgewählte Ereignis relevant sind. Die detaillierten Informationen enthalten Links zu zusätzlichen Informationen über die relevanten Entitäten (Quell-Asset, Ziel-Asset, Richtlinie, Gruppe usw.).

- **Kopfleiste** – Zeigt einen Überblick über wichtige Informationen über das Ereignis.
- **Details** – Gibt eine kurze Beschreibung des Ereignisses sowie eine Erklärung, warum diese Informationen wichtig sind, und schlägt Schritte vor, die unternommen werden sollten, um den durch das Ereignis verursachten potenziellen Schaden zu mindern. Darüber hinaus werden die Quell- und Ziel-Assets angezeigt, die an dem Ereignis beteiligt waren.
- **Regeldetails** (für Intrusion Detection-Ereignisse) – Zeigt Informationen über die Suricata-Regel an, die für das Ereignis gilt.
- **Code** – Diese Registerkarte wird für Controller-Aktivitäten wie Code-Download und -Upload, HW-Konfiguration und Code-Löschung angezeigt. Sie enthält detaillierte Informationen über den relevanten Code, einschließlich spezifischer Codeblöcke, Zeilen und Tags. Die Codeelemente werden in einer Baumstruktur mit Pfeilen zum Erweitern/Minimieren der angezeigten Details angezeigt.
- **Quelle** – Zeigt detaillierte Informationen über das Quell-Asset für dieses Ereignis.
- **Ziel** – Zeigt detaillierte Informationen über das Ziel-Asset für dieses Ereignis.
- **Betroffenes Asset** – Zeigt detaillierte Informationen über das von diesem Ereignis betroffene Asset.
- **Gescannte Ports** (für Port-Scan-Ereignisse) – Zeigt die gescannten Ports an.
- **Gescannte Adressen** (für ARP-Scan-Ereignisse) – Zeigt die gescannten Adressen an.
- **Richtlinie** – Zeigt detaillierte Informationen über die Richtlinie, die das Ereignis ausgelöst hat.
- **Status** – Zeigt an, ob das Ereignis als aufgelöst markiert wurde oder nicht. Für aufgelöste Ereignisse werden Details dazu angezeigt, welcher Benutzer sie als aufgelöst markiert haben und wann sie aufgelöst wurden.

Anzeigen von Ereignisclustern



Um die Überwachung von Ereignissen zu vereinfachen, werden mehrere Ereignisse mit denselben Merkmalen in einem einzigen Cluster zusammengefasst. Das Clustering basiert auf dem Ereignistyp (d. h. Nutzung derselben Richtlinie), Quell- und Ziel-Assets und dem Zeitraum, in dem die Ereignisse auftreten. Informationen zum Konfigurieren von Ereignisclustern finden Sie unter **Ereigniscluster**.

Geclusterte Ereignisse sind mit einem Pfeil neben der Protokoll-ID gekennzeichnet. Wenn Sie die einzelnen Ereignisse in einem Cluster anzeigen möchten, klicken Sie auf den Datensatz, um die Liste zu erweitern.

Auflösen von Ereignissen

Sobald ein autorisierter Techniker ein Ereignis bewertet und die erforderlichen Maßnahmen zur Behebung des Problems ergriffen hat oder festgestellt hat, dass kein Handlungsbedarf besteht, sollte das Ereignis als *Aufgelöst* gekennzeichnet werden. Beim Auflösen eines Ereignisses, das Teil eines Clusters ist, werden alle Ereignisse in diesem Cluster als aufgelöst markiert. Sie können mehrere Ereignisse auswählen, um sie in einem Sammelvorgang als aufgelöst zu markieren. Sie können auch alle Ereignisse (oder alle Ereignisse einer bestimmten Kategorie) gleichzeitig als aufgelöst markieren.

Auflösen einzelner Ereignisse

➡ So markieren Sie bestimmte Ereignisse als aufgelöst:

1. Aktivieren Sie im entsprechenden Bildschirm für **Ereignisse** (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse) das Kontrollkästchen neben einem oder mehreren Ereignissen, die Sie als aufgelöst markieren möchten.
2. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen**.

Auch wenn Sie mehrere Ereignisse als aufgelöst markieren, müssen Sie auf die Schaltfläche *Auflösen* klicken, um alle ausgewählten Ereignisse aufzulösen, und **nicht** auf die Schaltfläche *Alle auflösen*. Die Schaltfläche *Alle auflösen* wird verwendet, um alle Ereignisse aufzulösen, auch diejenigen, die nicht ausgewählt sind.

3. Wählen Sie im Dropdown-Menü **Auflösen** aus.
   Das Fenster **Ereignis auflösen** wird angezeigt.

4. Im Feld **Kommentar** können Sie einen Kommentar hinzufügen, der die zur Behebung des Problems bzw. der Probleme ausgeführten Risikominderungsschritte beschreibt. (Optionales Feld)
5. Klicken Sie auf **Auflösen**.
   Der Status der ausgewählten Ereignisse wird in *Aufgelöst* geändert.

Auflösen aller Ereignisse

Die Aktion **Alle auflösen** gilt für alle Ereignisse im aktuellen Bildschirm (d. h., wenn der Bildschirm „Konfigurationsereignisse" geöffnet ist, werden mit „Alle auflösen" alle Konfigurationsereignisse aufgelöst, aber keine SCADA-Ereignisse usw.), basierend auf den aktuell auf die Anzeige angewendeten Filtern. Bei geclusterten Ereignissen werden alle Ereignisse im Cluster als aufgelöst markiert.

So markieren Sie alle Ereignisse als aufgelöst:

1. Klicken Sie im entsprechenden Bildschirm für **Ereignisse** (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse) in der Kopfleiste auf **Alle auflösen**.

2. Das Fenster **Alle Ereignisse auflösen** wird mit der Anzahl der aufzulösenden Ereignisse in der oberen rechten Ecke angezeigt.

3. Im Feld **Kommentar** können Sie einen Kommentar zu der Gruppe von Ereignissen hinzufügen, die aufgelöst werden sollen. (Optionales Feld)
4. Klicken Sie auf **Auflösen**.
   Die Warnmeldung wird angezeigt.
5. Klicken Sie auf **Auflösen**.
   Alle Ereignisse in der aktuellen Anzeige werden als aufgelöst markiert.

Erstellen von Richtlinienausschlüssen

Wenn Sie feststellen, dass eine Richtlinie Ereignisse für bestimmte Bedingungen generiert, die keine Sicherheitsbedrohung darstellen, können Sie diese Bedingungen aus der Richtlinie *ausschließen* (d. h. es sollen keine Ereignisse mehr für diese bestimmten Bedingungen generiert werden). Ein Beispiel: Wenn eine Richtlinie Änderungen des Controller-Status erkennt, die während der Arbeitszeit auftreten, Sie jedoch feststellen, dass Statusänderungen während dieser Zeiten für einen bestimmten Controller normal sind, können Sie diesen Controller aus der Richtlinie *ausschließen*.

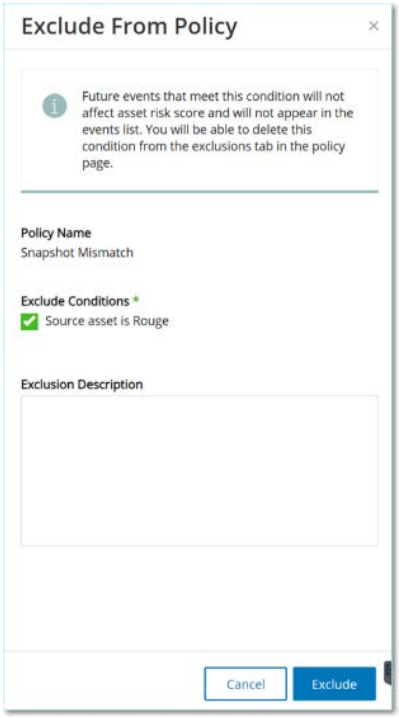
Ausschlüsse werden über den Bildschirm „Ereignisse“ erstellt, basierend auf Ereignissen, die von Ihren Richtlinien generiert wurden. Sie können angeben, welche Bedingungen eines bestimmten Ereignisses Sie aus der Richtlinie ausschließen möchten.

Wenn Sie die Generierung von Ereignissen für die angegebenen Bedingungen zu einem späteren Zeitpunkt fortsetzen möchten, können Sie den Ausschluss löschen, wie unter **Löschen von Richtlinienausschlüssen** beschrieben.

So erstellen Sie einen Richtlinienausschluss:

1. Wählen Sie im entsprechenden Bildschirm für **Ereignisse** (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse) das Ereignis aus, für das Sie einen Ausschluss erstellen möchten.
2. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen** (oder klicken Sie mit der rechten Maustaste auf das Ereignis).
   Das Menü **Aktionen** wird angezeigt.
3. Klicken Sie auf **Aus Richtlinie ausschließen**.
   Das Fenster **Aus Richtlinie ausschließen** wird geöffnet.
4. Im Abschnitt **Ausschlussbedingungen** sind standardmäßig alle Bedingungen ausgewählt (wodurch Ereignisse mit *irgendeiner* der angegebenen Bedingungen aus der Richtlinie ausgeschlossen werden). Sie können das Kontrollkästchen neben jeder Bedingung **deaktivieren**, für die weiterhin Ereignisse generiert werden sollen.

Wenn Sie beispielsweise im unten gezeigten Dialogfeld die angegebenen Quell- und Ziel-Assets und -IP-Adressen aus dieser Richtlinie ausschließen möchten, diese Richtlinie jedoch weiterhin auf UDP-Konversationen zwischen anderen Assets im Netzwerk angewendet werden soll, deaktivieren Sie die Bedingung „Protokoll ist UDP“.



Welche Bedingungen ausgeschlossen werden können, hängt vom Richtlinientyp ab, siehe Tabelle unten.

5. Im Feld **Ausschlussbeschreibung** können Sie einen Kommentar zum Ausschluss hinzufügen (optional).
6. Klicken Sie auf **Ausschließen**.
   Der Ausschluss wird erstellt.

Die folgende Tabelle zeigt die Bedingungen, die für die einzelnen Ereignistypen ausgeschlossen werden können.

Richtlinienkategorie	Ereignistyp	Ausschließbare Bedingungen
Controller-Aktivitäten	Konfigurationsereignisse (d. h. Aktivitäten)	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
Controller-Validierung	Änderung des Schlüsselstatus	• Quell-Asset
	Änderung des Controller-Status	• Quell-Asset
	Änderung der FW-Version	• Quell-Asset
	Modul nicht gesehen	• Quell-Asset
	Snapshot-Konflikt	• Quell-Asset
Netzwerk	Asset nicht gesehen	• Quell-Asset
	Änderung der USB-Konfiguration	• Quell-Asset • USB-Geräte-ID
	IP-Konflikt	• MAC-Adressen • IP-Adresse
	Netzwerk-Baseline-Abweichung	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP • Protokoll
	Offener Port	• Quell-Asset • Quell-IP • Port
	RDP-Verbindung	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
	Nicht autorisierte Konversation	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP • Protokoll
	FTP-Login (fehlgeschlagen und erfolgreich)	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
	Telnet-Login (Versuch, fehlgeschlagen und erfolgreich)	• Quell-Asset • Quell-IP • Ziel-Asset

Richtlinienkategorie	Ereignistyp	Ausschließbare Bedingungen
		• Ziel-IP
Netzwerkbedrohung	Intrusion Detection	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP • SID
	ARP-Scan	• Quell-Asset • Quell-IP
	Port-Scan	• Quell-Asset • Quell-IP
SCADA	Unzulässige Modbus-Datenadresse	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
	Unzulässiger Modbus-Datenwert	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
	Unzulässige Modbus-Funktion	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
	Nicht autorisierter Schreibvorgang	• Quell-Asset • Ziel-Asset • Tag-Name
	IEC60870-5-104 StartDT IEC60870-5-104 StopDT	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP
	IEC60870-5-104 Funktionscode-basierte Ereignisse	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP • COT
	DNP3-Ereignisse	• Quell-Asset • Quell-IP • Ziel-Asset • Ziel-IP • DNP3-Quelladresse • DNP3-Zieladresse

Herunterladen einzelner Erfassungsdateien

Tenable.ot speichert die zugehörigen Paketerfassungsdaten jedes Ereignisses im Netzwerk. Die Daten werden als PCAP-Dateien gespeichert, die heruntergeladen und mit Tools zur Analyse von Netzwerkprotokollen (z. B. Wireshark usw.) analysiert werden können. In diesem Abschnitt wird erläutert, wie Sie die PCAP-Datei für ein einzelnes Ereignis herunterladen. Sie können auch PCAP-Dateien für das gesamte Netzwerk herunterladen, siehe **PAKETERFASSUNGEN**.

PCAP-Dateien sind nur verfügbar, wenn die Funktion „Paketerfassung“ aktiviert ist. Die Funktion „Paketerfassung“ kann über den Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Paketerfassungen** aktiviert werden, siehe **PAKETERFASSUNGEN**.

PCAP-Dateien sind nur für Ereignisse verfügbar, die sich auf Netzwerkaktivitäten beziehen, z. B. Controller-Aktivitäten, Netzwerkbedrohungen, SCADA-Ereignisse und einige Arten von Netzwerkereignissen.

Herunterladen einer PCAP-Datei

So laden Sie eine PCAP-Datei herunter:

1. Aktivieren Sie im Bildschirm **Ereignisse** das Kontrollkästchen neben dem Ereignis, für das Sie die PCAP-Datei herunterladen möchten.
2. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen**.
3. Wählen Sie im Dropdown-Menü **Erfassungsdatei herunterladen** aus.
   Die gezippte PCAP-Datei wird auf Ihren lokalen Computer heruntergeladen.

Erstellen von FortiGate-Richtlinien

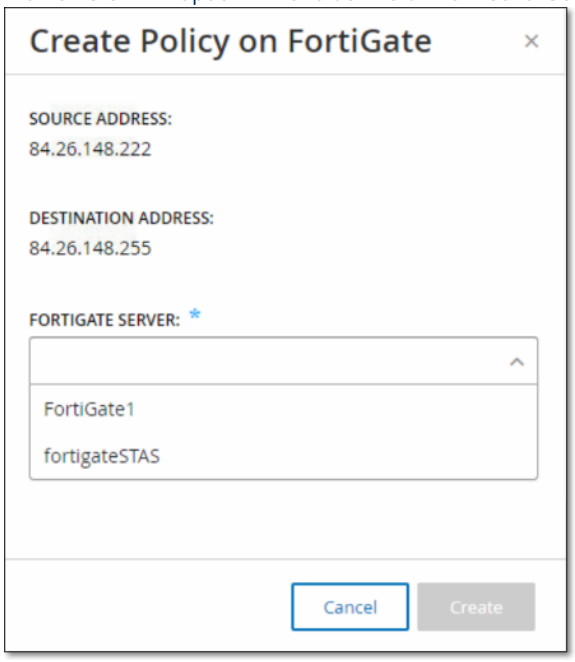
Die FortiGate-Integration ermöglicht es Ihnen, bestimmte Tenable.ot-Ereignisse zu verwenden, um Firewall-Richtlinien/-Regeln in der FortiGate Next Generation Firewall (NGFW) zu erstellen. Die Ereignistypen, für die diese Funktion zur Verfügung steht (unterstützte Ereignisse), sind *Baseline-Abweichung*, *Nicht autorisierte Konversation*, *Intrusion Detection* und *RDP-Verbindung (authentifiziert und nicht authentifiziert)*. Die FortiGate-Richtlinie wird automatisch so eingestellt, dass sie für die Quell- und Ziel-Assets gilt, die am Tenable.ot-Ereignis beteiligt waren. Standardmäßig bewirkt die Richtlinie, dass FortiGate Traffic des angegebenen Typs ablehnt (d. h. blockiert). Ein FortiGate-Administrator kann die Richtlinieneinstellungen in der FortiGate-Anwendung anpassen.

Bevor Sie FortiGate-Richtlinien vorschlagen können, müssen Sie die Integration für Ihren FortiGate-Firewall-Server mit Tenable.ot einrichten. Siehe **FORTIGATE-FIREWALL**.

So schlagen Sie eine FortiGate-Richtlinie vor:

1. Wählen Sie im entsprechenden Bildschirm für **Ereignisse** (*Konfigurationsereignisse*, *SCADA-Ereignisse*, *Netzwerkbedrohungen* oder *Netzwerkereignisse*) das Ereignis aus, für das Sie eine FortiGate-Richtlinie erstellen möchten.
2. Klicken Sie in der Kopfleiste auf die Schaltfläche **Aktionen** (oder klicken Sie mit der rechten Maustaste auf das Ereignis).
3. Wählen Sie im Dropdown-Menü **FortiGate-Richtlinie erstellen** aus.
   Das Fenster **Richtlinie auf FortiGate erstellen** wird geöffnet. Die Felder **Quelladresse** und **Zieladresse** der am Tenable.ot-Ereignis beteiligten Assets sind bereits ausgefüllt.

4. Wählen Sie im Dropdown-Menü des Felds **FortiGate-Server** den gewünschten Server aus.



5. Klicken Sie auf **Erstellen**.
   Die Richtlinie wird in FortiGate erstellt und das Fenster wird geschlossen.
6. Sie können die neue Richtlinie in der FortiGate-Anwendung anzeigen.

7. Ein FortiGate-Administrator kann die Einstellungen nach Wunsch anpassen.

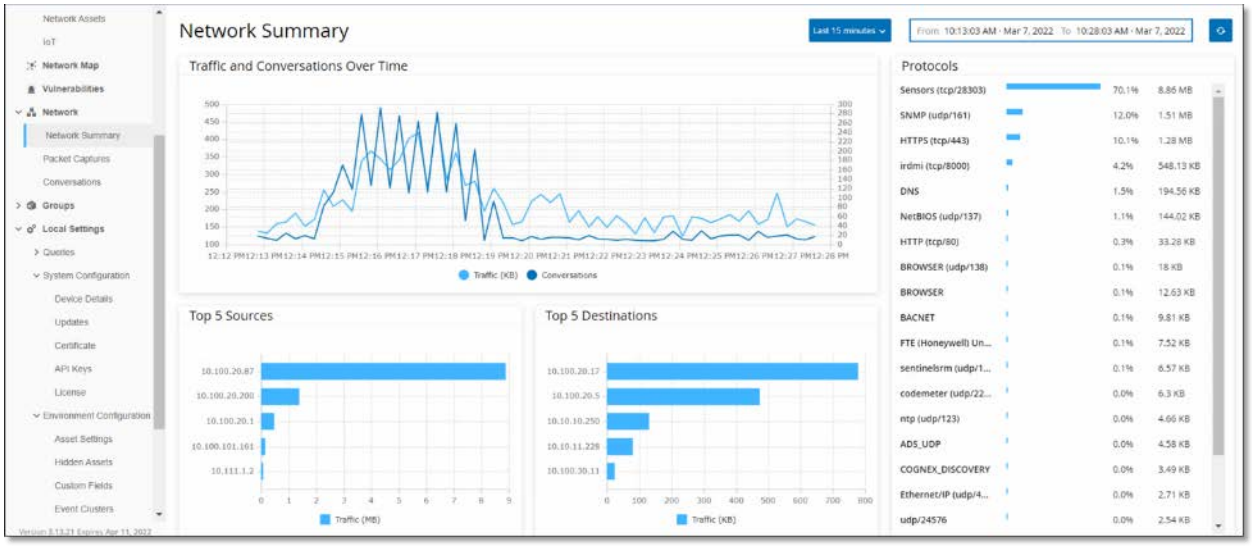
NETZWERK

Tenable.ot überwacht alle Aktivitäten in Ihrem Netzwerk. Diese Informationen werden im Abschnitt **Netzwerk** der Benutzeroberfläche angezeigt.

Es sind drei Bildschirme mit Netzwerkdaten vorhanden.

- **NETZWERK – ZUSAMMENFASSUNG** – Zeigt eine Übersicht der Netzwerkaktivität.
- **PAKETERFASSUNGEN** – Zeigt eine Liste der vom System erfassten PCAP-Dateien.
- **KONVERSATIONEN** – Zeigt eine Liste aller im Netzwerk erkannten Konversationen mit Details über den Zeitpunkt, an dem sie stattgefunden haben, beteiligte Assets usw.

Netzwerk – Zusammenfassung



Der Bildschirm **Netzwerk – Zusammenfassung** enthält visuelle Diagramme, die einen Überblick über die Netzwerkaktivitäten geben. Sie können den Zeitraum festlegen, für den die Daten angezeigt werden. Sie können auch mit den Widgets interagieren, um zusätzliche Details anzuzeigen.

Der Bildschirm enthält vier Widgets:

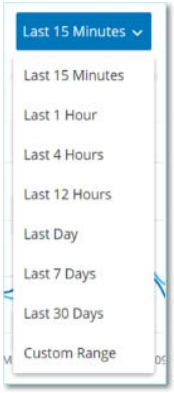
- **Traffic und Konversationen im zeitlichen Verlauf** – Dieses Diagramm zeigt das Traffic-Volumen in GB/MB und die Anzahl der im Netzwerk stattfindenden Konversationen an.
- **Top 5 Quellen** – Dieses Säulendiagramm zeigt die fünf Quell-Assets an, die die meiste Netzwerkaktivität initiiert haben. Das Diagramm enthält für jede Quelle einen Balken, der das Traffic-Volumen darstellt. Wenn Sie den Mauszeiger über das Diagramm bewegen, wird die Anzahl der Konversationen in einer QuickInfo angezeigt.
- **Top 5 Ziele** – Dieses Säulendiagramm zeigt die fünf Ziel-Assets an, die die meiste Netzwerkaktivität empfangen haben. Das Diagramm enthält für jedes Ziel einen Balken, der das eingehende Traffic-Volumen darstellt. Wenn Sie den Mauszeiger über das Diagramm bewegen, wird die Anzahl der Konversationen in einer QuickInfo angezeigt.
- **Protokolle** – Dieses Balkendiagramm zeigt die im Netzwerk verwendeten Kommunikationsprotokolle sortiert nach Frequenz an. Das Diagramm zeigt für jedes Protokoll die Nutzungsrate (als Prozentsatz des gesamten Traffic) und das Traffic-Volumen an.

Festlegen des Zeitraums

Alle im Netzwerk-Bildschirm angezeigten Daten stellen Aktivität im Netzwerk während eines bestimmten Zeitraums dar. Der Zeitraum, für den Daten aktuell angezeigt werden, ist in der Kopfleiste angegeben. Der Standardzeitraum ist auf *Letzte 15 Minuten* festlegt. Die *Startzeit* und die *Endzeit* des ausgewählten Zeitraums werden in der Kopfleiste angezeigt.

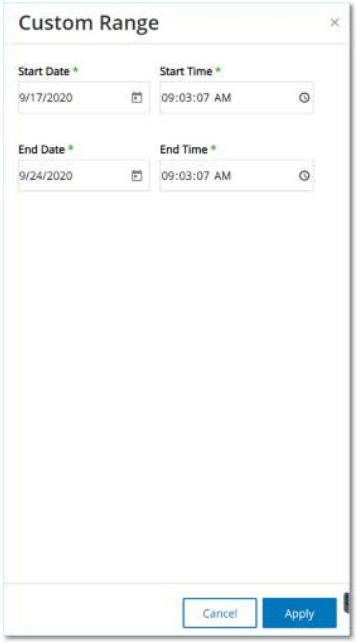
So legen Sie den Zeitraum fest:

1. Klicken Sie in der Kopfleiste auf die **Zeitraumauswahl** (Standardeinstellung: „Letzte 15 Minuten“).
   Ein Dropdown-Menü mit Zeitraumoptionen wird angezeigt.



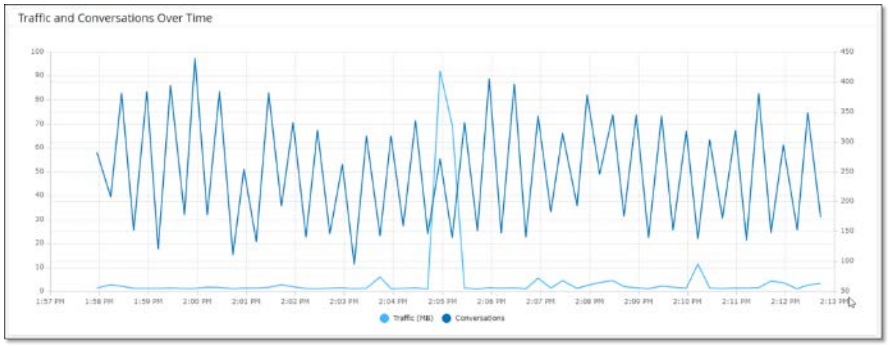
2. Wählen Sie mit einer der folgenden Methoden einen Zeitraum aus.
   - Wählen Sie einen voreingestellten Zeitraum aus, indem Sie auf den gewünschten Zeitraum klicken (verfügbare Optionen: „Letzte 15 Minuten“, „Letzte Stunde“, „Letzte 4 Stunden“, „Letzte 12 Stunden“, „Letzter Tag“, „Letzte 7 Tage“ oder „Letzte 30 Tage“). ODER
   - Legen Sie mithilfe des folgenden Verfahrens einen benutzerdefinierten Zeitraum fest:

     a. Klicken Sie auf **Benutzerdefinierter Bereich**.
     Das Fenster **Benutzerdefinierter Bereich** wird angezeigt.



     b. Geben Sie das **Startdatum** und die **Startzeit** sowie das **Enddatum** und die **Endzeit** in die entsprechenden Felder ein.
     c. Klicken Sie auf **Anwenden**.
     Damit ist der Zeitraum festgelegt. Startdatum und -zeit sowie Enddatum und -zeit werden in der Kopfleiste neben der Zeitraumauswahl angezeigt. Der Bildschirm wird aktualisiert, um nur Daten für den ausgewählten Zeitraum anzuzeigen.

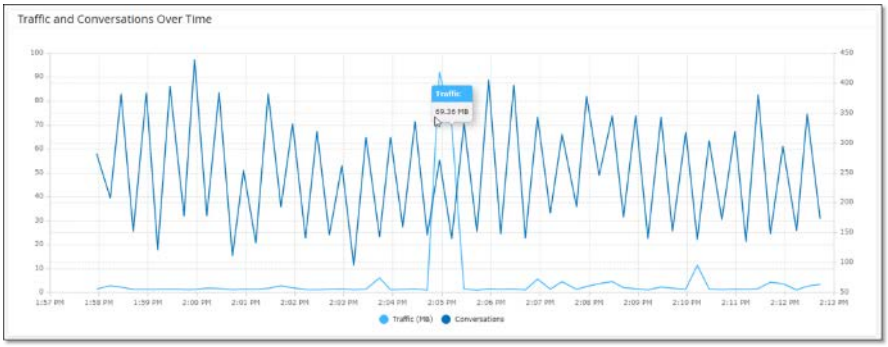
Traffic und Konversationen im zeitlichen Verlauf



Ein Liniendiagramm zeigt das Traffic-Volumen (gemessen in KB/MB/GB) und die Anzahl der Konversationen an, die im Laufe der Zeit im Netzwerk stattgefunden haben. Der Anzeigeschlüssel wird oben im Diagramm angezeigt.

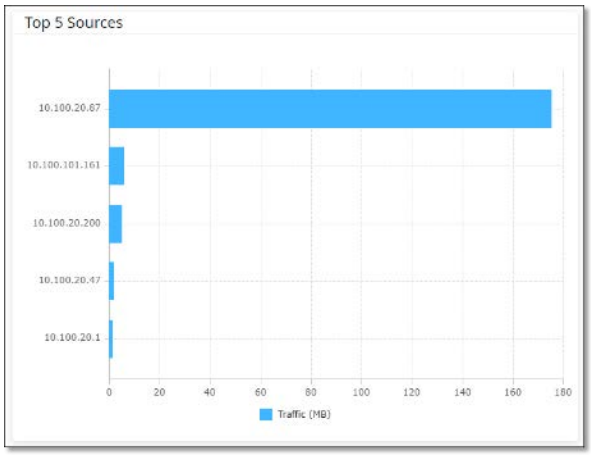
So zeigen Sie Daten für einen bestimmten Zeitabschnitt an:

1. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um ein Popout-Fenster mit spezifischen Daten über den Traffic und die Konversationen anzuzeigen, die in diesem Zeitsegment stattgefunden haben.



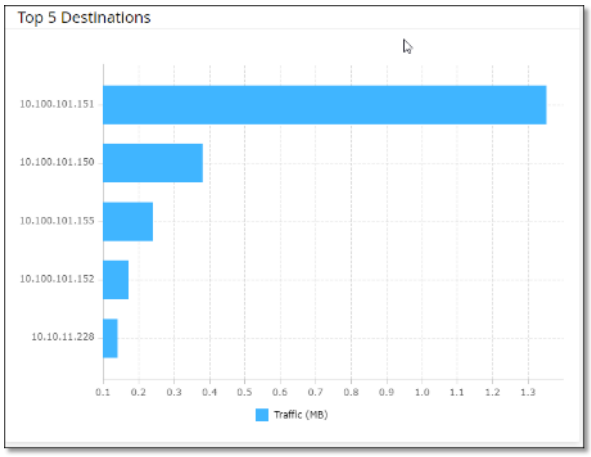
Die Länge des angezeigten Zeitabschnitts wird entsprechend der angezeigten Zeitskala angepasst (z. B. werden für einen 15-Minuten-Zeitraum die Daten für jede Minute separat angezeigt, für einen 30-Tage-Zeitraum hingegen für 6-Stunden-Abschnitte).

Top 5 Quellen



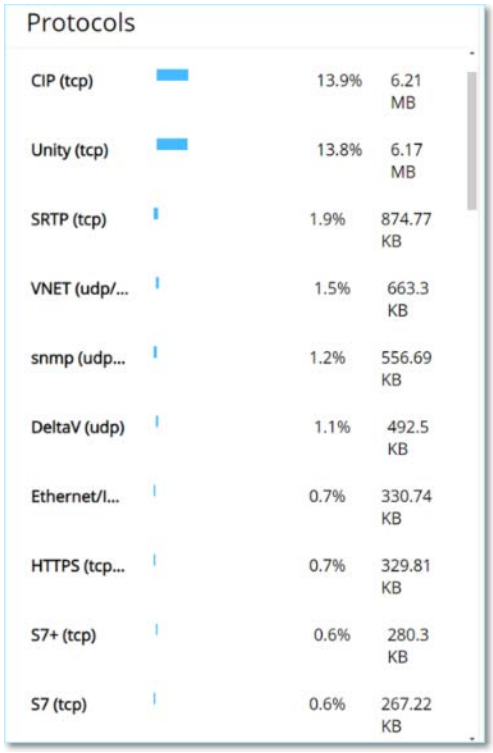
Der Fensterbereich **Top 5 Quellen** zeigt die Anzahl der Konversationen und das Traffic-Volumen für jedes der Top 5 Assets an, die während des angegebenen Zeitraums Mitteilungen über das Netzwerk gesendet haben. Die Quell-Assets werden anhand ihrer IP-Adressen identifiziert. Wenn Sie den Mauszeiger über ein Balkendiagramm bewegen, werden die Anzahl der Konversationen und das von diesem Asset gesendete Traffic-Volumen angezeigt.

Top 5 Ziele



Der Fensterbereich **Top 5 Ziele** zeigt die Anzahl der Konversationen und das Traffic-Volumen für jedes der Top 5 Assets an, die während des angegebenen Zeitraums Mitteilungen über das Netzwerk empfangen haben. Die Ziel-Assets werden anhand ihrer IP-Adressen identifiziert. Wenn Sie den Mauszeiger über ein Balkendiagramm bewegen, werden die Anzahl der Konversationen und das von diesem Asset empfangene Traffic-Volumen angezeigt.

Protokolle



Der Fensterbereich **Protokolle** enthält Daten über die Verwendung verschiedener Protokolle für die Kommunikation innerhalb des Netzwerks während des angegebenen Zeitrahmens. Die Protokolle sind von den am häufigsten verwendeten (oben) bis zu den am seltensten verwendeten (unten) aufgelistet. Für jedes Protokoll werden die folgenden Informationen angezeigt:

- Ein Balkendiagramm, das die Nutzungsrate anzeigt (wobei ein vollständiger Balken die höchste Nutzung anzeigt und Teilbalken das Ausmaß der Nutzung im Vergleich zum am häufigsten genutzten Protokoll angeben)
- Der Prozentsatz der Nutzung
- Gesamtvolumen der Kommunikation

Paketerfassungen

Das System speichert Dateien mit vollständigen Netzwerk-Paketerfassungen von Aktivitäten im Netzwerk. Die Daten werden als PCAP-Dateien gespeichert, die mit Tools zur Analyse von Netzwerkprotokollen (z. B. Wireshark usw.) analysiert werden können. Dies ermöglicht eine umfassende forensische Analyse kritischer Ereignisse. Wenn die Speicherkapazität des Systems (1,8 TB) überschritten wird, löscht das System ältere Dateien.

Der Bildschirm **Paketerfassungen** zeigt alle Paketerfassungsdateien im System an. Die Registerkarte *Abgeschlossen* enthält Listen für jede abgeschlossene Datei, die zum Herunterladen verfügbar ist. Die Registerkarte *Laufend* enthält Details zu der Paketerfassung, die derzeit im System ausgeführt wird.

Die *Kopfleiste* zeigt die älteste noch im System verfügbare erfasste Datei. Außerdem enthält sie eine Schaltfläche zum Herunterladen von Dateien sowie zum manuellen Schließen der aktuellen Paketerfassung.

In der Tabelle mit Dateilisten können Sie Spalten ein- und ausblenden und die Listen sortieren und filtern sowie nach Schlüsselwörtern suchen. Eine Erläuterung der Anpassungsfunktionen finden Sie unter **Arbeiten mit Listen**.

Sie können die PCAP-Datei für ein einzelnes Ereignis auch über den Bildschirm **Ereignisse** herunterladen, siehe **Herunterladen von Dateien**.

Paketerfassungsparameter

Die folgende Tabelle beschreibt die Parameter, die für die Paketerfassungslisten angezeigt werden.

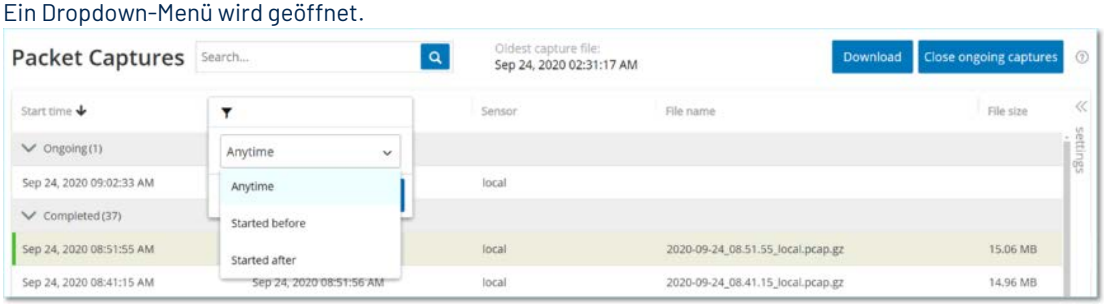
Parameter	Beschreibung
Startzeit	Das Datum und die Uhrzeit des Beginns der Paketerfassung.
Endzeit	Das Datum und die Uhrzeit des Endes der Paketerfassung.
Status	Der Status der Erfassung. Mögliche Werte: *Abgeschlossen* oder *Laufend*.
Sensor	Der Tenable.ot Sensor, der das Paket erfasst hat. Für Pakete, die direkt von der Tenable.ot Appliance erfasst werden, wird der Wert *lokal*angegeben.
Dateiname	Der Name der Datei.
Dateigröße	Die Größe der Datei, angegeben in KB/MB.

Filtern der Paketerfassungsanzeige

Die Anzeige der **Paketerfassungen** kann gefiltert werden, um eine bestimmte PCAP durch Eingabe der Parameter für Start- und/oder Endzeit zu suchen.

So filtern Sie Paketerfassungen:

1. Wählen Sie unter **Netzwerk** die Option **Paketerfassungen** aus.
2. Um nach der Startzeit zu filtern, bewegen Sie den Mauszeiger über **Startzeit** und klicken Sie auf das angezeigte Menüsymbol.
   Ein Dropdown-Menü wird geöffnet.

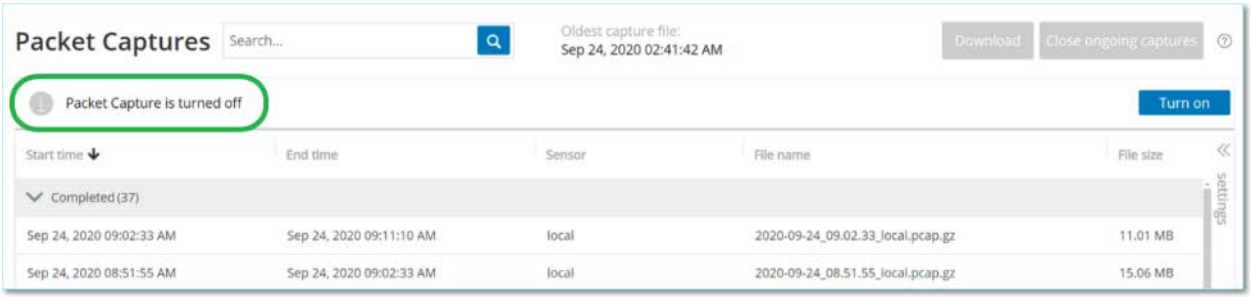


   Legen Sie den Filter wie folgt fest:
   a. Wählen Sie die gewünschte Filteroption in der Dropdown-Liste aus. Verfügbare Optionen: *Jederzeit* (Standardeinstellung), *Begonnen vor* oder *Begonnen nach*.
   b. Wenn **Begonnen vor** oder **Begonnen nach** ausgewählt wurde, öffnet sich ein Fenster mit den Feldern **Datum** und **Uhrzeit**, in denen Sie das gewünschte Datum und die gewünschte Uhrzeit auswählen können.
   c. Klicken Sie auf **Anwenden**.
3. Um nach der Endzeit zu filtern, klicken Sie auf das **Filter**-Symbol neben **Endzeit**.
   Ein Dropdown-Menü wird geöffnet. Legen Sie den Filter wie folgt fest:
   a. Wählen Sie die gewünschte Filteroption in der Dropdown-Liste aus. Verfügbare Optionen: *Jederzeit* (Standardeinstellung), *Begonnen vor* oder *Begonnen nach*.
   b. Wenn **Begonnen vor** oder **Begonnen nach** ausgewählt wurde, öffnet sich ein Fenster mit den Feldern **Datum** und **Uhrzeit**, in denen Sie das gewünschte Datum und die gewünschte Uhrzeit auswählen können.
   c. Klicken Sie auf **Anwenden**.
   Der Filter wird angewendet und nur die innerhalb des ausgewählten Zeitraums generierten Dateien werden angezeigt.

Aktivieren/Deaktivieren der Paketerfassung

Die Paketerfassung kann im Bildschirm **Lokale Einstellungen** > **Gerätedetails** aktiviert/deaktiviert werden, siehe **PAKETERFASSUNGEN**.

Wenn die Funktion **Paketerfassung** deaktiviert ist, wird im Bildschirm **Paketerfassungen** eine entsprechende Informationsmeldung angezeigt.

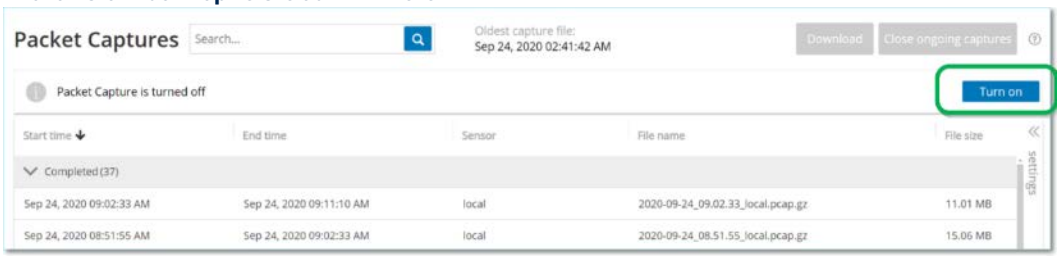


Sie können die Paketerfassung über den Bildschirm **Netzwerk** > **Paketerfassungen** aktivieren (aber nicht deaktivieren).

So aktivieren Sie die Paketerfassung über den Bildschirm „Paketerfassungen“:

1. Wählen Sie unter **Netzwerk** die Option **Paketerfassungen** aus.

2. Klicken Sie in der **Kopfleiste** auf **Aktivieren**.



Das System startet die Paketerfassung.

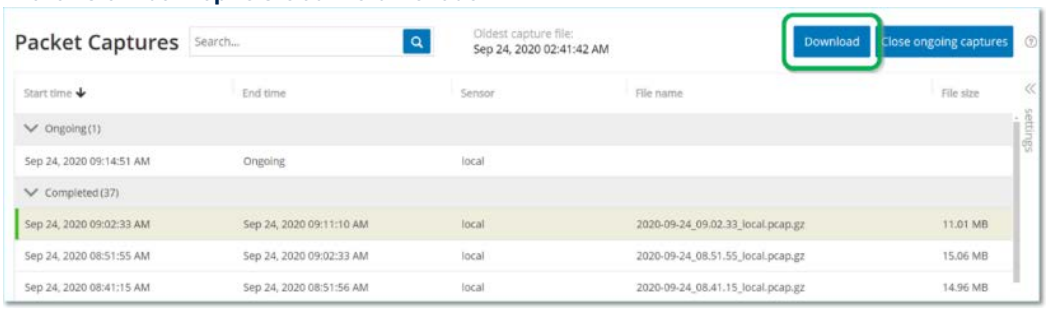
Herunterladen von Dateien

Sie können alle *abgeschlossenen* PCAP-Dateien auf Ihren lokalen Computer herunterladen. Die PCAP-Dateien können dann mit Tools zur Analyse von Netzwerkprotokollen (z. B. Wireshark usw.) analysiert werden.

Noch laufende Dateierfassungen stehen noch nicht zum Herunterladen zur Verfügung. Sie können eine laufende Erfassung manuell schließen, um die aktuelle Datei zu schließen und mit der Erfassung von Informationen für eine neue Datei zu beginnen.

So laden Sie eine abgeschlossene Datei herunter:

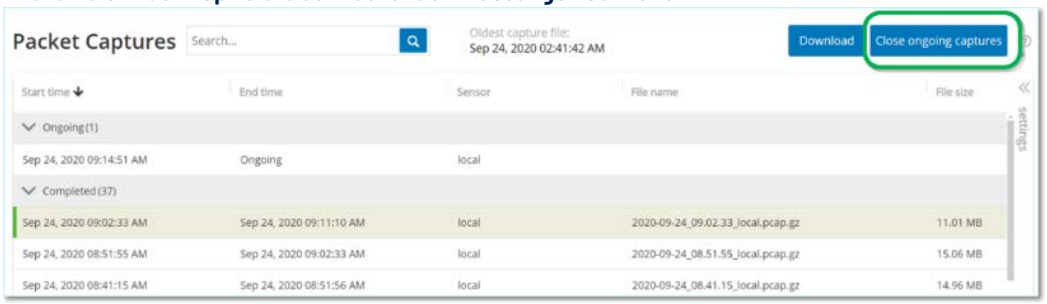
1. Wählen Sie unter **Netzwerk** die Option **Paketerfassungen** aus.
2. Wählen Sie die gewünschte Datei in den Paketerfassungslisten aus.
3. Klicken Sie in der **Kopfleiste** auf **Herunterladen**.



Die gezippte PCAP-Datei wird auf Ihren lokalen Computer heruntergeladen.

So schließen Sie die aktuelle Paketerfassung manuell:

1. Wählen Sie unter **Netzwerk** die Option **Paketerfassungen** aus.
2. Klicken Sie in der **Kopfleiste** auf **Laufende Erfassungen schließen**.



Die aktuelle Erfassung wird gestoppt und die Datei steht zum Herunterladen zur Verfügung. Es wird automatisch eine neue Paketerfassung gestartet.

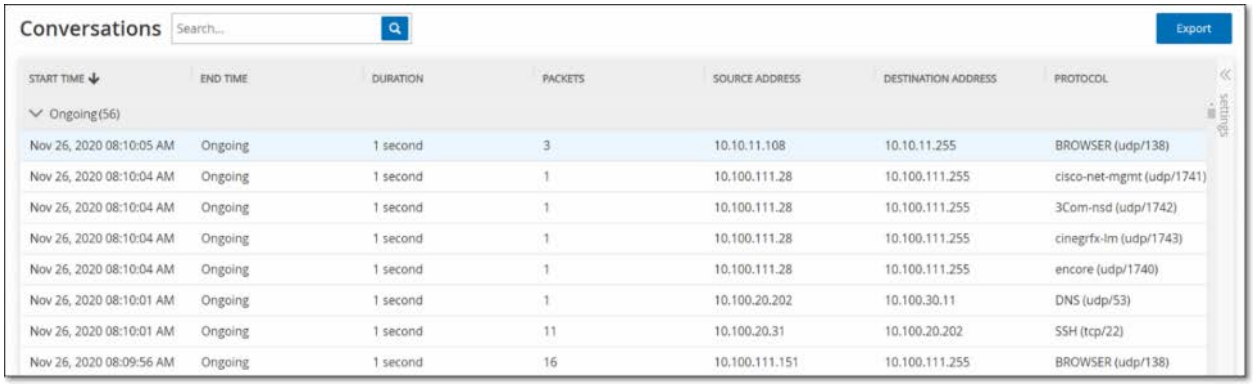
Konversationen

Konversationen sind Netzwerkkommunikationen zwischen zwei Assets – einer Quelle und einem Ziel. Beispielsweise eine Interaktion zwischen einer Engineering-Workstation und einer SPS oder zwischen zwei Servern. Der Bildschirm **Konversationen** enthält eine Liste der aktuellen und vergangenen Konversationen, einschließlich detaillierter Informationen zu den Konversationen.

Der Bildschirm „Konversationen" bietet die folgenden zusätzlichen Funktionalitäten:

- **Suchen** – Suchen Sie nach bestimmten Konversationen, indem Sie Informationen zur Identifizierung in das Feld **Suchen** eingeben.
- **Exportieren** – Exportieren Sie alle Daten aus der Registerkarte „Konversationen" als CSV-Datei auf Ihren lokalen Computer, indem Sie auf **Exportieren** klicken.

Die Konversationstabelle enthält die letzten 10.000 Netzwerkkonversationen.

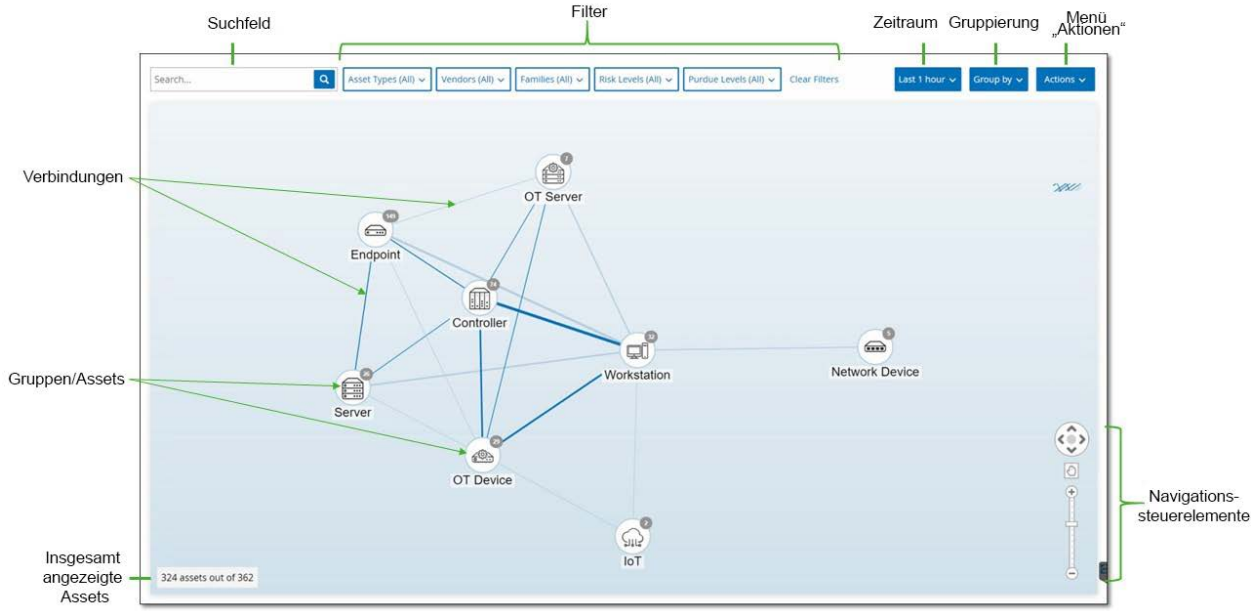


Die auf der Registerkarte „Konversationen" angezeigten Informationen werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Startzeit	Die Uhrzeit, zu der die Konversation begonnen hat.
Endzeit	Die Uhrzeit, zu der die Konversation geendet hat. Zeigt *Laufend* für Konversationen an, die noch laufen.
Dauer	Die Dauer der Konversation.
Pakete	Die Anzahl der gesendeten Datenpakete.
Quelladresse	Die IP des Assets, das die Daten gesendet hat.
Zieladresse	Die IP des Assets, das die Daten empfangen hat.
Protokoll	Das Protokoll, das für die Kommunikation verwendet wurde.

NETZWERKÜBERSICHT

Der Bildschirm **Netzwerkübersicht** bietet eine visuelle Darstellung der Netzwerk-Assets und ihrer Verbindungen im zeitlichen Verlauf, wie sie von den Netzwerkerkennungsfunktionen von Tenable.ot erfasst wurden. Die Netzwerkerkennung bietet einen detaillierten Echtzeit-Einblick in alle Aktivitäten, die über das Betriebsnetzwerk ausgeführt werden, mit besonderem Schwerpunkt auf den technischen Aktivitäten auf der Steuerungsebene. Dies sind beispielsweise Firmware-Downloads/-Uploads, Code-Updates und Konfigurationsänderungen, die über proprietäre, anbieterspezifische Protokolle durchgeführt werden. Die Assets können nach Gruppen von zusammenhängenden Assets oder als einzelne Assets angezeigt werden.



Die Netzwerkübersicht zeigt alle Assets und Verbindungen an, die während des angegebenen Zeitraums erfasst wurden.

Im Folgenden finden Sie eine Erläuterung der Elemente im Bildschirm „Netzwerkübersicht“.

- **Suchfeld** – Geben Sie Suchtext ein, um in der Anzeige nach Assets zu suchen. Die Suchergebnisse werden durch Hervorheben aller Gruppen angezeigt, in denen eine Übereinstimmung mit dem Suchtext gefunden wurde. Sie können jede Gruppe aufschlüsseln, um die relevanten Assets anzuzeigen.
- **Filter** – Sie können die Übersicht nach einer oder mehreren der angegebenen Kategorien filtern: *Asset-Typ*, *Anbieter*, *Familien*, *Risikostufen*, *Purdue-Level*. Eine Erläuterung der Asset-Typen finden Sie unter **Asset-Typen**.
- **Zeitraum** – Die Netzwerkübersicht zeigt Assets und Verbindungen an, die während des angegebenen Zeitraums erkannt wurden. Der Standardzeitraum ist auf *Letzter Monat* festlegt. Klicken Sie auf die **Zeitraumauswahl**, um einen anderen Zeitraum im Dropdown-Menü auszuwählen.
- **Gruppierung** – Sie können die Kategorie angeben, nach der die Assets in der Anzeige gruppiert werden. Verfügbare Optionen: *Asset-Typ*, *Purdue-Level*, *Risikostufe* oder *Keine Gruppierung*. Die Option *Alle Gruppen reduzieren* behält die aktuelle Gruppierungsauswahl bei, reduziert jedoch alle geöffneten Gruppen.

- **Aktionen** – Sie können die folgenden Aktionen im Dropdown-Menü auswählen:
    - **Als Baseline festlegen** – Hiermit können Sie die Baseline festlegen, die zum Erkennen anomaler Netzwerkaktivitäten verwendet wird, siehe **Festlegen einer Netzwerk-Baseline**.
    - **Automatisch anordnen** – Optimiert die Übersicht automatisch für die aktuell angezeigten Entitäten.
- **Gruppen/Assets** – Jede Gruppe von Assets wird durch ein Symbol in der Übersicht dargestellt, wobei jeder Asset-Typ durch ein anderes Symbol dargestellt wird (wie unter **Asset-Typen** beschrieben). Bei Gruppen gibt die Zahl oben im Symbol die Anzahl der Assets an, die in dieser Gruppe enthalten sind. Sie können die Anzeige aufschlüsseln, um separate Symbole für jede Untergruppe anzuzeigen, bis Sie zu den Symbolen für einzelne Assets gelangen. Bei einzelnen Assets zeigt die Farbe des Rahmens um das Asset dessen Risikostufe an (rot, gelb, grün).

Sie können die Gruppen und Assets ziehen und neu positionieren, um einen besseren Überblick über die Assets und ihre Verbindungen zu erhalten.

- **Verbindungen** – Jede Kommunikation zwischen Asset-Gruppen und/oder einzelnen Assets, entsprechend dem Granularitätsgrad, der gerade in der Übersicht angezeigt wird. Die Dicke der Linie zeigt das Kommunikationsvolumen über diese Verbindung an.
- **Gesamtzahl der angezeigten Assets** – Zeigt die Anzahl der im Netzwerk erkannten (und in der Übersicht angezeigten) Assets basierend auf dem angegebenen Zeitraum und den Asset-Filtern. Diese Zahl wird relativ zur Gesamtzahl der in Ihrem Netzwerk erkannten Assets angezeigt.
- **Navigationssteuerelemente** – Sie können die Anzeige vergrößern und verkleinern und darin navigieren, um die gewünschten Elemente anzuzeigen. Hierzu können Sie die Steuerelemente auf dem Bildschirm oder die Standard-Maussteuerungen verwenden.

Asset-Gruppierungen

Die Netzwerkübersicht kann Assets nach verschiedenen Kategorien gruppiert anzeigen. Verbindungen werden zwischen Gruppen von Assets angezeigt. Sie können auf ein Asset klicken, um die Gruppe aufzuschlüsseln und die darin enthaltenen Elemente anzuzeigen. Mehrere Gruppen können gleichzeitig aufgeschlüsselt werden. Tenable.ot enthält mehrere Ebenen eingebetteter Gruppen, sodass Sie bei jeder Aufschlüsselung eine detailliertere Ansicht der einbezogenen Assets erhalten.

Im Folgenden sind die Gruppierungen aufgeführt, die auf die Hauptanzeige angewendet werden können, sowie die Aufschlüsselungsoptionen für diese Auswahl.

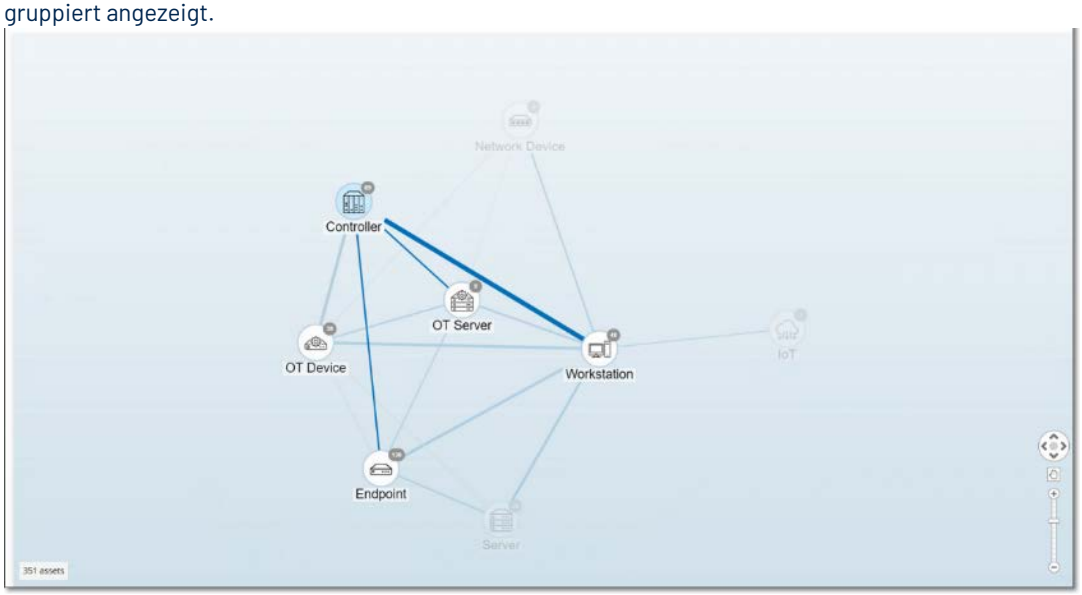
Wenn die Übersicht nach *Asset-Typ* (Standardeinstellung) gruppiert ist, sieht die Aufschlüsselungshierarchie wie folgt aus: **Asset-Typ** > **Anbieter** > **Familie** > **Einzelnes Asset**.

Wenn die Übersicht nach *Risikostufe* oder *Purdue-Level* gruppiert ist, wird eine zusätzliche Ebene *über* der Asset-Typ-Gruppierung hinzugefügt, sodass die Hierarchie wie folgt lautet: **Purdue-Level/Risikostufe** > **Asset-Typ** > **Anbieter** > **Familie** > **Einzelnes Asset**. Jede Ebene wird durch einen Kreis dargestellt, der die enthaltenen Gruppen/Assets umgibt.

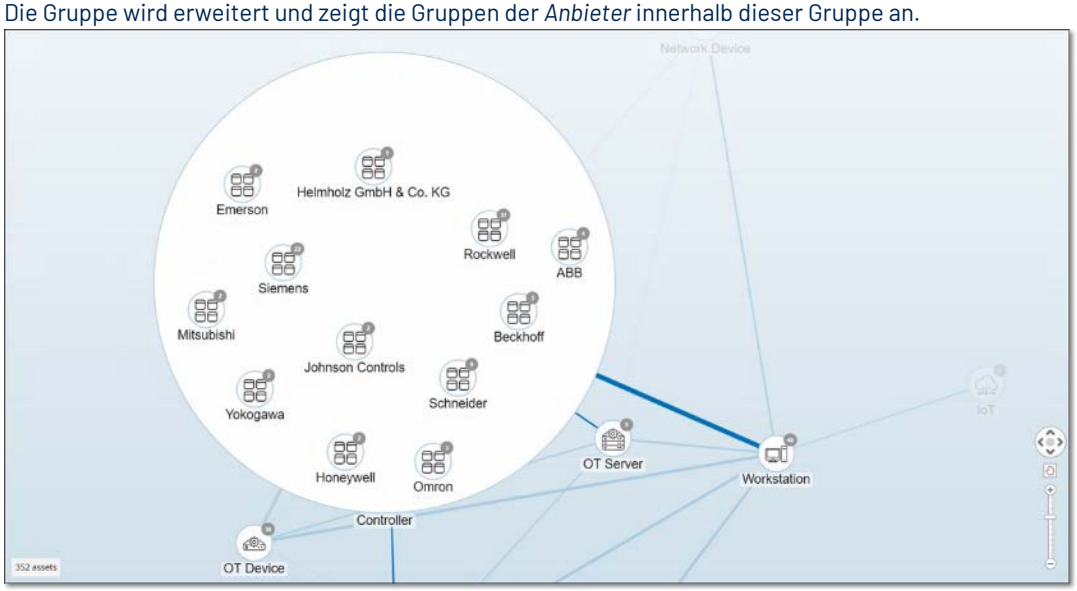
Das folgende Beispiel zeigt, wie Sie die Anzeige aufschlüsseln können:

So schlüsseln Sie eine Asset-Typ-Gruppe auf:

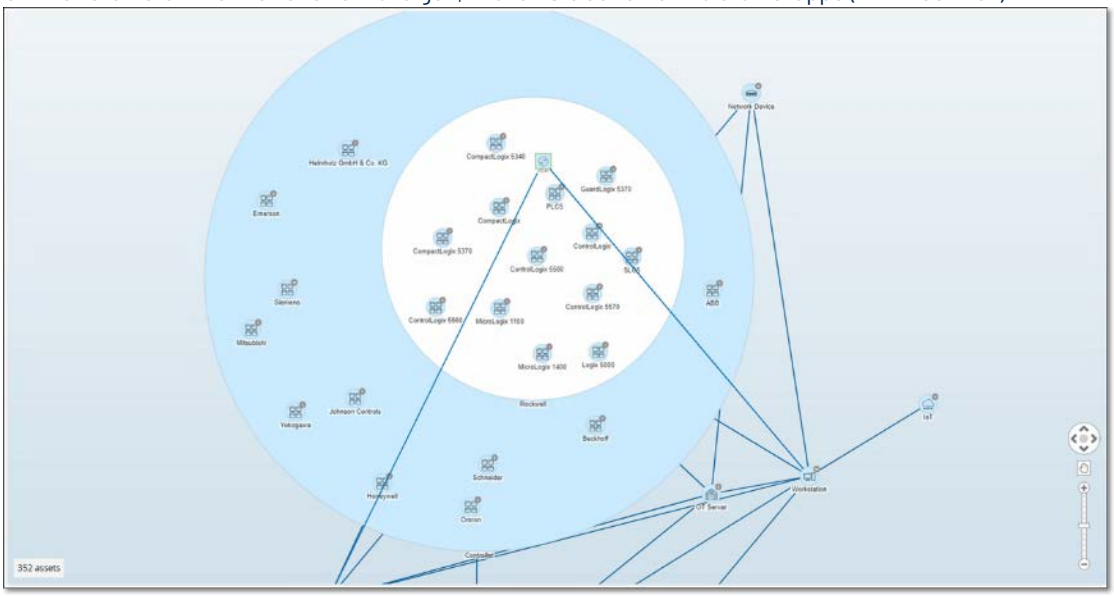
1. Wenn Sie den Bildschirm **Netzwerkübersicht** öffnen, werden die Assets standardmäßig nach *Asset-Typ* gruppiert angezeigt.



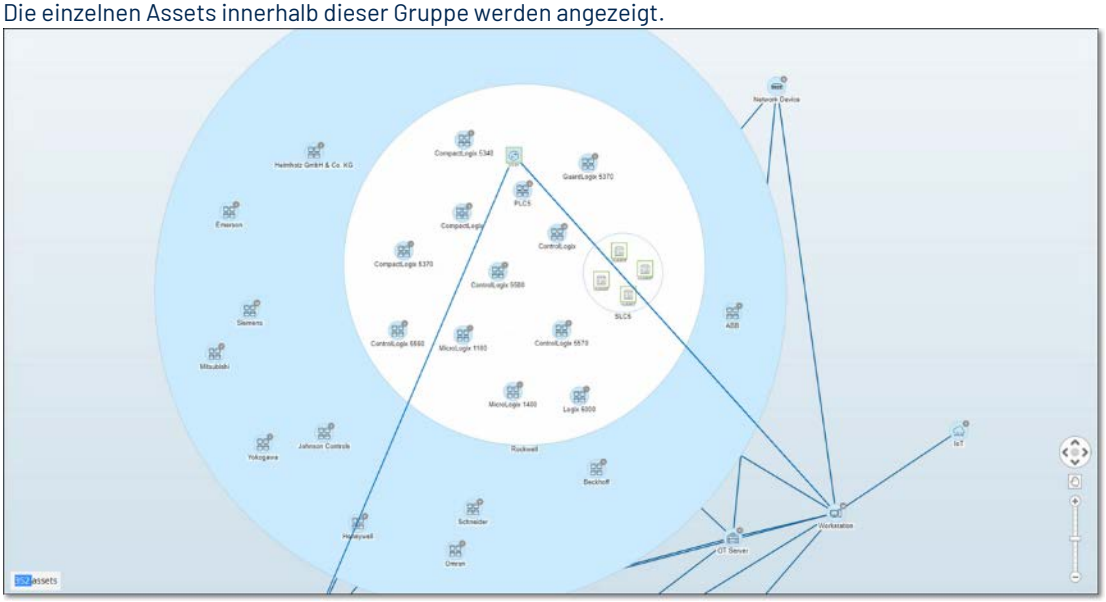
2. Doppelklicken Sie auf das Symbol der Gruppe, die Sie aufschlüsseln möchten (z. B. **Controller**).
Die Gruppe wird erweitert und zeigt die Gruppen der *Anbieter* innerhalb dieser Gruppe an.



3. Um weitere Detailinformationen anzuzeigen, klicken Sie auf eine *Anbieter*-Gruppe (z. B. Rockwell).



4. Klicken Sie zur weiteren Aufschlüsselung auf eine Familiengruppe (z. B. SLC5).
5. Die einzelnen Assets innerhalb dieser Gruppe werden angezeigt.



6. Sie können jetzt auf ein bestimmtes Asset klicken, um Details für dieses Asset und seine Verbindungen anzuzeigen, siehe **Anzeigen von Asset-Details**.

So reduzieren Sie die Anzeige:

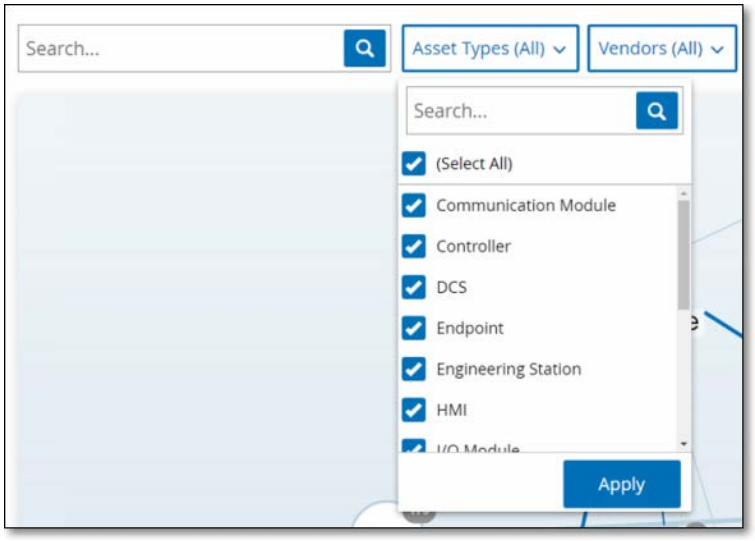
1. Klicken Sie auf **Gruppieren nach**.
2. Klicken Sie auf **Alle Gruppen reduzieren**.
   Es werden wieder die Gruppen der obersten Ebene angezeigt.

So entfernen Sie jegliche Gruppierung:

1. Klicken Sie auf die Schaltfläche **Gruppieren nach**.
2. Wählen Sie **Keine Gruppierung** aus.
   In der Übersicht werden alle einzelnen Assets angezeigt, ohne dass eine Gruppierung vorgenommen wurde.

Anwenden von Filtern auf die Übersicht

Sie können die Übersicht nach einer oder mehreren der angegebenen Kategorien filtern: Asset-Typ, Anbieter, Familien, Risikostufen, Purdue-Level.



So wenden Sie Filter auf die Übersicht an:

1. Klicken Sie auf die gewünschte Filterkategorie.
2. Aktivieren/deaktivieren Sie die Kontrollkästchen für jedes Element, das Sie in die Anzeige einschließen bzw. aus der Anzeige ausschließen möchten.

> Standardmäßig sind alle Elemente im Filter enthalten.

3. Sie können auf das Kontrollkästchen **Alle auswählen** klicken, um die Auswahl aller Werte aufzuheben, und dann die gewünschten Werte hinzufügen.
4. Sie können im Filtersuchfeld eine Suche durchführen, um einen bestimmten Wert im Filterfenster zu finden.
5. Wiederholen Sie den Vorgang nach Bedarf für jede Filterkategorie.
6. Klicken Sie auf **Anwenden**.
   Nur die ausgewählten Elemente werden in der Übersicht angezeigt.

Anzeigen von Asset-Details

Klicken Sie auf ein bestimmtes Asset, um grundlegende Informationen über das Asset und seine Netzwerkaktivitäten anzuzeigen, einschließlich Risikostufe, IP-Adresse, Asset-Typ, Anbieter und Familie. Die Übersicht zeigt Verbindungen vom ausgewählten Asset zu allen anderen Assets, die mit diesem kommunizieren. Sie können dann auf den Link im Asset-Namen klicken, um zum Bildschirm **Asset-Details** mit detaillierteren Informationen über das Asset zu gelangen.

Festlegen einer Netzwerk-Baseline

Eine Netzwerk-Baseline ist eine Übersicht aller Konversationen, die während eines bestimmten Zeitraums zwischen Assets im Netzwerk stattgefunden haben. Die Netzwerk-Baseline wird in Richtlinien vom Typ *Netzwerk-Baseline-Abweichung* verwendet, die vor anomalen Konversationen im Netzwerk warnen, siehe **Netzwerkereignistypen.**

Jede Konversation zwischen Assets, die während der Baseline-Stichprobe nicht interagiert haben, löst eine Richtlinienwarnung aus (in der Annahme, dass sie im Geltungsbereich der angegebenen Richtlinienbedingungen liegt). Eine anfängliche Netzwerk-Baseline muss im Bildschirm „Netzwerkübersicht" erstellt werden, damit Richtlinien vom Typ „Netzwerk-Baseline-Abweichung" erstellt werden können. Die Netzwerk-Baseline kann jederzeit durch Festlegen einer neuen Netzwerk-Baseline aktualisiert werden. Sie sollten jedes Mal eine neue Netzwerk-Baseline festlegen, wenn Ihrem Netzwerk neue Assets oder Verbindungen hinzugefügt werden.

➡ So legen Sie eine Netzwerk-Baseline fest:

1. Wählen Sie im Bildschirm **Netzwerkübersicht** mithilfe der **Zeitraumauswahl** oben im Bildschirm den Zeitraum der Konversationen aus, die Sie in die Netzwerk-Baseline aufnehmen möchten.
   Die **Netzwerkübersicht** für den ausgewählten Zeitraum wird angezeigt.
2. Klicken Sie oben im Bildschirm auf **Aktionen** > **Als Baseline festlegen**.
   Die neue Netzwerk-Baseline wird im System konfiguriert und auf alle Richtlinien vom Typ „Netzwerk-Baseline-Abweichung" angewendet.

SCHWACHSTELLEN

Tenable.ot identifiziert verschiedene Arten von Bedrohungen, von denen Assets in Ihrem Netzwerk betroffen sind. Sobald Informationen über neue Schwachstellen aufgedeckt und öffentlich zugänglich gemacht werden, entwickeln Forschungsmitarbeiter von Tenable, Inc. Programme, mit denen Nessus diese Schwachstellen erkennen kann.

Diese Programme heißen *Plugins* und werden in der proprietären Nessus-Skriptsprache namens *Nessus Attack Scripting Language* (NASL) geschrieben. Plugins erkennen CVEs sowie andere Bedrohungen, die Assets in Ihrem Netzwerk betreffen können (z. B. veraltete Betriebssysteme, Verwendung anfälliger Protokolle, anfällige offene Ports usw.).

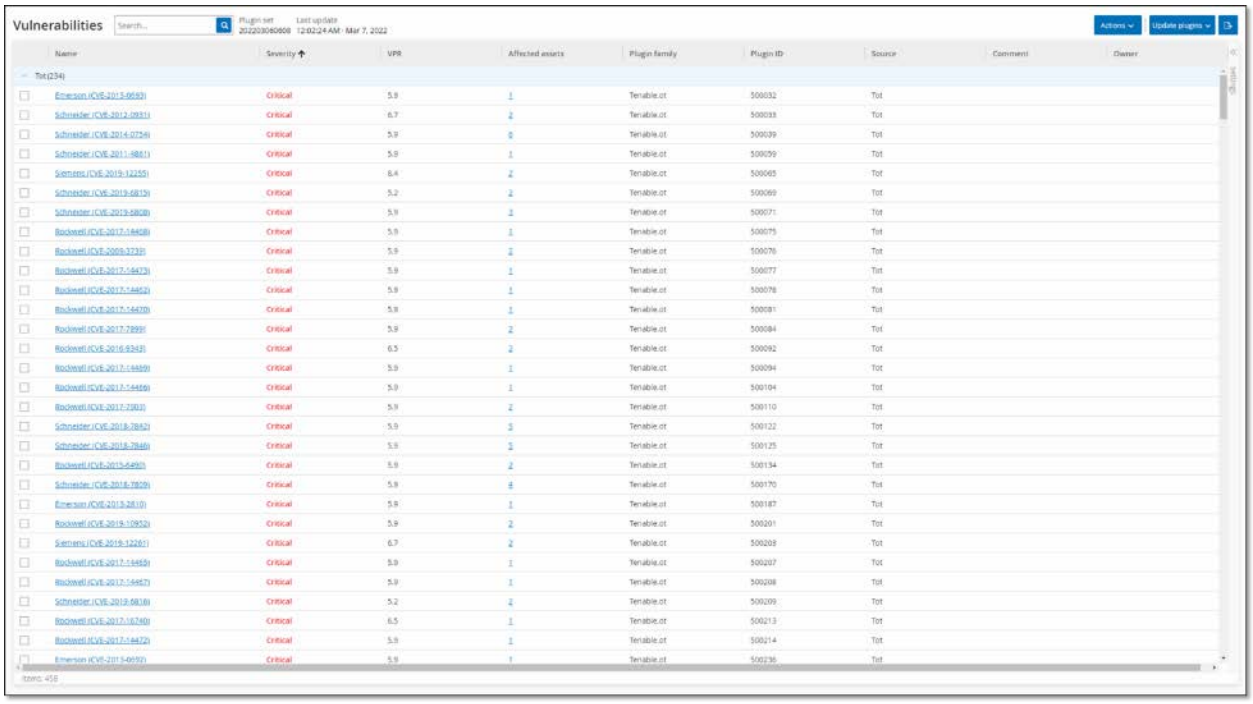
Plugins enthalten Schwachstelleninformationen, einen generischen Satz von Behebungsmaßnahmen sowie den Algorithmus, mit dem auf das Vorhandensein des Sicherheitsproblems getestet wird.

Informationen zum Aktualisieren Ihres Plugin-Satzes finden Sie unter **Updates**.

Bildschirm „Schwachstellen“

Der Bildschirm **Schwachstellen** enthält eine Liste aller von den Tenable-Plugins erkannten Schwachstellen, die ihr Netzwerk und ihre Assets betreffen.

Sie können die Anzeigeeinstellungen anpassen, indem Sie festlegen, welche Spalten angezeigt werden und wo die einzelnen Spalten positioniert sind. Eine Erläuterung der Anpassungsfunktionen finden Sie unter **Arbeiten mit Listen**.



Die Informationen auf der Registerkarte **Schwachstellen** werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Name	Der Name der Schwachstelle. Der Name ist ein Link zur Anzeige der vollständigen Schwachstellenauflistung.
Schweregrad	Dieser Wert gibt den Schweregrad der von diesem Plugin erkannten Bedrohung an. Mögliche Werte: *Info*, *Gering*, *Mittel* oder *Hoch*.

Parameter	Beschreibung
VPR	Vulnerability Priority Rating (VPR) ist ein dynamischer Indikator des Schweregrads, der basierend auf der aktuellen Ausnutzbarkeit der Schwachstelle ständig aktualisiert wird. Dieser Wert wird von Tenable als Ergebnis von Predictive Prioritization generiert, eine Tenable-Funktion, die die technischen Auswirkungen und die Bedrohung durch die Schwachstelle bewertet. VPR-Werte reichen von 0,1 bis 10,0, wobei ein höherer Wert eine höhere Wahrscheinlichkeit einer Ausnutzung darstellt.
Plugin-ID	Der eindeutige Bezeichner des Plugins.
Betroffene Assets	Die Anzahl der Assets in Ihrem Netzwerk, die von dieser Schwachstelle betroffen sind.
Plugin-Familie	Die Familie (Gruppe), der dieses Plugin zugeordnet ist.
Kommentar	Sie können Freitextkommentare zu diesem Plugin hinzufügen.

Plugin-Details

Klicken Sie auf einen Plugin-Namen, um detaillierte Informationen über dieses Plugin anzuzeigen.

Dieser Bildschirm enthält drei Elemente:

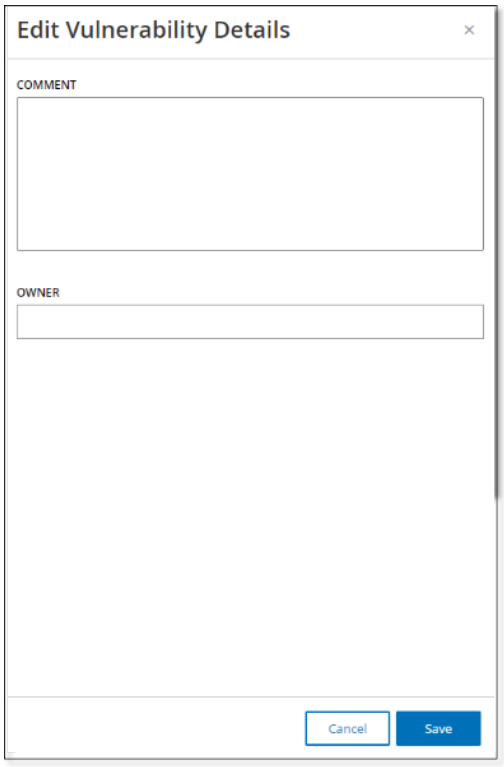
- **Kopfleiste** – Zeigt grundlegende Informationen über die angegebene Schwachstelle und enthält die Schaltfläche **Aktionen**, über die Sie Schwachstellendetails bearbeiten können. Siehe **Bearbeiten von Schwachstellendetails**.
- **Registerkarte „Details“** – Zeigt die vollständige Beschreibung der Schwachstelle und enthält Links zu relevanten Ressourcen.
- **Registerkarte „Betroffene Assets“** – Zeigt eine Liste aller Assets an, die von der angegebenen Schwachstelle betroffen sind. Jede Liste enthält detaillierte Informationen über das Asset sowie einen Link zum Aufrufen des Fensters „Asset-Details“ für das betreffende Asset.

Bearbeiten von Schwachstellendetails

➡ **So bearbeiten Sie Schwachstellendetails:**

1. Klicken Sie auf der relevanten Seite **Details zum Sicherheitsrisiko** auf die Schaltfläche **Aktionen** in der oberen rechten Ecke.
   Das Menü „Aktionen“ wird angezeigt.

2. Klicken Sie im Menü **Aktionen** auf **Details bearbeiten**.
   Der Seitenbereich **Schwachstellendetails bearbeiten** wird angezeigt.



3. Geben Sie im Feld **Kommentare** Kommentare zur Schwachstelle ein.
4. Geben Sie im Feld **Besitzer** den Namen der Person ein, die mit der Behebung der Schwachstelle beauftragt ist.
5. Klicken Sie auf **Speichern**.

LOKALE EINSTELLUNGEN

Die verschiedenen Einstellungsbildschirme werden unter **Lokale Einstellungen** in der Hauptnavigation aufgelistet.

Im Folgenden finden Sie eine kurze Beschreibung der auf den einzelnen Registerkarten angezeigten Informationen und verfügbaren Aktionen.

- **Abfragen** – Abfragefunktionen aktivieren/deaktivieren und ihre Frequenz und Einstellungen anpassen. Abfragen sind in separate Bildschirme für *Asset-Erfassung*, *Controller* und *Netzwerk* unterteilt. Siehe
- Abfragen.
- **Systemkonfiguration**
    - **Gerät** – Gerätedetails und Netzwerkinformationen anzeigen und bearbeiten (z. B. Systemzeit, DNS-Server, automatisches Ausloggen (d. h. Zeitüberschreitung bei Inaktivität)).
    - **Sensoren** – Sensoren anzeigen und verwalten, eingehende Sensor-Kopplungsanforderungen genehmigen oder löschen und aktive Abfragen konfigurieren, die von Sensoren durchgeführt werden. Siehe **Sensoren**.
    - **Portkonfiguration** – Konfiguration der Ports des Geräts anzeigen. Weitere Informationen zur Portkonfiguration finden Sie unter **Installieren der Tenable.ot Appliance** > **Schritt 4 – Setup-Assistent** > **Bildschirm 2 – Gerät.**
    - **Updates** – Updates von Plugins durchführen, entweder automatisch oder manuell über die Cloud oder offline.
    - **Zertifikat** – Informationen zu Ihrem HTTPS-Zertifikat anzeigen und eine sichere Verbindung sicherstellen, indem Sie entweder ein neues HTTPS-Zertifikat im System generieren oder Ihr eigenes hochladen. Siehe **Zertifikat**.
    - **API-Schlüssel** – API-Schlüssel generieren, um Apps von Drittanbietern den Zugriff auf Tenable.ot über die API zu ermöglichen. Alle Benutzer können API-Schlüssel erstellen. Der API-Schlüssel verfügt über dieselben Berechtigungen wie der Benutzer, der ihn erstellt hat, abhängig von dessen Rolle. Ein API-Schlüssel wird nur einmal angezeigt, nämlich wenn er generiert wird. Der Benutzer muss ihn zur späteren Verwendung an einem sicheren Ort speichern.
    - **Lizenz** – Die Lizenz anzeigen, aktualisieren und verlängern. Siehe **Lizenz**.
- **Umgebungskonfiguration**
    - **Asset-Einstellungen** –
        - **Überwachtes Netzwerk** – Die Aggregation von IP-Bereichen, in denen das System Assets klassifiziert, anzeigen und bearbeiten.
        - **Asset-Details per CSV aktualisieren** – Die Details von Assets mithilfe einer CSV-Vorlage aktualisieren.
        - **Assets manuell hinzufügen** – Der Asset-Liste mithilfe einer CSV-Vorlage neue Assets hinzufügen.

Maximal können 128 IP-Bereiche an den NNM gesendet werden, daher empfehlen wir, diese Grenze nicht zu überschreiten.

Zusätzlich zu den angegebenen IP-Bereichen werden alle Hosts in den Subnetzen der Tenable.ot-Plattform oder alle Geräte, die Aktivitäten ausführen, als Asset eingestuft.

  - **Ausgeblendete Assets** – Liste von Assets anzeigen, die im System ausgeblendet wurden (d. h. solche, die der Benutzer aus den Asset-Listen entfernt hat), siehe **Ausblenden von Assets**. Sie können ausgeblendete Assets über diesen Bildschirm wiederherstellen.
  - **Benutzerdefinierte Felder** – Sie können benutzerdefinierte Felder erstellen, um Assets mit relevanten Informationen zu taggen. Ein benutzerdefiniertes Feld kann Klartext oder ein Link zu einer externen Ressource sein.
  - **Ereigniscluster** – Ermöglicht es Ihnen, mehrere ähnliche Ereignisse, die innerhalb eines bestimmten Zeitraums auftreten, zusammenzufassen, um deren Überwachung zu vereinfachen. Siehe **Ereigniscluster**.
  - **PCAP-Player** – Ermöglicht es Ihnen, eine PCAP-Datei mit aufgezeichneter Netzwerkaktivität hochzuladen und auf Tenable.ot „abzuspielen", wobei die Daten in Ihr System geladen werden. Siehe **PCAP-Player**.

- **Benutzer und Rollen** – Informationen zu allen Benutzerkonten anzeigen, bearbeiten und exportieren.

  - **Benutzereinstellungen** – Informationen zu dem derzeit beim System eingeloggten Benutzer anzeigen und bearbeiten (vollständiger Name, Benutzername und Passwort) und die Sprache der Benutzeroberfläche ändern (Englisch, Japanisch, Chinesisch, Französisch oder Deutsch).
  - **Lokale Benutzer** – Ein Administratorbenutzer kann lokale Benutzerkonten für bestimmte Benutzer erstellen und dem Konto eine Rolle zuweisen. Siehe **Lokale Benutzer**.
  - **Benutzergruppen** – Ein Administratorbenutzer kann Benutzergruppen anzeigen, bearbeiten, hinzufügen und löschen. Siehe **Benutzergruppen**.
  - **Authentifizierungsserver** – Zugangsdaten von Benutzern können optional über einen LDAP-Server wie beispielsweise Active Directory zugewiesen werden. In diesem Fall werden die Benutzerrechte in Active Directory verwaltet. Siehe **Authentifizierungsserver**.

- **Integrationen** – Integration in andere Plattformen einrichten. Tenable.ot unterstützt derzeit die Integration in Palo Alto Networks Next Generation Firewall (NGFW) und Aruba ClearPass sowie in andere Tenable-Produkte (Tenable.sc und Tenable.io). Siehe **Integrationen**.
- **Server** – In Ihrem System konfigurierte Server anzeigen, erstellen und bearbeiten. Es werden separate Bildschirme für Folgendes angezeigt:

  - **SMTP-Server** – SMTP-Server ermöglichen das Versenden von Ereignisbenachrichtigungen per E-Mail.
  - **Syslog-Server** – Syslog-Server ermöglichen das Protokollieren von Ereignisprotokollen auf einem externen SIEM-System.
  - **FortiGate-Firewalls** – Mit der Tenable.ot-FortiGate-Integration können Benutzer auf der Grundlage der Tenable.ot-Netzwerkereignisse Vorschläge für Firewall-Richtlinien an eine FortiGate-Firewall senden.

- **Systemaktionen** – Zeigt ein Untermenü mit Systemaktivitäten an. Das Untermenü enthält die folgenden Optionen:

  - **Systemsicherung** – Ermöglicht es Ihnen, Ihre Tenable.ot-Appliance zu sichern (mit Ausnahme von Paketerfassungsdaten). Um das System aus einer Sicherungsdatei wiederherzustellen, besuchen Sie https://www.tenable.com/products/tenable-ot. Beachten Sie, dass Tenable.ot während des Sicherungsprozesses für Benutzer nicht verfügbar ist.
  - **Einstellungen exportieren** – Exportiert die Konfigurationseinstellungen der Tenable.ot-Plattform als NDG-Datei auf den lokalen Computer. Dies dient als Backup im Falle einer Systemzurücksetzung oder ermöglicht das Importieren der Einstellungen in eine neue Tenable.ot-Plattform.
  - **Einstellungen importieren** – Importiert die Konfigurationseinstellungen der Tenable.ot-Plattform, die als NDG-Datei auf dem lokalen Computer gespeichert wurden.
  - **Diagnosedaten herunterladen** – Erstellt eine Datei mit Diagnosedaten auf der Tenable.ot-Plattform und speichert sie auf dem lokalen Computer.
  - **Neu starten** – Startet die Tenable.ot-Plattform neu. Dies ist für die Aktivierung bestimmter Konfigurationsänderungen erforderlich.

- **Deaktivieren** – Deaktiviert alle Überwachungsaktivitäten. Sie können die Überwachungsaktivitäten jederzeit wieder aktivieren.
- **Herunterfahren** – Fährt die Tenable.ot-Plattform herunter. Drücken Sie zum Einschalten die Power-Taste auf der Tenable.ot Appliance.
- **Zurücksetzung auf Werkseinstellungen** – Setzt alle Einstellungen auf die standardmäßigen Werkseinstellungen zurück. Warnung: Dieser Vorgang kann nicht rückgängig gemacht werden und alle Daten im System gehen verloren.

- **Systemprotokoll** – Zeigt ein Protokoll aller Systemereignisse an (z. B. Richtlinie aktiviert, Richtlinie bearbeitet, Ereignis aufgelöst usw.), die im System aufgetreten sind. Sie können das Protokoll als CSV-Datei exportieren oder an einen Syslog-Server senden. Siehe **Systemprotokoll**.

Abfragen

In den Abfrage-Bildschirmen von Tenable.ot können Sie die Abfragefunktionen konfigurieren und aktivieren. Eine allgemeine Erläuterung der Abfragetechnologie finden Sie unter **Tenable.ot-Technologien**. Im Rahmen der Ersteinrichtung wurde empfohlen, die gesamte Abfragefunktionalität zu aktivieren. Sie können jede der Abfragefunktionen jederzeit aktivieren/deaktivieren. Außerdem können Sie die Einstellungen anpassen, die steuern, wann und wie die Abfragen ausgeführt werden.

Zusätzlich zur regelmäßigen Ausführung automatischer Abfragen können die meisten Abfragen vom Benutzer bei Bedarf initiiert werden, indem er auf die Schaltfläche **Jetzt ausführen** neben der Abfrage klickt.

Die Schwachstellen-Scans Log4J und Ripple20 können nur **manuell** ausgeführt werden, nicht nach einem regelmäßigen Zeitplan. Sie werden über den Bildschirm **Lokale Einstellungen** > **Abfragen** > **Netzwerk** aktiviert, siehe **Tabelle der Netzwerkabfragefunktionen**.

Das Deaktivieren der Abfragen verhindert, dass das System signifikante Ereignisse im Netzwerk erkennt. Viele Funktionen sind dann nicht mehr verfügbar.

Die Aktivierung und Konfiguration von Abfragen erfolgt unter **Lokale Einstellungen** > **Abfragen**. Die Abfragen sind in drei separate Bildschirme unterteilt. In den folgenden Abschnitten werden die verschiedenen Typen von Abfragen erläutert und Verfahren zum Aktivieren und Konfigurieren der einzelnen Abfragetypen beschrieben.

Alle Controller-Abfragen

➡ So aktivieren Sie Controller-Abfragen:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Abfragen** > **Controller**.
2. Stellen Sie den Umschalter für **Alle Controller-Abfragen** auf **EIN**.
3. Aktivieren/deaktivieren Sie bestimmte Abfragetypen, indem Sie den Status für jeden Abfragetyp auf **EIN/AUS** umschalten. Eine Beschreibung der verschiedenen Typen von Controller-Abfragen finden Sie in der **Tabelle der Controller-Abfragefunktionen**.

4. Sie können die Einstellungen für jeden Controller-Abfragetyp mithilfe des folgenden Verfahrens bearbeiten:
    a. Klicken Sie neben dem gewünschten Abfragetyp auf **Bearbeiten**.
    b. Passen Sie die Frequenz und den Zeitplan der Abfragen an (eine Erklärung der verfügbaren Einstellungsoptionen finden Sie in der **Tabelle der Controller-Abfragefunktionen**).
    c. Klicken Sie auf **Speichern**.

Tabelle der Controller-Abfragefunktionen

Funktion	Beschreibung	Frequenz (Min.–Max.)
Alle Controller-Abfragen	Aktiviert alle Abfragefunktionen in Bezug auf Controller, wie unten beschrieben.	N/A
Periodische Snapshots	Erfasst das auf den einzelnen Controllern bereitgestellte aktuelle Programm. Durch die regelmäßige Erstellung von Snapshots kann Tenable.ot Änderungen erkennen, die am Programm eines Controllers vorgenommen wurden, selbst wenn die Änderungen nicht über das Netzwerk gesendet wurden.	1/Tag–1/6 Wochen
Per Richtlinie ausgelöste Snapshots	Ermöglicht es dem Benutzer, Richtlinien so zu konfigurieren, dass ein Snapshot ausgelöst wird, wenn die Bedingungen einer Richtlinie erfüllt sind.	N/A
Controller-Erfassung	Ein Broadcast, der nach neuen Controllern sucht und bei der Klassifizierung unbekannter Assets hilft.	1/Std.–1/6 Wochen
Abfrage des Controller-Status	Erkennt den aktuellen SPS-Status (Optionen: *Wird ausgeführt*, *Gestoppt*, *Fehler*, *Keine Konfig.* und *Test*).	1/5 Min.–1/Std.
Abfrage des Diagnosepuffers	Abfragen der Diagnosepuffer-Ereignisprotokolle, wie in Siemens-Controllern definiert.	1/Tag–1/6 Wochen
Abfrage der Controller-Details	Ruft die Details zur Hardware und Firmware des Controllers ab.	1/Std.–1/6 Wochen
Backplane-Abfrage	Erfasst Module und ihre Spezifikationen innerhalb einer Backplane. Diese Abfrage ermöglicht die schnelle Identifizierung der gesamten Backplane-Konfiguration.	1/15 Min.–1/Woche

Alle Netzwerkabfragen

So aktivieren Sie Netzwerkabfragen:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Abfragen** > **Netzwerk**.
2. Stellen Sie den Umschalter für **Alle Netzwerkabfragen** auf **EIN**.
3. Aktivieren/deaktivieren Sie bestimmte Abfragetypen, indem Sie den Status für jeden Abfragentyp auf **EIN/AUS** umschalten. Eine Beschreibung der verschiedenen Netzwerkabfragefunktionen finden Sie in der **Tabelle der Netzwerkabfragefunktionen**.
4. Sie können die Einstellungen für jeden Netzwerkabfragetyp mithilfe des folgenden Verfahrens bearbeiten:
    a. Klicken Sie neben dem gewünschten Abfragetyp auf **Bearbeiten**.
    b. Passen Sie die Frequenz und den Zeitplan der Abfragen an (eine Erklärung der verfügbaren Einstellungsoptionen finden Sie in der **Tabelle der Netzwerkabfragefunktionen**).
    c. Klicken Sie auf **Speichern**.

Tabelle der Netzwerkabfragefunktionen

Funktion	Beschreibung	Einstellungen
Alle Netzwerkabfragen	Aktiviert alle Abfragefunktionen in Bezug auf andere Netzwerk-Assets als Controller, wie unten beschrieben.	N/A
Port-Zuordnung	Identifiziert alle offenen Ports in Netzwerk-Assets. Dies ermöglicht es Ihnen, Sicherheitsrisiken zu minimieren, indem Sie ungenutzte Ports schließen.	Zuordnungsbereich – Legen Sie fest, ob die Zuordnung für alle Ports oder nur für die 1.000 am häufigsten verwendeten Ports erfolgen soll. Zuordnungsrate – Legen Sie die Anzahl der pro Sekunde standardmäßig zugeordneten Ports und die maximale Rate für die On-Demand-Zuordnung fest.
SNMP-Abfrage	Sammelt Konfigurationsinformationen von SNMP-fähigen Assets im Netzwerk.	SNMP V2-Community-Zeichenfolgen SNMP V3-Benutzernamen Frequenz und Zeitplan – 1/Tag–1/6 Wochen
DNS-Abfrage	Sucht nach den DNS-Namen der Assets im Netzwerk.	N/A
ARP-Abfrage	Ruft die MAC-Adresse von neuen IPs ab, die im Netzwerk erkannt wurden.	N/A
NetBIOS	Diese Abfrage sendet ein NetBIOS-Unicast-Paket, mit dem Windows-Computer im Netzwerk klassifiziert und ermittelt werden.	Frequenz und Zeitplan – 1/Std.–1/6 Wochen
Aktive Asset-Verfolgung	Ermittelt Assets, die für den angegebenen Zeitraum im Netzwerk inaktiv sind, und fragt sie ab, um zu überprüfen, ob sie noch aktiv sind.	Frequenz und Zeitplan – 1/5 Min.–1/Woche
WMI-Abfrage	Sammelt Informationen über Windows-Computer im Netzwerk.	WMI-Benutzername – von IT bereitgestellt Passwort – von IT bereitgestellt Frequenz und Zeitplan – 1/Tag–1/6 Wochen Test-IP-Adresse – Sie können die WMI-Konfiguration testen, indem Sie auf „Test-IP-Adresse“ klicken, die IP eines bekannten Windows-Computers in Ihrem Netzwerk eingeben und dann unten im Bildschirm auf „Test-IP-Adresse“ klicken. Anschließend können Sie die Asset-Details für dieses Asset öffnen und überprüfen, ob die WMI-Informationen hinzugefügt wurden.
Abfrage der USB-Verbindungen	Erkennt den Anschluss von USB/DoK-Geräten an Windows-PCs im Netzwerk.	Frequenz und Zeitplan – 1/Tag–1/6 Wochen

Funktion	Beschreibung	Einstellungen
Ripple20-Schwachstellen-Scanning	Dieser Scan identifiziert CVEs im Zusammenhang mit den Ripple20-Schwachstellen. Er verwendet ein Nessus-Plugin. **Hinweis:** Dieser Scan muss **manuell** ausgeführt werden und wird nur für die Assets innerhalb der angegebenen IP-Adressen und/oder CIDRs ausgeführt.	IP-Adressen oder CIDRs
Log4J-Schwachstellen-Scan	Dieser Scan identifiziert CVEs im Zusammenhang mit den Log4J-Schwachstellen. Er verwendet ein Nessus-Plugin. **Hinweis:** Dieser Scan muss manuell ausgeführt werden und wird nur für die Assets innerhalb der angegebenen IP-Adressen und/oder CIDRs ausgeführt.	IP-Adressen oder CIDRs

Asset-Erfassung

Tenable.ot identifiziert Assets im Netzwerk automatisch, indem es ihre Interaktionen mit anderen Assets über das Netzwerk erkennt. Mit dem Abfragetyp **Asset-Erfassung** verfügt Tenable.ot über eine zusätzliche Funktion zum Identifizieren von Assets, die nicht im Netzwerk aktiv sind oder deren Kommunikationsströme nicht von den Spiegelports erfasst werden. Sie können die Frequenz konfigurieren, mit der die Abfrage automatisch ausgeführt wird. Außerdem können Sie die Abfrage auch jederzeit von diesem Bildschirm aus manuell ausführen.

Sobald ein neues Asset erkannt wird, führt die Funktion **Erste Asset-Anreicherung** die folgenden Abfragen aus, um genaue Informationen über das Asset zu ermitteln: SNMP, Prüfung auf minimale Anzahl offener Ports, CIP/DCP, NetBIOS, Backplane-Abfrage, Unicast-Identifizierung, Controller-Details und Controller-Status.

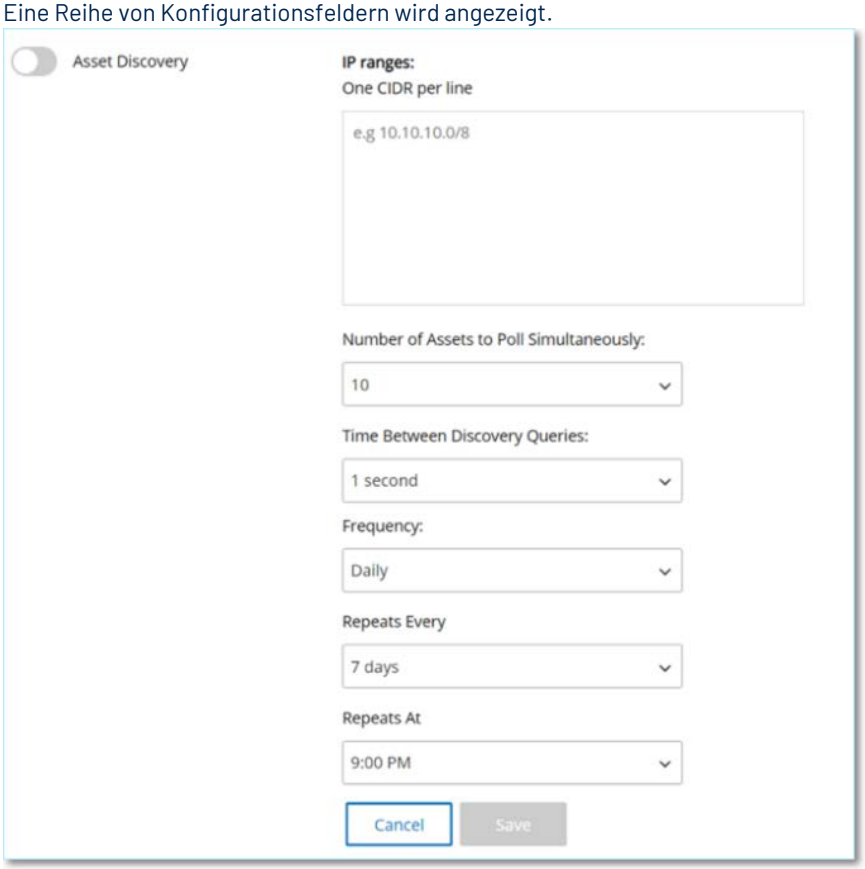
Nur IP-Adressen, die in den **Asset-Einstellungen** als überwachte Netzwerke definiert sind, werden in den Scan einbezogen.

Das Deaktivieren der Abfragen verhindert, dass das System signifikante Ereignisse im Netzwerk erkennt. Viele Funktionen sind dann nicht mehr verfügbar.

So aktivieren Sie den Abfragetyp „Asset-Erfassung“:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Abfragen** > **Asset-Erfassung**.

2. Klicken Sie im Abschnitt **Asset-Erfassung** auf **Bearbeiten**.
   Eine Reihe von Konfigurationsfeldern wird angezeigt.



3. Geben Sie im Feld **IP-Bereiche** einen oder mehrere IP-Bereiche ein (jeder Bereich in einer separaten Zeile).

> Segmente Ihres Netzwerks, die vom Spiegelport überwacht werden, müssen nicht eingegeben werden und werden automatisch von Tenable.ot abgefragt. Wenn Sie die Asset-Erfassungsabfrage für **zusätzliche** Segmente Ihres Netzwerks ausführen möchten, die nicht vom Spiegelport überwacht werden, geben Sie den IP-Bereich für diese Segmente in dieses Feld ein.

4. Sie können die folgenden Konfigurationseinstellungen anpassen (optional), indem Sie einen Wert im Dropdown-Menü auswählen.
   - **Anzahl an Assets, die gleichzeitig abgefragt werden** (Optionen: 10, 20, 30)
   - **Zeit zwischen Erfassungsabfragen** (Optionen: 1–3 Sekunden)
   - **Wird wiederholt** – Legen Sie die Art des Intervalls fest, das zum Festlegen der Frequenz der Abfrage verwendet wird (täglich oder wöchentlich).
   - **Wiederholungen alle** – Legen Sie die Abfragefrequenz fest (Täglich: 1–31 Tage, Wöchentlich: 1–6 Wochen).
   - **Am** – Für ein wöchentliches Intervall legen Sie den Wochentag fest, an dem die Abfrage ausgeführt wird.
   - **Um** – Legen Sie die Tageszeit fest, zu der die Abfrage ausgeführt wird.
5. Klicken Sie auf **Speichern**.
6. Setzen Sie den Umschalter **Asset-Erfassung** auf **EIN**.

➡ So aktivieren Sie die erste Asset-Anreicherung:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Abfragen** > **Asset-Erfassung**.
2. Stellen Sie den Umschalter **Erste Asset-Anreicherung** auf **EIN**.

Nessus-Plugin-Scans

Der Nessus-Plugin-Scan startet einen erweiterten Nessus-Scan, der eine benutzerdefinierte Liste von Plugins für die Assets ausführt, die in der Liste der CIDRs und IP-Adressen angegeben sind.

Der Scan wird für reaktionsfähige Assets innerhalb der angegebenen CIDRs ausgeführt. Um Ihre OT-Geräte zu schützen, werden jedoch nur bestätigte Netzwerk-Assets im angegebenen Bereich (Nicht-SPS) gescannt. Assets vom Typ „Endgerät“ werden nicht gescannt.

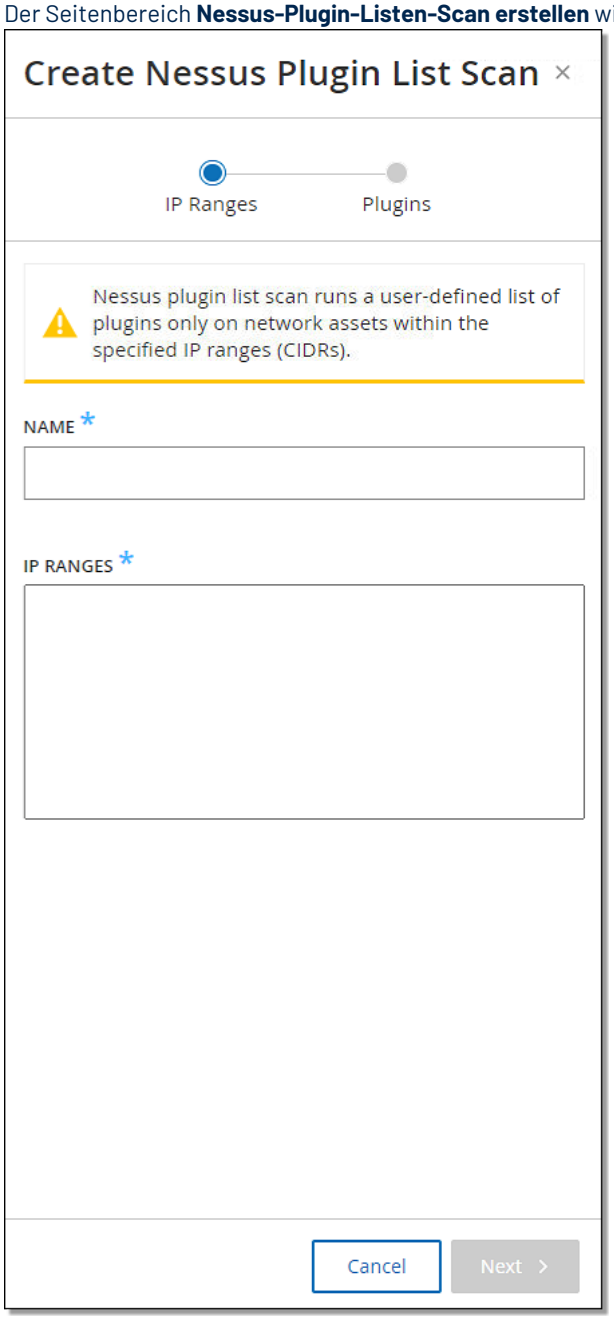
Nessus ist ein invasives Tool, das am besten in IT-Umgebungen funktioniert. Es wird nicht für die Verwendung auf OT-Geräten empfohlen, da es deren normalen Betrieb beeinträchtigen kann.

Um einen grundlegenden Nessus-Scan für ein einzelnes Asset durchzuführen, siehe **Durchführen eines Asset-spezifischen Nessus-Scans**.

Der einfache Scan kann für Assets vom Typ „Endgerät“ ausgeführt werden.

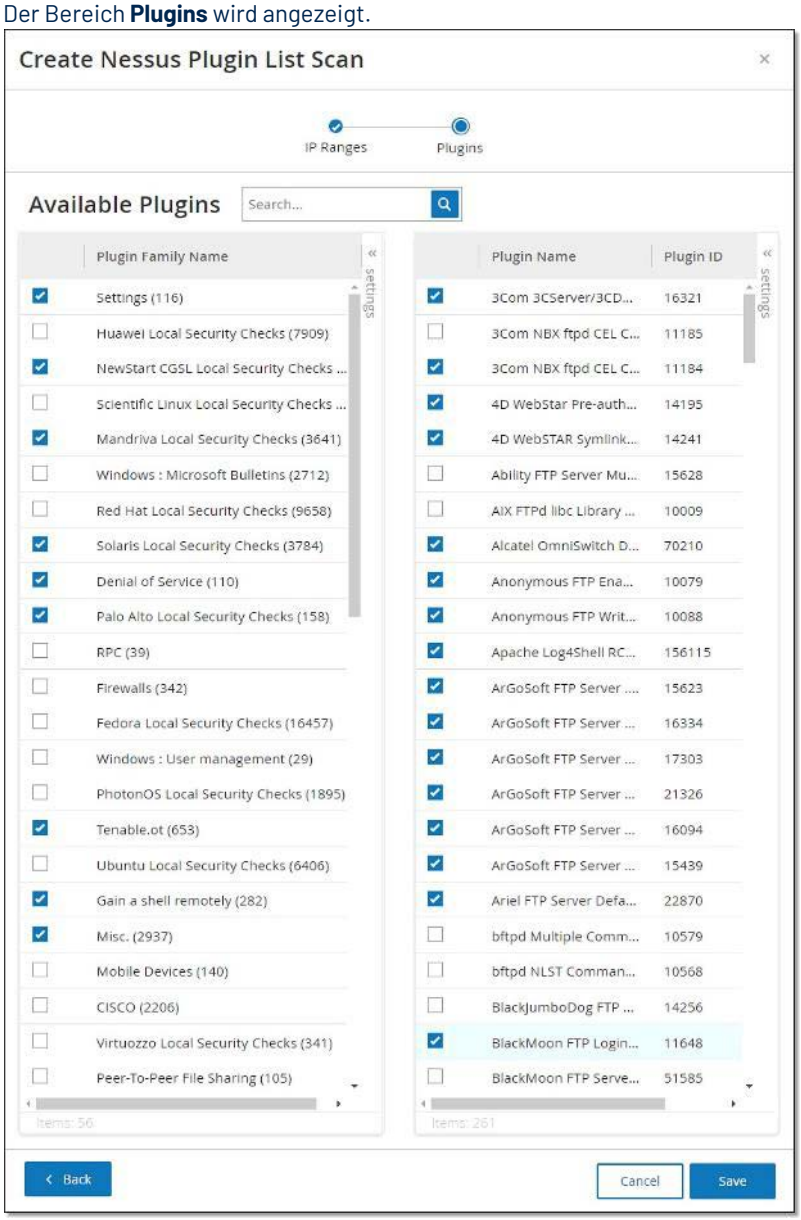
So erstellen Sie einen Nessus-Plugin-Scan:

1. Gehen Sie zu **Lokale Einstellungen** > **Abfragen** > **Nessus-Scans**.
2. Klicken Sie auf die Schaltfläche **Scan erstellen**.
   Der Seitenbereich **Nessus-Plugin-Listen-Scan erstellen** wird angezeigt.



3. Geben Sie im Feld **Name** einen Namen für den Nessus-Scan ein.
4. Geben Sie im Feld **IP-Bereiche** einen Bereich von IP-Adressen oder CIDRs ein.

5. Klicken Sie auf **Weiter**.
   Der Bereich **Plugins** wird angezeigt.



Die angezeigten Plugins sind gerätespezifisch. Sie benötigen eine aktuelle Lizenz, um neue Plugins zu erhalten. Informationen zum Aktualisieren Ihrer Lizenz finden Sie unter **Aktualisieren der Lizenz**.

6. Wählen Sie in der linken Spalte die gewünschten Plugin-Familien aus, die in den Scan einbezogen werden sollen, und deaktivieren Sie in der rechten Spalte einzelne Plugins nach Bedarf.

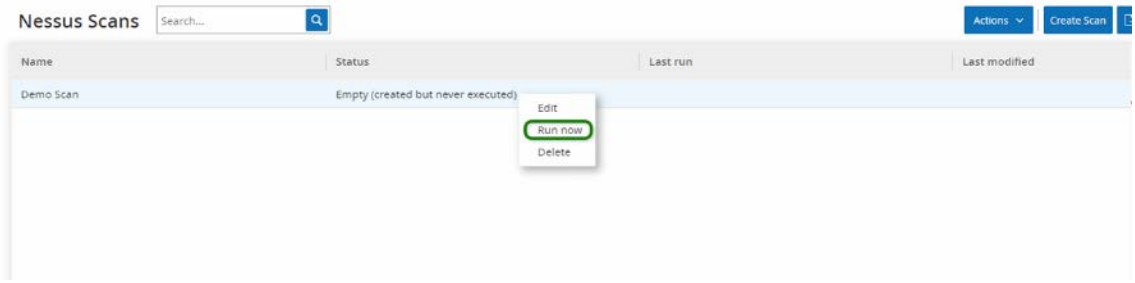
Weitere Informationen zu Nessus-Plugin-Familien finden Sie unter https://www.tenable.com/plugins/nessus/families.

7. Klicken Sie auf **Speichern**.
   Der neue Nessus-Scan wird im Bildschirm **Nessus-Scans** angezeigt.

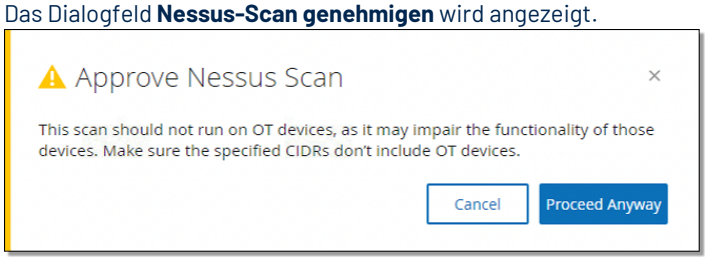
Um einen vorhandenen Nessus-Scan zu bearbeiten oder zu löschen, klicken Sie mit der rechten Maustaste auf die Zeile des gewünschten Scans und wählen Sie **Bearbeiten** oder **Löschen** aus.

So führen Sie einen Nessus-Plugin-Scan aus:

1. Wählen Sie im Bildschirm **Nessus-Scans** die Zeile des gewünschten Scans aus, klicken Sie mit der rechten Maustaste und wählen Sie **Jetzt ausführen** aus oder klicken Sie auf **Aktionen > Jetzt ausführen**.



   Das Dialogfeld **Nessus-Scan genehmigen** wird angezeigt.



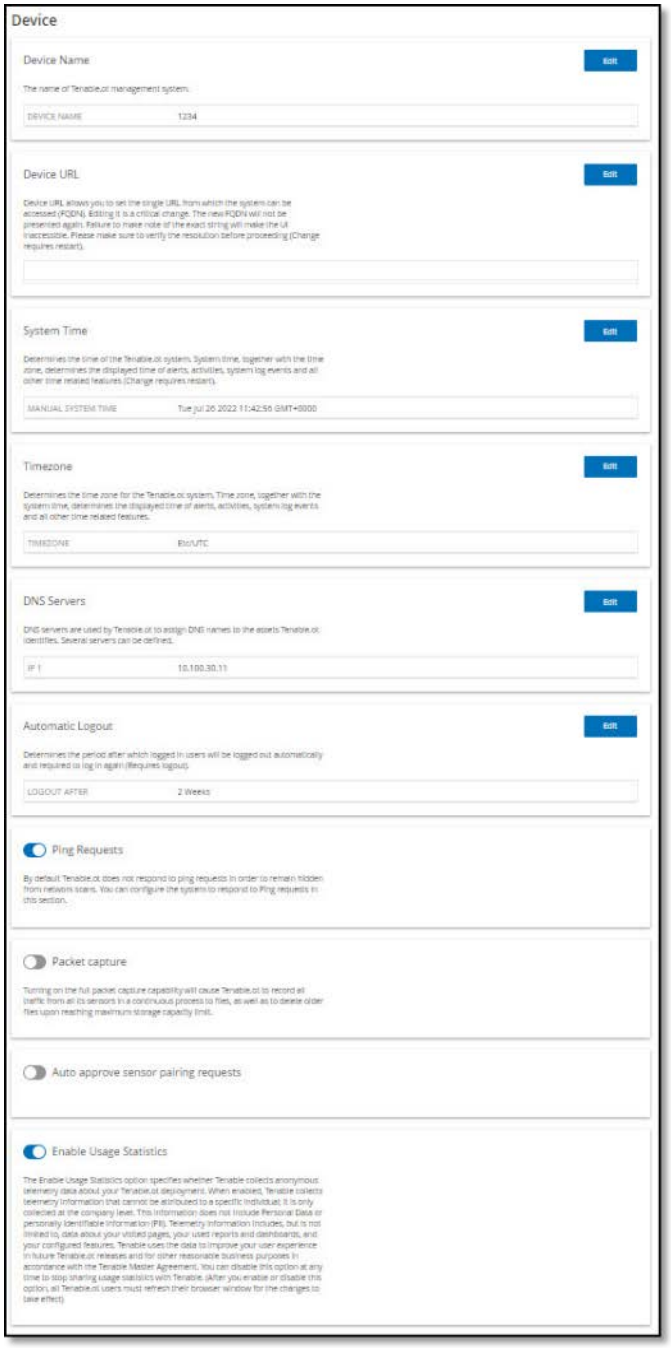
2. Wenn Sie wissen, dass der Scan keine OT-Geräte umfasst, klicken Sie auf **Trotzdem fortfahren**.
   Das Dialogfeld wird geschlossen und der Scan wird gespeichert.
3. Um den Scan auszuführen, klicken Sie erneut mit der rechten Maustaste auf die Zeile des Scans und wählen Sie **Jetzt ausführen** aus.
   Das Dialogfeld **Nessus-Scan genehmigen** wird erneut angezeigt.
4. Klicken Sie auf **Trotzdem fortfahren**.
   Der Scan wird jetzt ausgeführt. Scans können abhängig von ihrem aktuellen Status angehalten/fortgesetzt, gestoppt und beendet werden.

Systemkonfiguration

Die Bildschirme zur Systemkonfiguration von Tenable.ot ermöglichen es Ihnen, Plugin-Updates automatisch zu konfigurieren und manuell durchzuführen sowie Details zu Ihrem Gerät, HTTPS-Zertifikat, den API-Schlüsseln und der Lizenz anzuzeigen und zu aktualisieren.

Gerät

Dieser Bildschirm enthält detaillierte Informationen zu Ihrer Tenable.ot-Konfiguration. Sie können in diesem Bildschirm die Informationen anzeigen und die Konfiguration bearbeiten.



Die folgenden Informationen werden angezeigt:

- **Gerätename** – Ein eindeutiger Bezeichner für die Tenable.ot Appliance.

- **Geräte-URL** – Hier können Sie die einzelne URL festlegen, über die auf das System zugegriffen werden kann (FQDN).

Eine Bearbeitung der Geräte-URL ist eine kritische Änderung. Der neue FQDN wird nicht noch einmal angezeigt. Wenn Sie sich die exakte Zeichenfolge nicht notieren, wird die Benutzeroberfläche unzugänglich. Prüfen Sie unbedingt die Auflösung, bevor Sie fortfahren.

- **Systemzeit** – Die richtige Uhrzeit und das richtige Datum werden im Allgemeinen automatisch eingestellt, können jedoch bearbeitet werden.

Die Einstellung des richtigen Datums und der richtigen Uhrzeit ist für die genaue Aufzeichnung von Protokollen und Warnungen unerlässlich.

- **Zeitzone** – Wählen Sie die lokale Zeitzone am Standort in der Dropdown-Liste aus.
- **DNS-Server** – DNS-Server werden vom Tenable.ot-System verwendet, um den von Tenable.ot identifizierten Assets DNS-Namen zuzuweisen. Es können mehrere Server identifiziert werden.
- **Automatisch ausloggen** – Legt den Zeitraum fest, nach dem eingeloggte Benutzer automatisch ausgeloggt werden und sich erneut einloggen müssen.
- **Zeitraum, nach dem offene Ports als veraltet gelten**– Legt den Zeitraum fest, nach dem Auflistungen offener Ports aus dem Bildschirm mit individuellen Asset-Details entfernt werden, wenn kein weiterer Hinweis darauf eingeht, dass der Port noch offen ist. Die Standardeinstellung ist zwei Wochen. Weitere Informationen finden Sie unter **Offene Ports**.

Ping-Anfragen

Durch Aktivieren von Ping-Anfragen wird die automatische Antwort der Tenable.ot-Plattform auf Ping-Anfragen aktiviert.

➡ So aktivieren Sie Ping-Anfragen:

1. Gehen Sie zum Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Gerät**.
2. Setzen Sie den Umschalter **Ping-Anfragen** auf **EIN**.

Paketerfassungen

Durch Einschalten der Funktion zur vollständigen Paketerfassung wird die kontinuierliche Aufzeichnung von vollständigen Paketerfassungen des gesamten Traffic im Netzwerk aktiviert. Dadurch sind umfangreiche Möglichkeiten zur Fehlersuche und forensischen Untersuchung gegeben. Wenn die Speicherkapazität (1,8 TB) überschritten wird, löscht das System ältere Dateien. Sie können verfügbare Dateien im Bildschirm **Netzwerk** > **Paketerfassungen** anzeigen und herunterladen, siehe Abschnitt **Paketerfassungen**.

➡ So aktivieren Sie Paketerfassungen:

1. Gehen Sie zum Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Gerät**.
2. Stellen Sie den Umschalter **Paketerfassung** auf **EIN**.

Sie können die Paketerfassungsfunktion jederzeit stoppen, indem Sie den Umschalter auf **AUS** stellen.

Sensorkopplungsanforderungen automatisch genehmigen

Die Aktivierung der automatischen Genehmigung eingehender Sensorkopplungsanforderungen stellt sicher, dass alle Sensorkopplungsanforderungen genehmigt werden, ohne dass zusätzliche Schritte vom Administrator

ausgeführt werden müssen. Wenn diese Option nicht aktiviert ist, ist eine abschließende manuelle Genehmigung erforderlich, damit sich neue Sensoren mit Ihrem Netzwerk verbinden können.

➡ So aktivieren Sie die automatische Genehmigung eingehender Sensorkopplungsanforderungen:

1. Gehen Sie zum Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Gerät**.
2. Stellen Sie den Umschalter **Sensorkopplungsanforderungen automatisch genehmigen** auf **EIN**.

Sie können die automatische Genehmigung eingehender Sensorkopplungsanforderungen jederzeit zulassen, indem Sie den Schalter auf **AUS** stellen.

Nutzungsstatistiken aktivieren

Mit der Option „Nutzungsstatistiken aktivieren“ wird festgelegt, ob Tenable anonyme Telemetriedaten über Ihre Tenable.ot-Bereitstellung erfassen soll. Wenn diese Option aktiviert ist, erfasst Tenable Telemetriedaten, die keiner bestimmten Person zugeordnet werden können. Die Daten werden nur auf Unternehmensebene erhoben. Diese Informationen enthalten keine persönlichen Daten oder personenbezogenen Informationen (PII). Telemetriedaten umfassen unter anderem Angaben zu den von Ihnen besuchten Seiten, den von Ihnen verwendeten Berichten und Dashboards und den von Ihnen konfigurierten Funktionen. Tenable verwendet die Daten, um Ihre Benutzererfahrung in zukünftigen Tenable.ot-Versionen zu verbessern sowie für andere angemessene Geschäftszwecke in Übereinstimmung mit dem Tenable-Rahmenvertrag. Diese Einstellung ist standardmäßig aktiviert.

➡ So aktivieren Sie Nutzungsstatistiken:

1. Gehen Sie zum Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Gerät**.
2. Stellen Sie den Umschalter **Nutzungsstatistiken aktivieren** auf **EIN**.

Sie können das Teilen von Nutzungsstatistiken jederzeit deaktivieren, indem Sie den Umschalter auf **AUS** stellen.

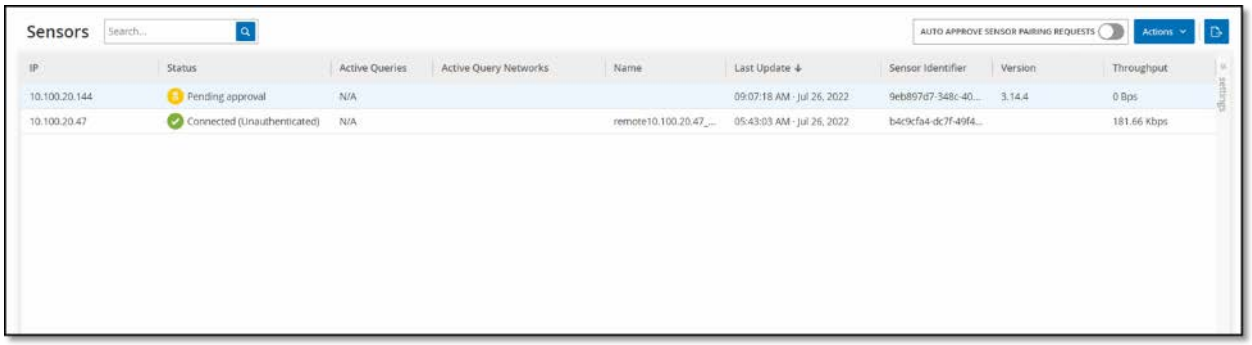
Sensoren

Nachdem Sensoren über die Tenable Core-UI gekoppelt wurden, können Sie neue Kopplungen genehmigen und Sensoren anzeigen und mit den Funktionen „Bearbeiten“, „Anhalten“ und „Löschen“ im Menü **Aktionen** verwalten. Sie können auch die automatische Genehmigung von Sensorkopplungsanforderungen mit dem Umschalter aktivieren.

Sensormodelle vor Version 2.214 werden nicht auf der Seite **Sensoren** für ICP angezeigt. Sie können jedoch weiterhin im nicht authentifizierten Modus verwendet werden.

Anzeigen des Bildschirms „Sensoren“

Die Sensortabelle enthält eine Liste aller Sensoren der Version 2.214 und höher im System.



Die angezeigten Informationen werden in der folgenden Tabelle beschrieben:

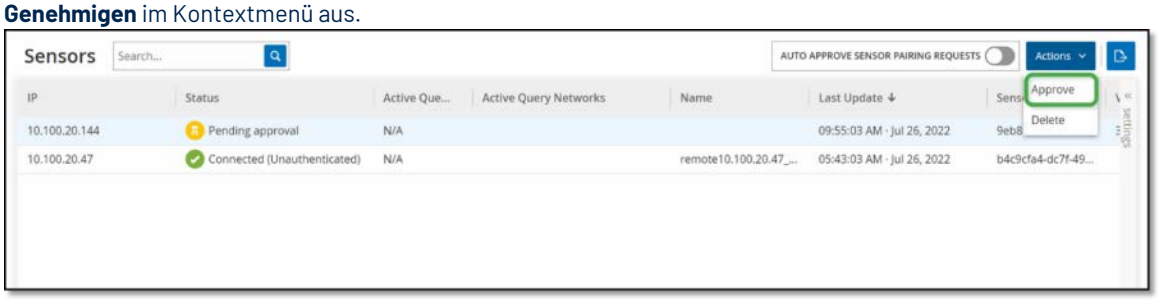
Parameter	Beschreibung
IP	Die IPv4-Adresse des Sensors.
Status	Der Status des Sensors: Verbunden, Verbunden (nicht authentifiziert), Genehmigung ausstehend, Getrennt oder Angehalten.
Aktive Abfragen	Die Fähigkeit des Sensors, aktive Abfragen zu senden (Aktiviert, Deaktiviert, N/A).
Aktive Abfragenetzwerke	Die Netzwerksegmente, denen der Sensor zugewiesen ist.
Name	Der Name des Sensors im System.
Letzte Aktualisierung	Datum und Uhrzeit der letzten Aktualisierung der Sensorinformationen.
Sensor-ID	Der universelle eindeutige Bezeichner (UUID) des Sensors, ein 128-Bit-Wert, der verwendet wird, um ein Objekt oder eine Entität im Internet eindeutig zu identifizieren.
Version	Die Version des Sensors.
Durchsatz	Ein Maß dafür, wie viele Daten den Sensor durchlaufen (in Kilobyte pro Sekunde).

Manuelles Genehmigen eingehender Sensorkopplungsanforderungen

Wenn die Einstellung **Sensorkopplungsanforderungen automatisch genehmigen** auf **AUS** festgelegt ist, müssen eingehende Sensorkopplungsanforderungen manuell genehmigt werden, bevor die Sensoren erfolgreich verbunden werden.

So genehmigen Sie eine Sensorkopplungsanforderung manuell:

1. Gehen Sie zum Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Sensoren**.
2. Klicken Sie in der Tabelle auf eine Zeile mit dem Status **Genehmigung ausstehend**.
3. Klicken Sie auf **Aktionen** > **Genehmigen** oder klicken Sie mit der rechten Maustaste und wählen Sie **Genehmigen** im Kontextmenü aus.



Wenn Sie einen Sensor löschen möchten, können Sie auf **Aktionen** > **Löschen** klicken oder mit der rechten Maustaste klicken und **Löschen** im Kontextmenü auswählen.

Konfigurieren aktiver Abfragen

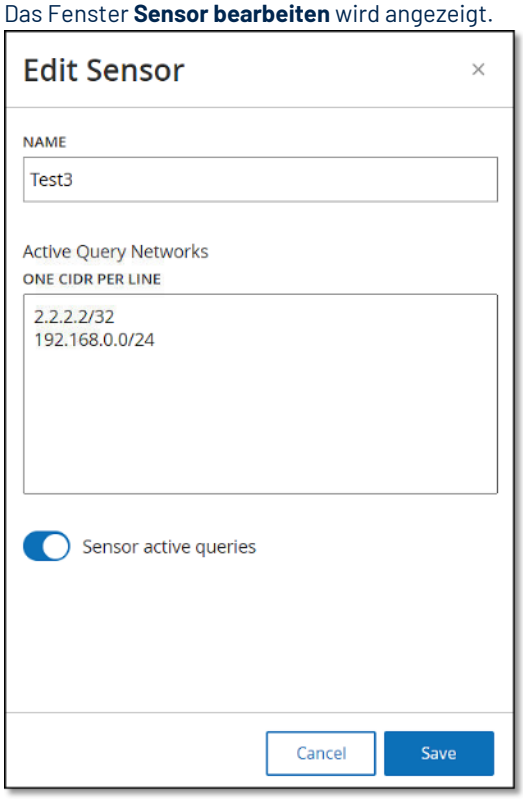
Sobald ein Sensor im *authentifizierten* Modus verbunden ist, kann er so konfiguriert werden, dass er aktive Abfragen in den Netzwerksegmenten durchführt, denen er zugewiesen ist. Sie müssen angeben, welche Netzwerksegmente abgefragt werden.

Sensoren führen unabhängig von dieser Konfiguration eine passive Netzwerkerkennung in allen verfügbaren Segmenten durch.

So konfigurieren Sie aktive Abfragen:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Sensoren**.
2. Klicken Sie in der Tabelle auf eine Zeile mit dem Status **Verbunden**.

3. Klicken Sie auf **Aktionen** > **Bearbeiten** oder klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten** im Kontextmenü aus.
   Das Fenster **Sensor bearbeiten** wird angezeigt.



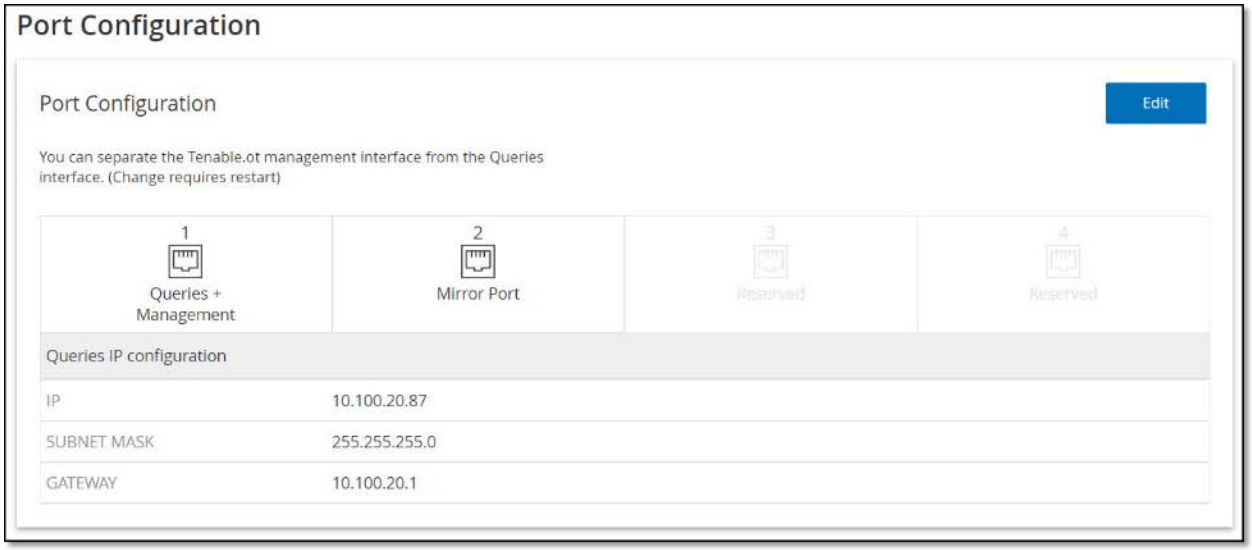
4. Wenn Sie den Sensor umbenennen möchten, bearbeiten Sie den Text im Feld **Name**.
5. Im Feld **Aktive Abfragenetzwerke** können Sie relevante Netzwerksegmente hinzufügen oder bearbeiten, an die der Sensor aktive Abfragen sendet. Verwenden Sie hierzu die CIDR-Notation und fügen Sie jedes Subnetzwerk in einer separaten Zeile hinzu.

> Abfragen können nur für CIDRs durchgeführt werden, die in den überwachten Netzwerkbereichen enthalten sind. Achten Sie darauf, nur CIDRs hinzuzufügen, auf die über diesen Sensor zugegriffen werden kann. Wenn Sie CIDRs hinzufügen, auf die nicht zugegriffen werden kann, wird hierdurch möglicherweise die Fähigkeit des ICP beeinträchtigt, diese Segmente auf andere Weise abzufragen.

6. Setzen Sie den Umschalter **Aktive Sensorabfragen** auf **EIN**, um aktive Abfragen zu aktivieren.
7. Klicken Sie auf **Speichern**.
   Das Fenster wird geschlossen.
   In der Tabelle **Sensoren** wird unter der Überschrift **Aktive Abfragen** für die aktivierten Sensoren jetzt **Aktiviert** angezeigt.

Portkonfiguration

Der Bildschirm **Portkonfiguration** zeigt die Konfiguration der Ports des Geräts. Weitere Informationen zur Portkonfiguration finden Sie unter **Installieren der Tenable.ot Appliance** > **Schritt 4 – Setup-Assistent** > **Bildschirm 2 – Gerät.**



Updates

Indem Sie dafür sorgen, dass Plugins und der IDS-Engine-Regelsatz stets auf dem neuesten Stand sind, stellen Sie sicher, dass Ihre Assets auf die neuesten bekannten Schwachstellen überwacht werden. Updates können über die Cloud – sowohl automatisch als auch manuell – und auch offline durchgeführt werden.

Sie können Updates auch über den Bildschirm **Schwachstellen** durchführen, indem Sie auf die Schaltfläche **Plugins aktualisieren** klicken.

Wenn die Benutzerlizenz abläuft, wird die Option zum Herunterladen neuer Updates blockiert und der Benutzer kann seine Plugins nicht aktualisieren.

Updates des Nessus-Plugin-Satzes

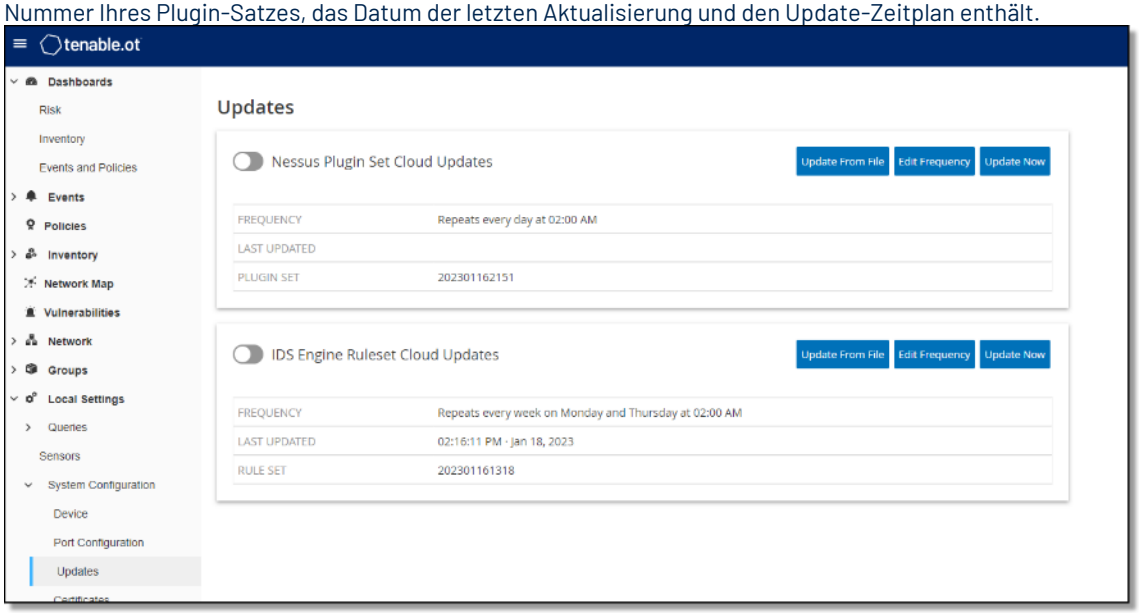
Cloud-Updates

Benutzer mit Internetverbindung können Plugins über die Cloud aktualisieren. Wenn automatische Updates aktiviert sind, werden Plugins zu der vom Benutzer festgelegten Zeit und in der festgelegten Frequenz aktualisiert (Standard: täglich um 02:00 Uhr).

Festlegen automatischer Cloud-Updates von Plugins

➡ So aktivieren Sie automatische Updates von Plugins:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für Nessus-Plugin-Satz** angezeigt, der die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.

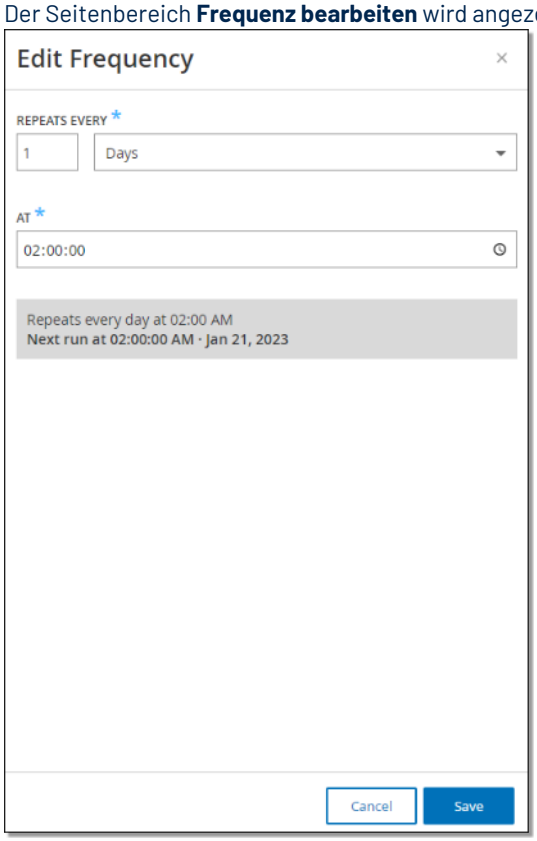


2. Wenn der Umschalter nicht auf EIN gestellt ist, klicken Sie darauf, um automatische Updates zu aktivieren.

➡ So bearbeiten Sie den Zeitplan für automatische Updates von Plugins:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für Nessus-Plugin-Satz** angezeigt, der die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.

2. Klicken Sie auf die Schaltfläche **Frequenz bearbeiten**.
   Der Seitenbereich **Frequenz bearbeiten** wird angezeigt.



3. Legen Sie unter **Wiederholungen alle** das Zeitintervall fest, in dem Sie die Plugins aktualisieren möchten, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) aus dem Dropdown-Menü wählen.
4. Bei Auswahl von **Wochen** wählen Sie die Wochentage aus, an denen Sie ein wöchentliches Update der Plugins durchführen möchten.
5. Legen Sie unter **Um** die Tageszeit fest, zu der Sie die Plugins aktualisieren möchten (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.
6. Klicken Sie auf **Speichern**.
   Es wird ein Dialogfeld mit der Information angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Durchführen manueller Cloud-Updates von Plugins

So aktualisieren Sie Plugins manuell:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für Nessus-Plugin-Satz** angezeigt, der die letzte aktualisierte Version Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.
2. Klicken Sie auf die Schaltfläche **Jetzt aktualisieren**.
   Es wird ein Dialogfeld mit der Information angezeigt, dass das Update gestartet wurde. Wenn das Update abgeschlossen ist, wird im Feld **Plugin-Satz** die Nummer des aktuellen Plugin-Satzes angezeigt.

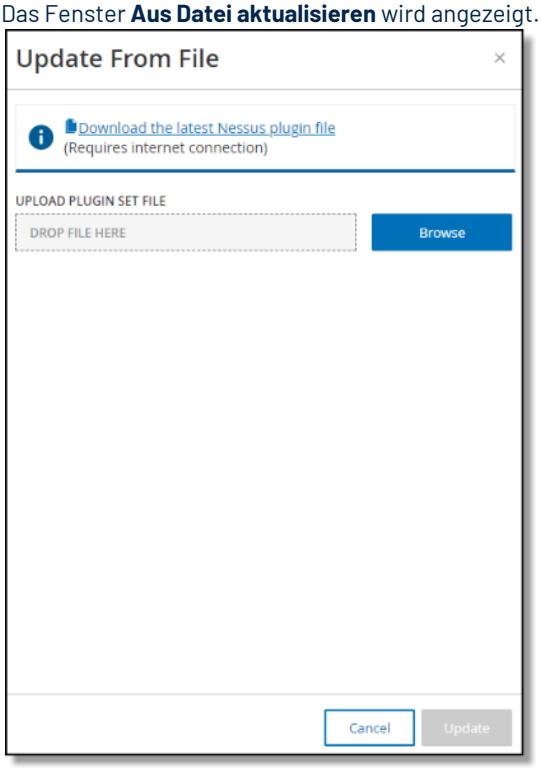
Lassen Sie das Browserfenster geöffnet und aktualisieren Sie die Seite nicht, während das Update des Plugin-Satzes durchgeführt wird.

Offline-Updates

Benutzer ohne Internetverbindung auf ihrem Tenable.ot-Gerät können Plugins manuell aktualisieren, indem sie den neuesten Plugin-Satz aus dem Tenable-Kundenportal herunterladen und die Datei hochladen.

So aktualisieren Sie Plugins offline:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für Nessus-Plugin-Satz** angezeigt, der die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.
2. Klicken Sie auf die Schaltfläche **Aus Datei aktualisieren**.
   Das Fenster **Aus Datei aktualisieren** wird angezeigt.



3. Sofern Sie dies noch nicht getan haben, klicken Sie auf den Link, um die neueste Plugin-Datei herunterzuladen, und kehren Sie dann zum Fenster **Aus Datei aktualisieren** zurück.

> Das Herunterladen der neuesten Plugin-Datei über den Link ist nur über eine Internetverbindung möglich, z. B. mit einem mit dem Internet verbundenen PC.

4. Klicken Sie auf **Durchsuchen** und navigieren Sie zu der Datei mit dem Plugin-Satz, die Sie aus dem Tenable.ot-Kundenportal heruntergeladen haben.
5. Klicken Sie auf **Aktualisieren**.

Updates des IDS-Engine-Regelsatzes

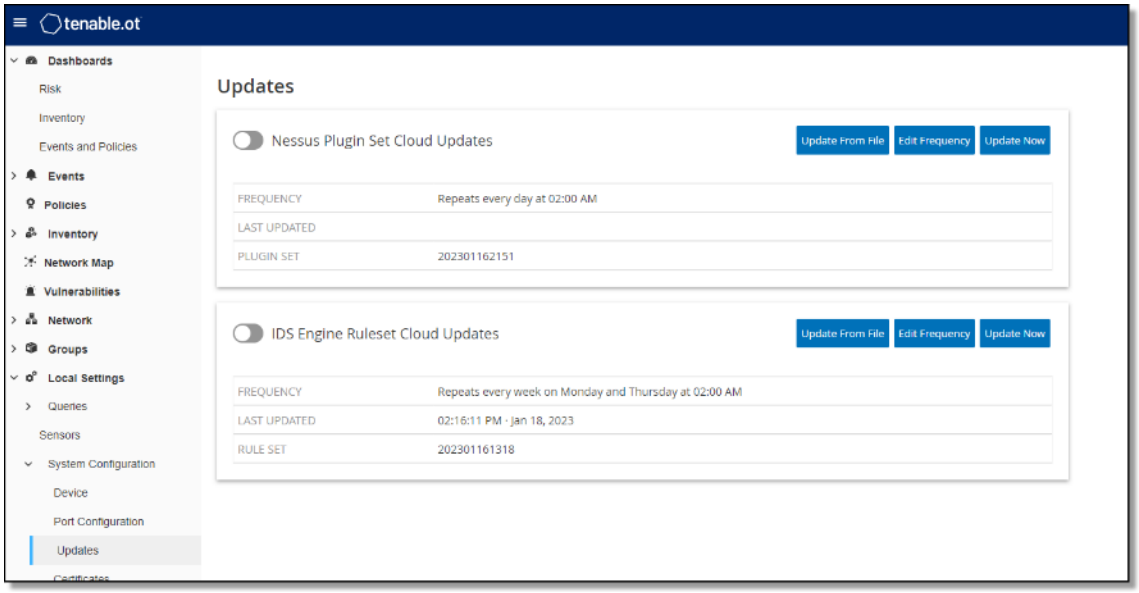
Cloud-Updates

Benutzer mit Internetverbindung können Ihren IDS-Engine-Regelsatz über die Cloud aktualisieren. Wenn automatische Updates aktiviert sind, wird der IDS-Engine-Regelsatz zu der vom Benutzer festgelegten Zeit und mit der festgelegten Frequenz aktualisiert (Standard: Wiederholung jede Woche am Montag und Donnerstag um 02:00 Uhr).

Festlegen automatischer Cloud-Updates des IDS-Engine-Regelsatzes

➡ So aktivieren Sie automatische Updates des IDS-Engine-Regelsatzes:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für IDS-Engine-Regelsatz** angezeigt, der die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.

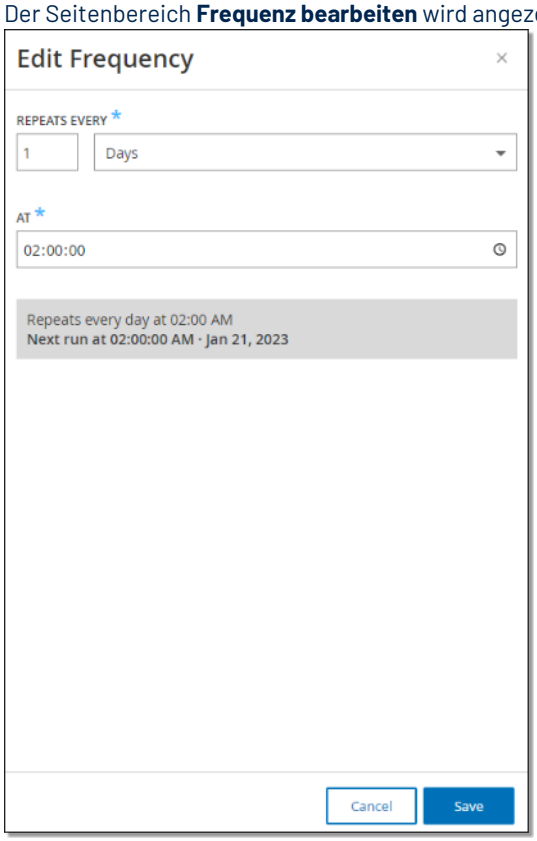


2. Wenn der Umschalter nicht auf EIN gestellt ist, klicken Sie darauf, um automatische Updates zu aktivieren.

➡ So bearbeiten Sie den Zeitplan für automatische Updates des IDS-Engine-Regelsatzes:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für IDS-Engine-Regelsatz** angezeigt, der die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.

2. Klicken Sie auf die Schaltfläche **Frequenz bearbeiten**.
   Der Seitenbereich **Frequenz bearbeiten** wird angezeigt.



3. Legen Sie unter **Wiederholungen alle** das Zeitintervall fest, in dem Sie den Regelsatz aktualisieren möchten, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) aus dem Dropdown-Menü wählen.
4. Bei Auswahl von **Wochen** wählen Sie die Wochentage aus, an denen Sie ein wöchentliches Update des Regelsatzes durchführen möchten.
5. Legen Sie unter **Um** die Tageszeit fest, zu der Sie den IDS-Engine-Regelsatz aktualisieren möchten (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.
   Klicken Sie auf **Speichern**.
   Es wird ein Dialogfeld mit der Information angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Durchführen manueller Cloud-Updates des IDS-Engine-Regelsatzes

➡ So aktualisieren Sie den IDS-Engine-Regelsatz manuell:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates**.
   Der Bildschirm **Updates** wird mit dem Bereich **Cloud-Updates für IDS-Engine-Regelsatz** angezeigt, der die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und den Update-Zeitplan enthält.
2. Klicken Sie auf die Schaltfläche **Jetzt aktualisieren**.
   Es wird ein Dialogfeld mit der Information angezeigt, dass das Update gestartet wurde. Wenn das Update abgeschlossen ist, wird im Feld **Regelsatz** die Nummer des aktuellen IDS-Engine-Regelsatzes angezeigt.

Offline-Updates

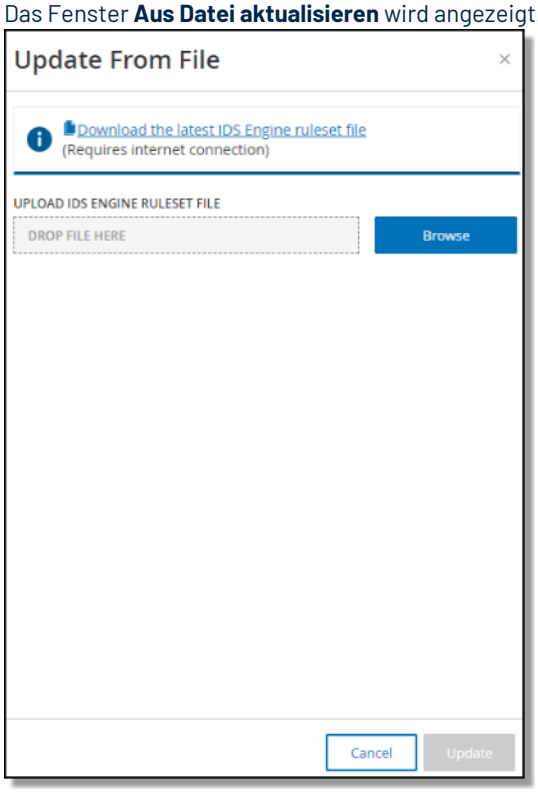
Benutzer ohne Internetverbindung auf ihrem Tenable.ot-Gerät können ihren IDS-Engine-Regelsatz manuell aktualisieren, indem sie den neuesten Regelsatz aus dem Tenable-Kundenportal herunterladen und die Datei hochladen.

➡ So aktualisieren Sie den IDS-Engine-Regelsatz offline:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Updates** > **Cloud-Updates für IDS-Engine-Regelsatz**.

Der Bildschirm **Updates** wird mit der Nummer Ihres Regelsatzes, dem Datum der letzten Aktualisierung und dem Update-Zeitplan angezeigt.

2. Klicken Sie auf die Schaltfläche **Aus Datei aktualisieren**.
   Das Fenster **Aus Datei aktualisieren** wird angezeigt.



3. Falls Sie dies noch nicht getan haben, klicken Sie auf den Link, um die neueste IDS-Engine-Regelsatzdatei herunterzuladen.

> Das Herunterladen der neuesten IDS-Engine-Regelsatzdatei über den Link ist nur über eine Internetverbindung möglich, z. B. über einen mit dem Internet verbundenen PC.

4. Klicken Sie auf **Durchsuchen** und navigieren Sie zu der IDS-Engine-Regelsatzdatei, die Sie aus dem Tenable.ot-Kundenportal heruntergeladen haben.
5. Klicken Sie auf **Aktualisieren**.

Zertifikat

Generieren eines HTTPS-Zertifikats

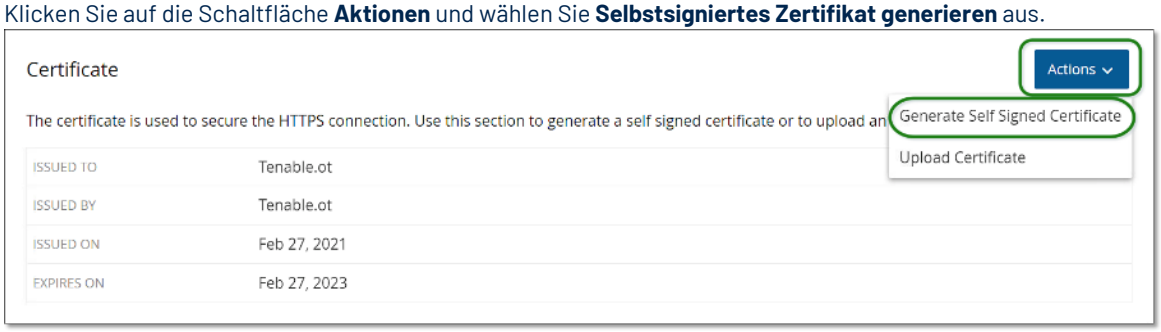
Das HTTPS-Zertifikat stellt sicher, dass das System eine sichere Verbindung zur Tenable.ot Appliance und zum Server verwendet. Das Erstzertifikat läuft nach zwei Jahren ab. Sie können jederzeit ein neues selbstsigniertes Zertifikat generieren. Das neue Zertifikat ist ein Jahr gültig.

> Wenn Sie ein neues Zertifikat generieren, wird das aktuelle Zertifikat überschrieben.

So generieren Sie ein selbstsigniertes Zertifikat:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Systemkonfiguration** > **Zertifikat**.

2. Klicken Sie auf die Schaltfläche **Aktionen** und wählen Sie **Selbstsigniertes Zertifikat generieren** aus.



Das Bestätigungsfenster zum Generieren eines Zertifikats wird angezeigt.

3. Klicken Sie auf **Generieren**.
Das selbstsignierte Zertifikat wird generiert und kann im Bildschirm **Lokale Einstellungen** > **Systemkonfiguration** > **Zertifikat** eingesehen werden.

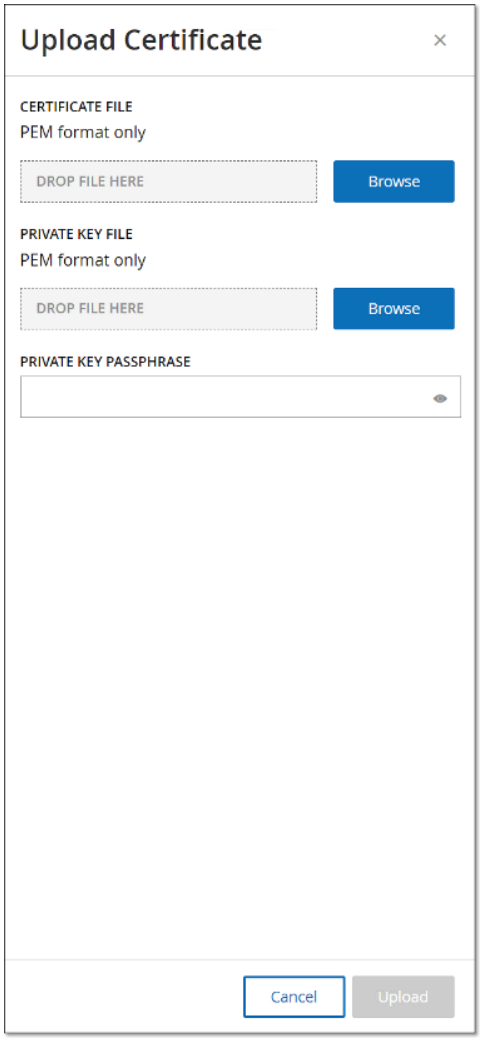
Hochladen von HTTPs-Zertifikaten

Benutzer können nicht nur ein selbstsigniertes HTTPS-Zertifikat generieren, sondern auch ihr eigenes HTTPS-Zertifikat über die Benutzeroberfläche hochladen („Lokale Einstellungen“ > „Systemkonfiguration“ > „Zertifikat“). Das Zertifikat dient zur Absicherung der HTTPS-Verbindungen zu anderen Geräten, einschließlich Ihres Browsers, zwischen dem ICP und dem IM usw.

So laden Sie ein HTTPs-Zertifikat hoch:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Systemkonfiguration** > **Zertifikat**.
2. Klicken Sie auf die Schaltfläche **Aktionen** und wählen Sie **Zertifikat hochladen** aus.

Der Seitenbereich **Zertifikat hochladen** wird angezeigt.



3. Klicken Sie unter **Zertifikatdatei** auf die Schaltfläche **Durchsuchen** und navigieren Sie zu der Zertifikatdatei, die Sie hochladen möchten.
4. Klicken Sie unter **Datei mit privatem Schlüssel** auf die Schaltfläche **Durchsuchen** und navigieren Sie zu der Datei des privaten Schlüssels, die Sie hochladen möchten.
5. Geben Sie die Passphrase des privaten Schlüssels in das Feld **Passphrase für privaten Schlüssel** ein.
6. Klicken Sie auf die Schaltfläche **Hochladen**, um die Dateien hochzuladen.
   Der Seitenbereich wird geschlossen.

Nachdem Sie das Zertifikat ersetzt haben, sollten Sie die Registerkarte des Browsers neu laden, um sich zu vergewissern, dass die Aktualisierung des HTTP-Zertifikats erfolgreich war. Wenn dies nicht der Fall ist, wird ein Warnhinweis angezeigt.

Lizenz

Es kann vorkommen, dass Sie Ihre Tenable.ot-Lizenz aktualisieren oder neu initialisieren müssen. Nachdem Sie Ihren Tenable Account Manager kontaktiert haben, müssen Sie eines der folgenden Verfahren ausführen, um Ihre Lizenz zu aktualisieren oder neu zu initialisieren.

Aktualisieren der Lizenz

Wenn Sie Ihre vorhandene Lizenz aktualisieren müssen (z. B. um Ihr Asset-Limit zu erhöhen, Ihren Lizenzzeitraum zu verlängern oder Ihren Lizenztyp zu ändern), gehen Sie wie folgt vor.

Voraussetzungen

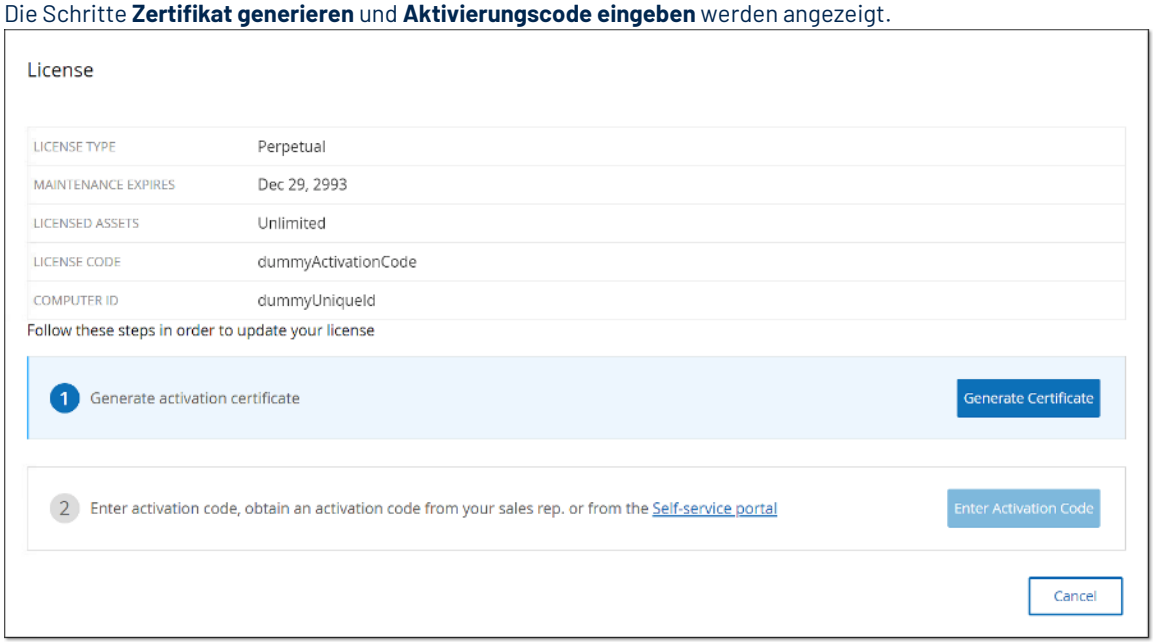
- Ihr Tenable Account Manager muss Ihre Lizenzinformationen bereits in seinem System aktualisiert haben, bevor Sie die neue Lizenz registrieren können.
- Sie benötigen Zugang zum Internet. Wenn Ihr Tenable.ot-Gerät nicht mit dem Internet verbunden ist, können Sie die Lizenz von jedem PC aus registrieren.

Registrieren einer neuen Lizenz

So registrieren Sie Ihre Lizenz:

1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Lizenz**.
   Der Bildschirm **Lizenz** wird angezeigt.

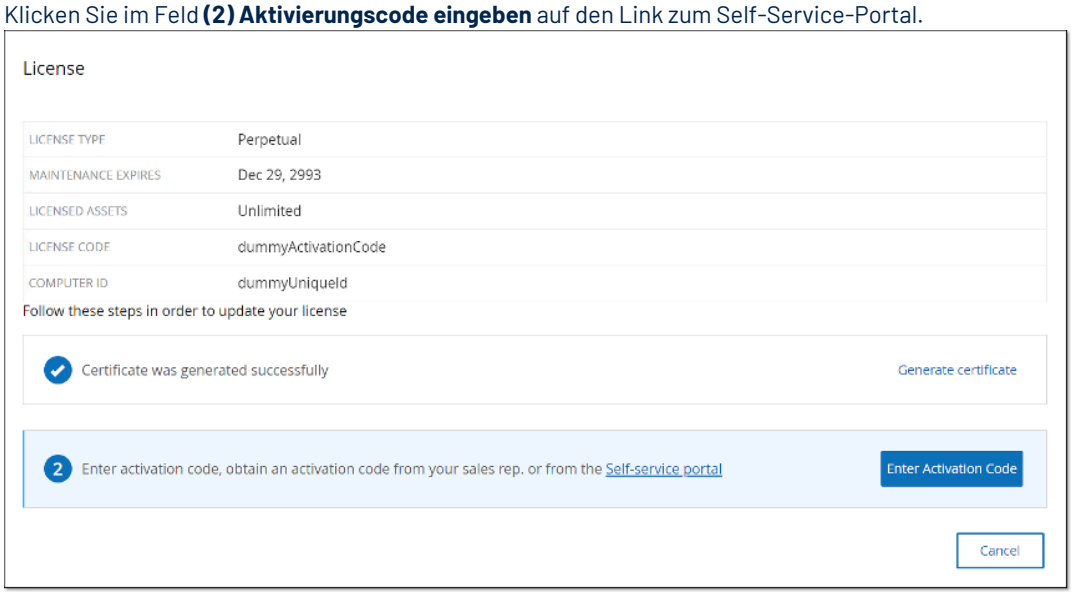
2. Klicken Sie auf die Schaltfläche **Aktionen** und wählen Sie **Lizenz aktualisieren** aus.
Die Schritte **Zertifikat generieren** und **Aktivierungscode eingeben** werden angezeigt.



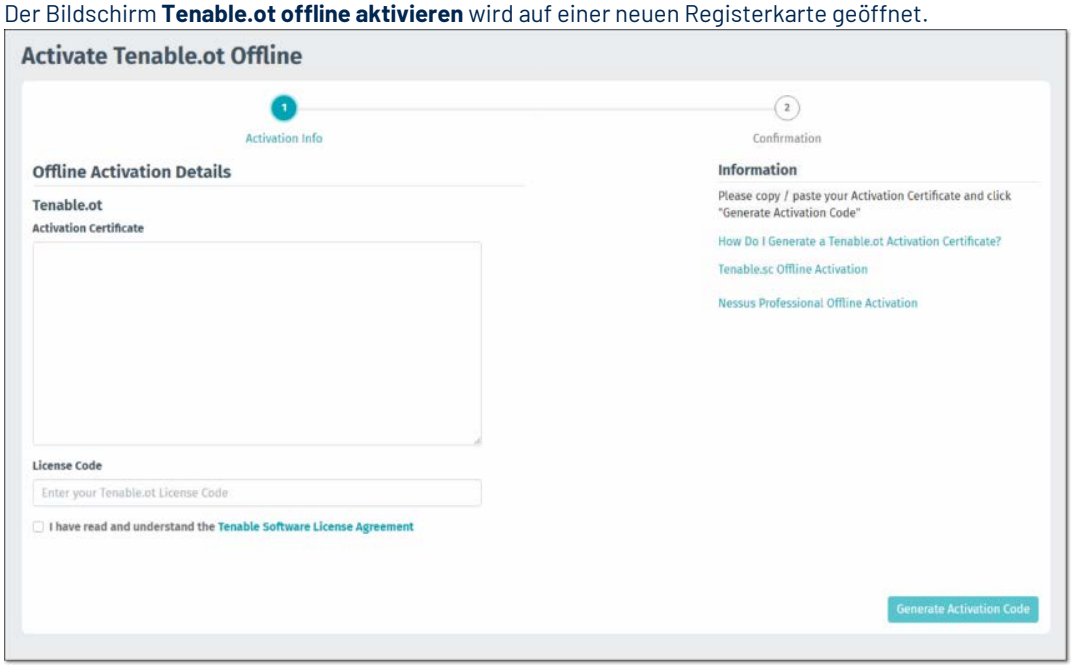
3. Klicken Sie im Feld **(1) Aktivierungszertifikat generieren** auf die Schaltfläche **Zertifikat generieren**.
Der Seitenbereich **Zertifikat generieren** wird mit dem Aktivierungszertifikat angezeigt.

4. Klicken Sie auf die Schaltfläche **Text in die Zwischenablage kopieren** und dann auf **Fertig**.
Der Seitenbereich wird geschlossen.

5. Klicken Sie im Feld **(2) Aktivierungscode eingeben** auf den Link zum Self-Service-Portal.



Der Bildschirm **Tenable.ot offline aktivieren** wird auf einer neuen Registerkarte geöffnet.



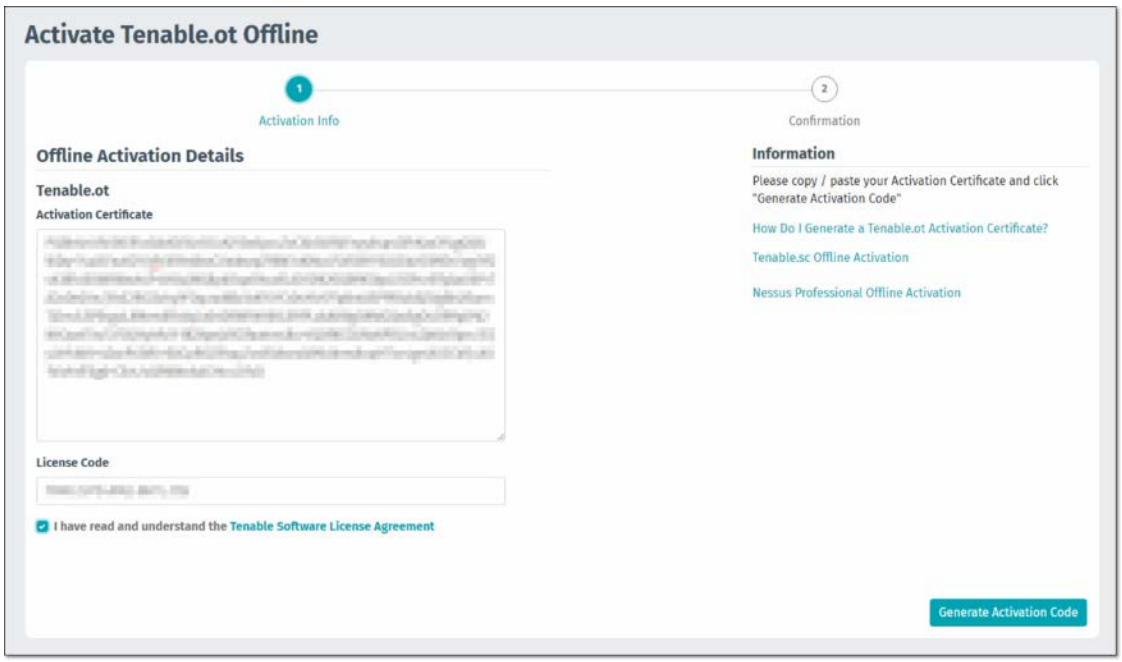
Sie müssen den Bildschirm „Tenable.ot offline aktivieren“ von einem mit dem Internet verbundenen Gerät über die folgende URL aufrufen: https://provisioning.tenable.com/activate/offline/tenable-ot.

Wenn Sie derzeit nicht bei tenable.com eingeloggt sind, müssen Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort einloggen. Sie müssen das E-Mail-Konto verwenden, über das Sie Ihren Lizenzcode erhalten haben.

Wenn Sie keine Zugangsdaten haben, können Sie entweder auf **Passwort vergessen** klicken (und den Anweisungen folgen) oder sich an Ihren Tenable Account Manager wenden.

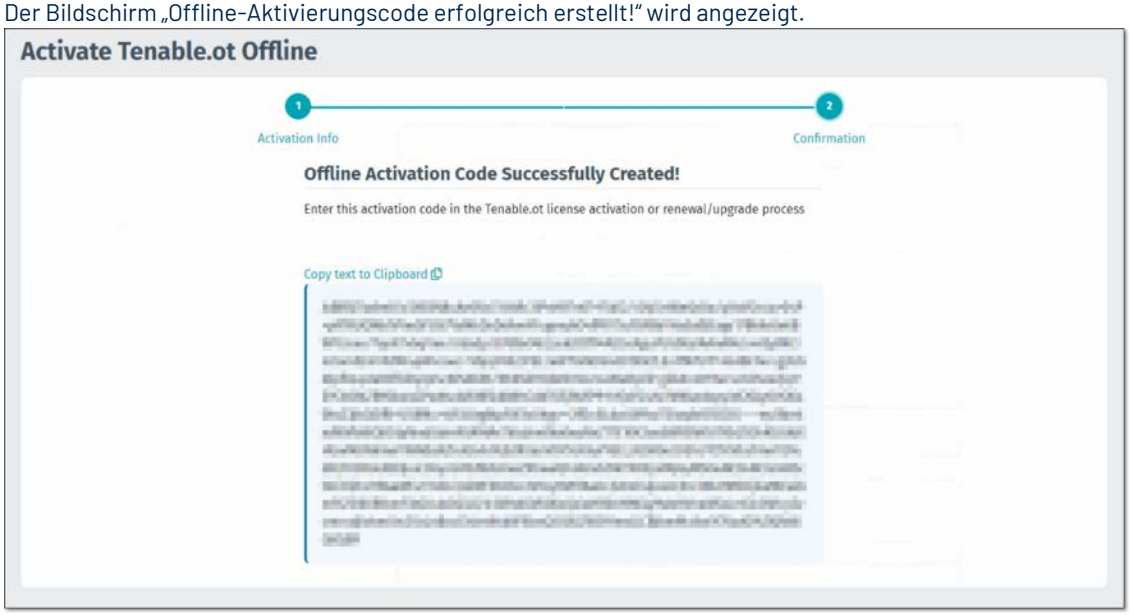
6. Geben Sie im Feld **Aktivierungszertifikat** das Aktivierungszertifikat ein.
7. Geben Sie im Feld **Lizenzcode** Ihren 20-stelligen **Lizenzcode** ein (kann im Bildschirm **Lizenz** kopiert und hier eingefügt werden).

8. Aktivieren Sie das Kontrollkästchen **Ich habe die Tenable-Softwarelizenzvereinbarung gelesen und verstanden**.

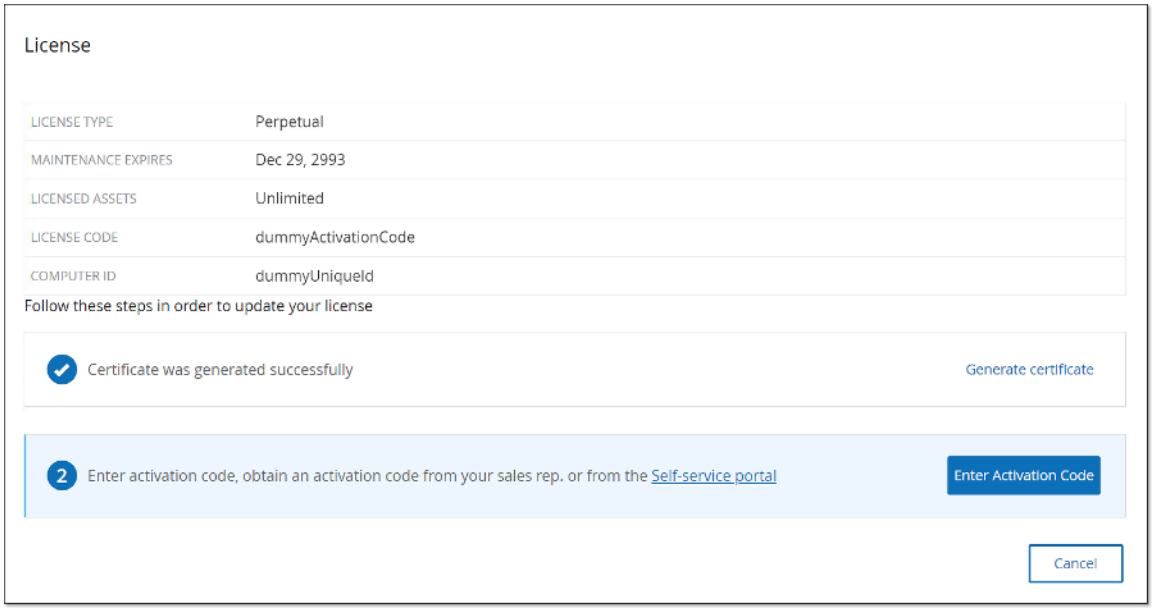


Um die Lizenzvereinbarung anzuzeigen, klicken Sie auf den Link **Tenable-Softwarelizenzvereinbarung**.

9. Klicken Sie auf die Schaltfläche **Aktivierungscode generieren** (Generate Activation Code).
Der Bildschirm „Offline-Aktivierungscode erfolgreich erstellt!“ wird angezeigt.

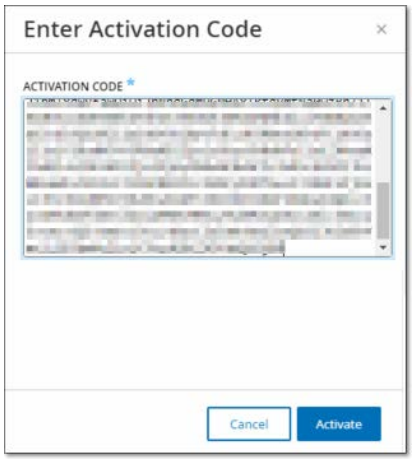


10. Klicken Sie auf **Text in die Zwischenablage kopieren**.
11. Navigieren Sie zurück zur Registerkarte **Lizenz** und klicken Sie auf die Schaltfläche **Aktivierungscode eingeben**.



Der Seitenbereich **Aktivierungscode eingeben** wird angezeigt.

12. Fügen Sie Ihren Aktivierungscode in das Feld **Aktivierungscode** ein und klicken Sie auf die Schaltfläche **Aktivieren**.



Der Seitenbereich wird geschlossen und die Lizenz wird aktualisiert.

Neuinitialisierung der Lizenz

Durch die Neuinitialisierung Ihrer Lizenz wird Ihre aktuelle Lizenz aus dem System entfernt und eine neue Lizenz aktiviert, ähnlich wie bei der Lizenzaktivierung während des Systemstarts. Wenn Sie Ihre Lizenz neu initialisieren müssen (d. h. eine neue Lizenz wurde für Sie ausgestellt), verwenden Sie das folgende Verfahren.

Voraussetzungen

- Ihr Tenable Account Manager muss Ihre neue Lizenz bereits in seinem System ausgestellt und Ihnen einen Lizenzcode (20 Buchstaben/Ziffern) bereitgestellt haben.
- Sie benötigen Zugang zum Internet. Wenn Ihr Tenable.ot-Gerät nicht mit dem Internet verbunden ist, können Sie die Lizenz von jedem PC aus registrieren.

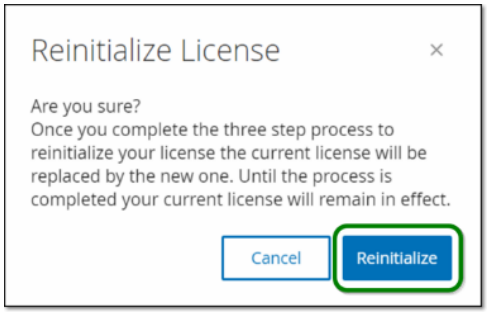
Erneutes Initialisieren einer Lizenz

So initialisieren Sie Ihre Lizenz neu:

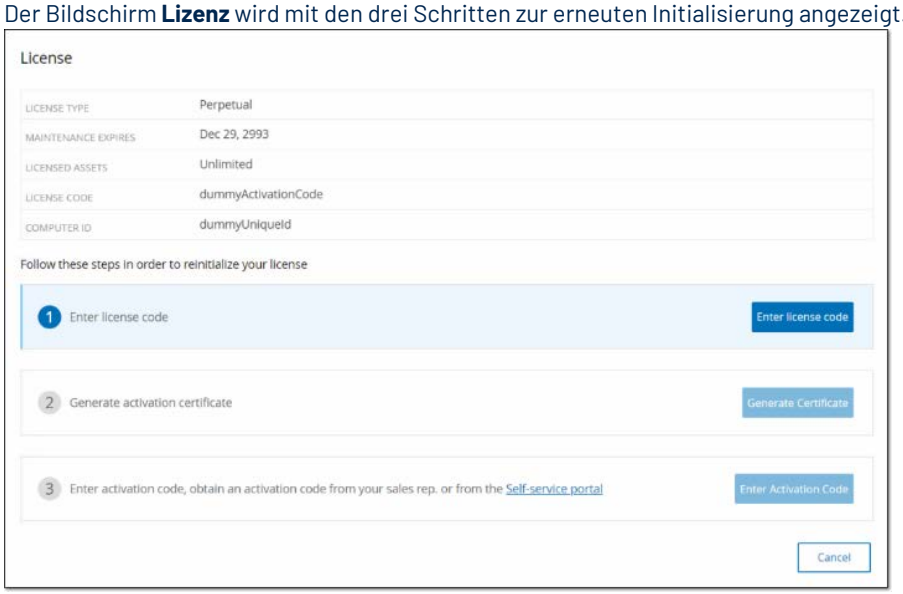
1. Gehen Sie unter **Lokale Einstellungen** zu **Systemkonfiguration** > **Lizenz**.

Klicken Sie auf die Schaltfläche **Aktionen** und wählen Sie **Lizenz erneut initialisieren** aus.
Ein Bestätigungsfenster wird angezeigt.

2. Klicken Sie auf **Neu initialisieren**.



Der Bildschirm **Lizenz** wird mit den drei Schritten zur erneuten Initialisierung angezeigt.



3. Befolgen Sie die Schritte zum Systemstart, um Ihre Lizenz zu aktivieren. Siehe **Aktivieren Ihrer Lizenz**.
Nach Eingabe Ihres Aktivierungscodes wird Ihre aktuelle Lizenz durch Ihre neue Lizenz ersetzt.

Lizenzberechnung

Lizenzen für Tenable-Konten werden basierend auf der Anzahl eindeutiger IP-Adressen im System berechnet. Jede IP erfordert eine separate Lizenz. Selbst wenn also mehrere Geräte dieselben IP-Adressen nutzen (z. B. mehrere Geräte, die mit derselben Backplane verbunden sind und dieselben drei IP-Adressen verwenden), basieren die Lizenzen immer noch auf der Anzahl von IP-Adressen, in diesem Fall 3 Lizenzen, unabhängig von der Anzahl der Geräte.

Umgebungskonfiguration

Asset-Einstellungen

Manuelles Hinzufügen von Assets

Um Ihr Inventar besser verfolgen zu können, sollten Sie eventuell einige zusätzliche Assets anzeigen, die Sie besitzen, auch wenn diese Assets noch nicht von Tenable.ot erkannt wurden. Sie können diese Assets manuell zu Ihrem Inventar hinzufügen, indem Sie eine CSV-Datei herunterladen und bearbeiten und die Datei dann in das System hochladen.

Benutzer können nur Assets hochladen, deren IP-Adressen noch nicht von einem vorhandenen Asset im System verwendet werden. Falls das System ein Asset erkennt, das mit derselben IP über das Netzwerk kommuniziert, verwendet es die über das erkannte Asset abgerufenen Informationen und überschreibt die zuvor hochgeladenen Informationen. Das System behandelt das Asset als reguläres Asset, sobald es erkennt, dass das Asset im Netzwerk kommuniziert.

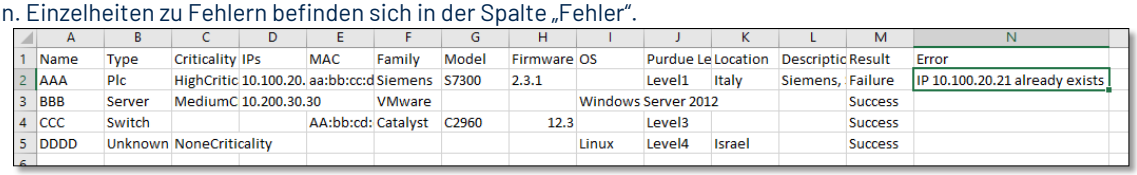
Die IP-Adressen hochgeladener Assets werden als Teil der Systemlizenzierung gezählt.

Hochgeladene Assets zeigen einen Risikowert von 0 an, bis sie vom System erkannt werden.

Für manuell hinzugefügte Assets werden keine Ereignisse erkannt, bis Tenable.ot erkennt, dass sie über das Netzwerk kommunizieren.

So fügen Sie Assets manuell hinzu:

1. Gehen Sie unter **Lokale Einstellungen** zu **Umgebungskonfiguration** > **Asset-Einstellungen**.
   Der Bildschirm **Asset-Einstellungen** wird angezeigt.
2. Klicken Sie unter **Assets manuell hinzufügen** auf die Schaltfläche **Aktionen** und wählen Sie **CSV-Vorlage herunterladen** aus.
3. Das Vorlagendokument „tot_Assets“ wird heruntergeladen.
4. Öffnen Sie das Vorlagendokument „tot_Assets“.
5. Bearbeiten Sie die Vorlage „tot_Assets“ genau gemäß den Anweisungen in der Datei und behalten Sie nur die Spaltenüberschriften (Name, Typ usw.) und die von Ihnen eingegebenen Werte bei.
6. Speichern Sie die bearbeitete Datei.
7. Kehren Sie zum Bildschirm **Asset-Einstellungen** zurück.
8. Klicken Sie auf die Schaltfläche **Aktionen**, wählen Sie **CSV-Datei hochladen** aus, navigieren Sie zu der gewünschten CSV-Datei und öffnen Sie sie, um sie hochzuladen.
9. Klicken Sie unter **Assets manuell hinzufügen** auf **Bericht herunterladen**.
   Eine CSV-Datei mit dem Bericht wird angezeigt und zeigt Erfolge und Fehlschläge in der Spalte „Ergebnis“ an. Einzelheiten zu Fehlern befinden sich in der Spalte „Fehler“.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Name	Type	Criticality	IPs	MAC	Family	Model	Firmware	OS	Purdue Le	Location	Descriptic	Result	Error
2	AAA	Plc	HighCritic	10.100.20.	aa:bb:cc:d	Siemens	S7300	2.3.1		Level1	Italy	Siemens,	Failure	IP 10.100.20.21 already exists
3	BBB	Server	MediumC	10.200.30.30		VMware			Windows Server 2012				Success	
4	CCC	Switch			AA:bb:cd:	Catalyst	C2960	12.3		Level3			Success	
5	DDDD	Unknown	NoneCriticality						Linux	Level4	Israel		Success	

Ereigniscluster

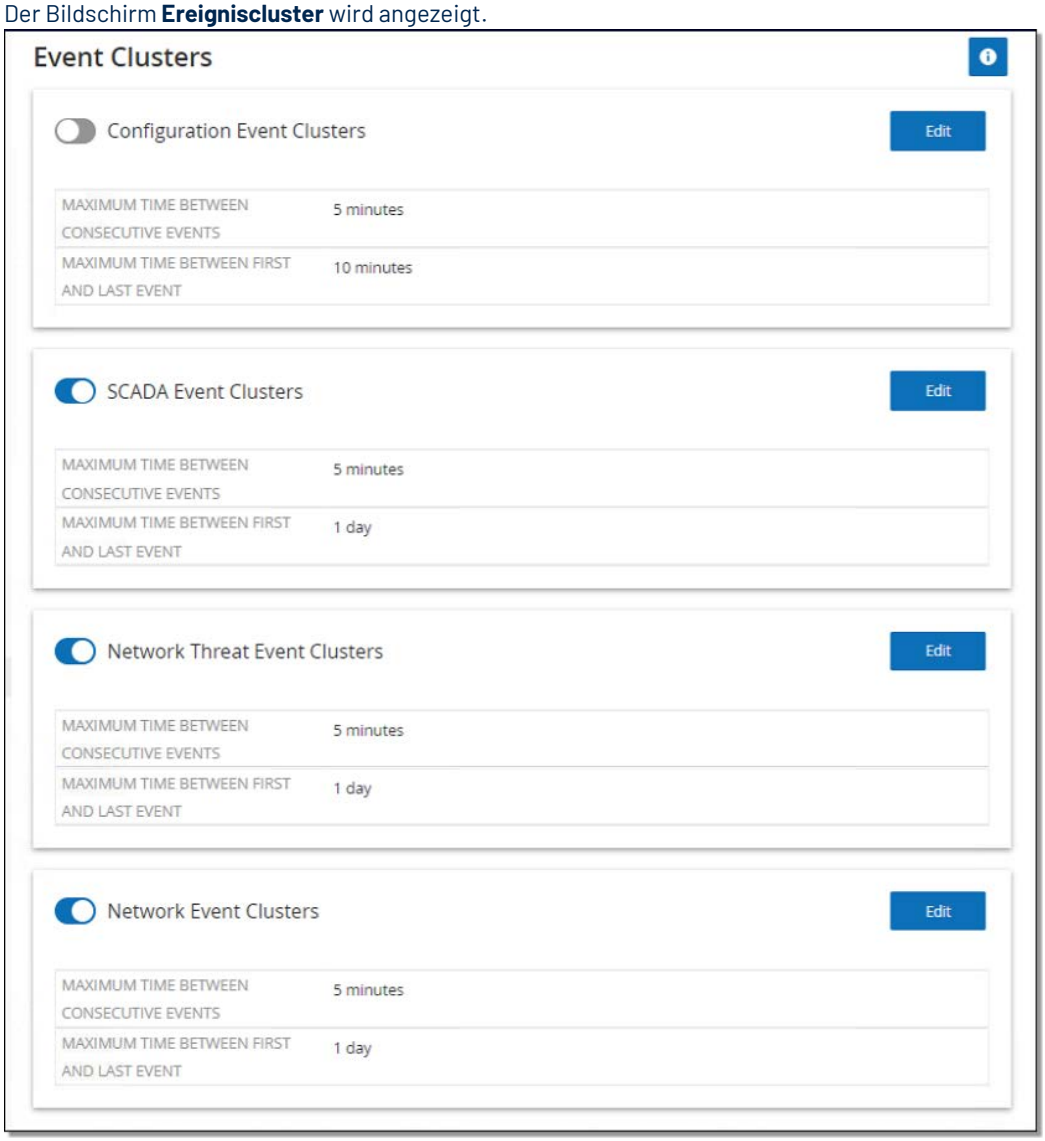
Um die Überwachung von Ereignissen zu vereinfachen, werden mehrere Ereignisse mit denselben Merkmalen in einem einzigen Cluster zusammengefasst. Das Clustering basiert auf dem Ereignistyp (d. h. Nutzung derselben Richtlinie), Quell- und Ziel-Assets usw.

Damit Ereignisse geclustert werden können, müssen sie innerhalb der folgenden konfigurierten Zeitintervalle generiert werden:

- **Maximale Zeit zwischen aufeinanderfolgenden Ereignissen** – Legt das maximale Zeitintervall zwischen Ereignissen fest. Wenn diese Zeit verstrichen ist, werden die aufeinanderfolgenden Ereignisse nicht geclustert.
- **Maximale Zeit zwischen erstem und letztem Ereignis** – Legt das maximale Zeitintervall für alle Ereignisse fest, die als Cluster angezeigt werden sollen. Ein Ereignis, das nach diesem Zeitintervall generiert wird, wird nicht in den Cluster aufgenommen.

So aktivieren Sie Clustering:

1. Gehen Sie unter **Lokale Einstellungen** zu **Umgebungskonfiguration** > **Ereigniscluster**.
   Der Bildschirm **Ereigniscluster** wird angezeigt.



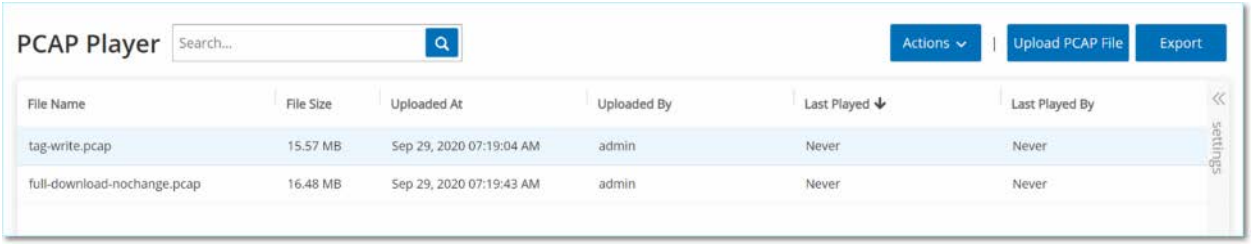
2. Klicken Sie auf den Umschalter, um die gewünschten Kategorien für das Clustering zu aktivieren.
3. Um die Zeitintervalle für eine Kategorie zu konfigurieren, klicken Sie auf die Schaltfläche **Bearbeiten**.
   Das Fenster **Konfiguration bearbeiten** wird angezeigt.

4. Geben Sie den gewünschten Zahlenwert in das Zahlenfeld ein und passen Sie die Zeiteinheit über die Dropdown-Liste an.

> Weitere Informationen zu Clustering und Zeitintervallen erhalten Sie über die Schaltfläche .

5. Klicken Sie auf **Speichern**.

PCAP-Player



Tenable.ot ermöglicht es Ihnen, eine PCAP-Datei mit aufgezeichneter Netzwerkaktivität hochzuladen und auf Tenable.ot „abzuspielen“. Wenn Sie eine PCAP-Datei „abspielen“, überwacht Tenable.ot den Netzwerk-Traffic und zeichnet alle Informationen über erkannte Assets, Netzwerkaktivitäten und Schwachstellen so auf, als ob der Traffic in Ihrem Netzwerk stattgefunden hätte. Diese Funktion kann zu Simulationszwecken oder zur Analyse von Traffic verwendet werden, der außerhalb des Netzwerks stattfindet, das von Ihrer Tenable.ot-Bereitstellung überwacht wird (z. B. Remote-Anlagen).

> Die folgenden Dateitypen werden für diese Funktion unterstützt: .pcap, .pcapng, .pcap.gz, .pcapng.gz. Sie können Dateien verwenden, die von einer Instanz von Tenable.ot oder anderen Netzwerküberwachungstools aufgezeichnet wurden.

Hochladen einer PCAP-Datei

So laden Sie eine PCAP-Datei hoch:

1. Gehen Sie unter **Lokale Einstellungen** zu **Umgebungskonfiguration** > **PCAP-Player**.
2. Klicken Sie auf **PCAP-Datei hochladen**.
   Der Datei-Explorer wird geöffnet.
3. Wählen Sie die gewünschte PCAP-Aufzeichnung aus.
4. Klicken Sie auf **Öffnen**.
   Die PCAP-Datei wird in das System hochgeladen.

Abspielen einer PCAP-Datei

So spielen Sie eine PCPAP-Datei ab:

1. Gehen Sie unter **Lokale Einstellungen** zu **Umgebungskonfiguration** > **PCAP-Player**.
2. Wählen Sie die PCAP-Aufzeichnung aus, die Sie abspielen möchten.
3. Klicken Sie auf **Aktionen** > **Abspielen**.
4. Der Assistent **PCAP abspielen** wird angezeigt.
5. Wählen Sie im Feld **Abspielgeschwindigkeit** in der Dropdown-Liste die Geschwindigkeit aus, mit der das System die Datei abspielen soll. Verfügbare Optionen: *1X*, *2X*, *4X*, *8X* oder *16X*.

> Durch das Abspielen einer PCAP-Datei werden Daten in das System eingebracht. Sobald dieser Vorgang ausgeführt wird, kann er nicht mehr rückgängig gemacht oder angehalten werden.

6. Klicken Sie auf **Abspielen**.

Die PCAP-Datei wird im System „abgespielt“. Alle Netzwerkaktivitäten in der PCAP-Datei werden im System registriert und vom System identifizierte Assets werden dem Asset-Inventar hinzugefügt.

Sie können keine andere PCAP-Datei abspielen, während bereits eine Datei abgespielt wird.

Benutzer und Rollen

Der Zugriff auf die Tenable.ot-Konsole (UI) wird über Benutzerkonten gesteuert, in denen die für den jeweiligen Benutzer verfügbaren Berechtigungen festgelegt sind. Die Berechtigungen des Benutzers werden durch die Benutzergruppe(n) bestimmt, der bzw. denen er zugeordnet ist. Jeder Benutzergruppe wird eine Rolle zugewiesen, die definiert, welche Berechtigungen ihren Mitgliedern zur Verfügung stehen. Wenn also beispielsweise die Benutzergruppe *Site-Operatoren* die Rolle *Site-Operator* hat, dann verfügen alle Benutzer, die dieser Gruppe zugewiesen sind, über die mit der Rolle *Site-Operator* verknüpften Berechtigungen.

Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe *Administratoren* > Rolle *Administrator*, Benutzergruppe *Site-Operatoren* > Rolle *Site-Operator* usw. Sie können außerdem benutzerdefinierte Benutzergruppen erstellen und ihre Rollen festlegen.

Es gibt drei Methoden, um Benutzer im System zu erstellen:

- **Lokale Benutzer hinzufügen** – Erstellen Sie Benutzerkonten, um den Zugriff einzelner Benutzer auf das System zu autorisieren. Weisen Sie Benutzer Benutzergruppen zu, die ihre Rollen definieren.
- **Authentifizierungsserver** – Verwenden Sie die Authentifizierungsserver Ihrer Organisation (z. B. Active Directory, LDAP), um den Zugriff von Benutzern auf das System zu autorisieren. Sie können Tenable.ot-Rollen auf der Grundlage Ihrer vorhandenen Gruppen in Active Directory zuweisen.
- **SAML** – Richten Sie eine Integration mit Ihrem Identitätsanbieter (z. B. Azure Active Directory) ein und weisen Sie Ihrer Tenable.ot-Anwendung Benutzer zu.

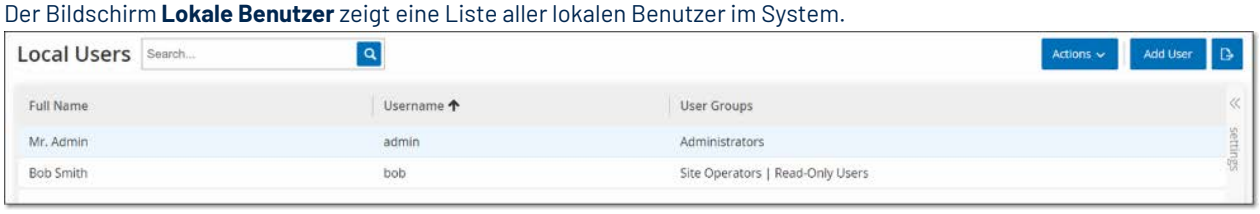
Lokale Benutzer

Ein Administratorbenutzer kann neue Benutzerkonten erstellen und vorhandene Konten bearbeiten. Jeder Benutzer wird einer oder mehreren Benutzergruppen zugewiesen, die die dem Benutzer zugewiesene(n) Rolle(n) bestimmen.

Benutzer können Benutzergruppen entweder während der Erstellung/Bearbeitung des Benutzerkontos oder der Benutzergruppe hinzugefügt werden.

Anzeigen lokaler Benutzer

Der Bildschirm **Lokale Benutzer** zeigt eine Liste aller lokalen Benutzer im System.



Die Informationen in diesem Bildschirm werden in der folgenden Tabelle beschrieben:

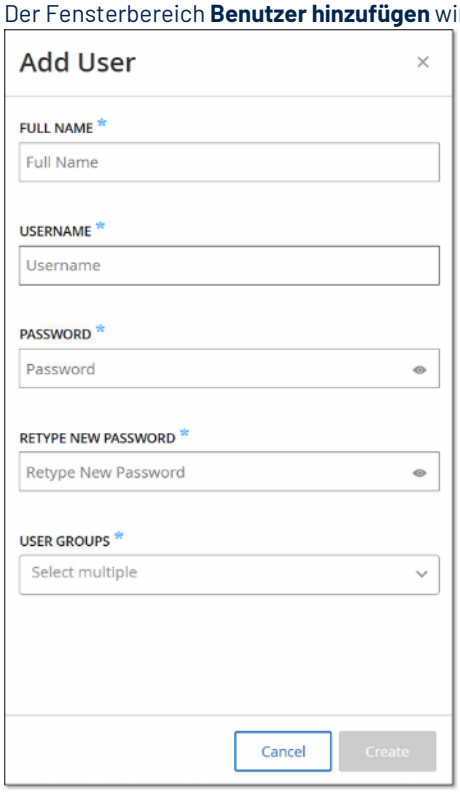
Parameter	Beschreibung
Vollständiger Name	Der vollständige Name des Benutzers.
Benutzername	Der Benutzername des Benutzers, der zum Einloggen verwendet wird.
Benutzergruppen	Die Benutzergruppe(n), der bzw. denen der Benutzer zugewiesen ist.

Hinzufügen lokaler Benutzer

Sie können Benutzerkonten erstellen, um den Zugriff einzelne Benutzer auf das System zu autorisieren. Jeder Benutzer muss einer oder mehreren Benutzergruppen zugewiesen werden.

So erstellen Sie ein Benutzerkonto:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Lokale Benutzer**.
2. Klicken Sie auf die Schaltfläche **Benutzer hinzufügen**.
   Der Fensterbereich **Benutzer hinzufügen** wird angezeigt.



3. Geben Sie im Feld **Vollständiger Name** den Vor- und Nachnamen ein.

> Der eingegebene Name wird in der Kopfleiste angezeigt, wenn der Benutzer eingeloggt ist.

4. Geben Sie im Feld **Benutzername** einen Benutzernamen ein, der für das Einloggen beim System verwendet werden soll.
5. Geben Sie im Feld **Passwort** ein Passwort ein.
6. Geben Sie im Feld **Passwort erneut eingeben** das gleiche Passwort erneut ein.

> Dies ist das Passwort, das der Benutzer für den ersten Login verwendet. Der Benutzer kann das Passwort im Bildschirm **Einstellungen** ändern, nachdem er sich beim System eingeloggt hat.

7. Klicken Sie auf das Feld **Benutzergruppen** und aktivieren Sie das Kontrollkästchen für jede Benutzergruppe, der Sie diesen Benutzer zuweisen möchten.

> Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe *Administratoren* > Rolle *Administrator*, Benutzergruppe *Site-Operatoren* > Rolle *Site-Operator* usw. Eine Erläuterung der verfügbaren Rollen finden Sie unter **BENUTZERROLLEN**.

8. Klicken Sie auf **Erstellen**.
   Das neue Benutzerkonto wird im System erstellt und der Liste der Benutzer hinzugefügt, die auf der Registerkarte **Lokale Benutzer** angezeigt werden.

Zusätzliche Aktionen für Benutzerkonten

Bearbeiten eines Benutzerkontos

Sie können einen Benutzer weiteren Benutzergruppen zuweisen oder den Benutzer aus einer Gruppe entfernen.

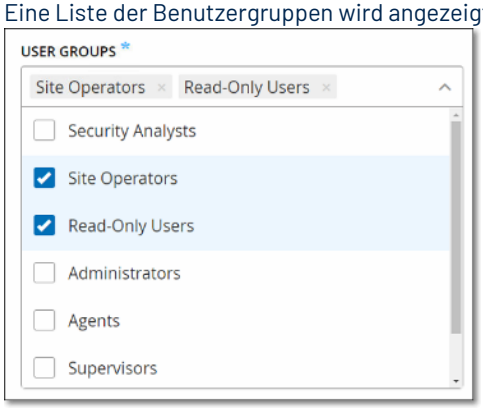
So ändern Sie die Benutzergruppen eines Benutzers:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Lokale Benutzer**.
   Der Bildschirm **Lokale Benutzer** wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer und wählen Sie **Benutzer bearbeiten** aus dem Kontextmenü.

> Alternativ können Sie einen Benutzer auswählen und dann auf die Schaltfläche **Aktionen** > **Benutzer bearbeiten** klicken.

3. Der Fensterbereich **Benutzer bearbeiten** wird angezeigt. Er zeigt die Benutzergruppen, denen der Benutzer zugewiesen ist.

4. Klicken Sie auf das Feld **Benutzergruppen**.
   Eine Liste der Benutzergruppen wird angezeigt.



5. Wählen Sie die gewünschten Benutzergruppen aus bzw. heben Sie die Auswahl von Benutzergruppen auf.
6. Klicken Sie auf **Speichern**.

Ändern des Passworts eines Benutzers

> Mit dem unten beschriebenen Verfahren kann ein Administratorbenutzer das Passwort für ein beliebiges Konto im System ändern. Alle Benutzer können ihr eigenes Passwort ändern, indem sie zu **Lokale Einstellungen** > **Benutzer** gehen.

So ändern Sie ein Benutzerpasswort:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Lokale Benutzer**.
   Der Bildschirm **Lokale Benutzer** wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer und wählen Sie **Passwort zurücksetzen** aus dem Kontextmenü.

Alternativ können Sie einen Benutzer auswählen und dann auf die Schaltfläche **Aktionen** > **Passwort zurücksetzen** klicken.

Das Fenster **Passwort zurücksetzen** wird angezeigt.

3. Geben Sie im Feld **Neues Passwort** ein neues Passwort ein.
4. Geben Sie im Feld **Neues Passwort erneut eingeben** das neue Passwort erneut ein.
5. Klicken Sie auf **Zurücksetzen**.
   Das neue Passwort wird auf das angegebene Benutzerkonto angewendet.

Löschen lokaler Benutzer

So löschen Sie ein Benutzerkonto:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Lokale Benutzer**.
   Der Bildschirm **Lokale Benutzer** wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer und wählen Sie **Benutzer löschen** aus dem Kontextmenü.

Alternativ können Sie einen Benutzer auswählen und dann auf die Schaltfläche **Aktionen** > **Benutzer löschen** klicken.

Ein Bestätigungsfenster wird angezeigt.

3. Klicken Sie auf **Löschen**.
   Das Benutzerkonto wird aus dem System gelöscht.

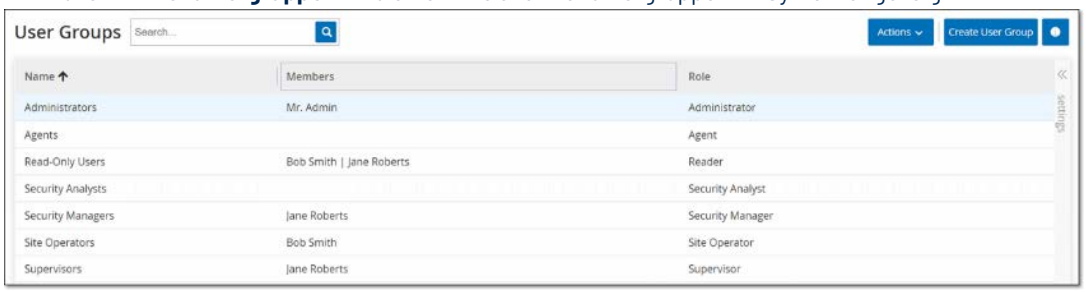
Benutzergruppen

Ein Administratorbenutzer kann neue Benutzergruppen erstellen und vorhandene Gruppen bearbeiten. Jeder Benutzer wird einer oder mehreren Benutzergruppen zugewiesen, die die dem Benutzer zugewiesene(n) Rolle(n) bestimmen.

Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe *Administratoren* > Rolle *Administrator*, Benutzergruppe *Site-Operatoren* > Rolle *Site-Operator* usw. Eine Erläuterung der verfügbaren Rollen finden Sie unter **Benutzerrollen**.

Anzeigen von Benutzergruppen

Im Bildschirm **Benutzergruppen** wird eine Liste aller Benutzergruppen im System angezeigt.



Die Informationen in diesem Bildschirm werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Name	Der Name der Benutzergruppe.
Mitglieder	Eine Liste aller Mitglieder, die der Gruppe zugewiesen sind.
Rolle	Die dieser Gruppe zugewiesene Rolle. Eine Erläuterung der den einzelnen Rollen zugeordneten Berechtigungen finden Sie in der **Tabelle der Benutzerrollen**.

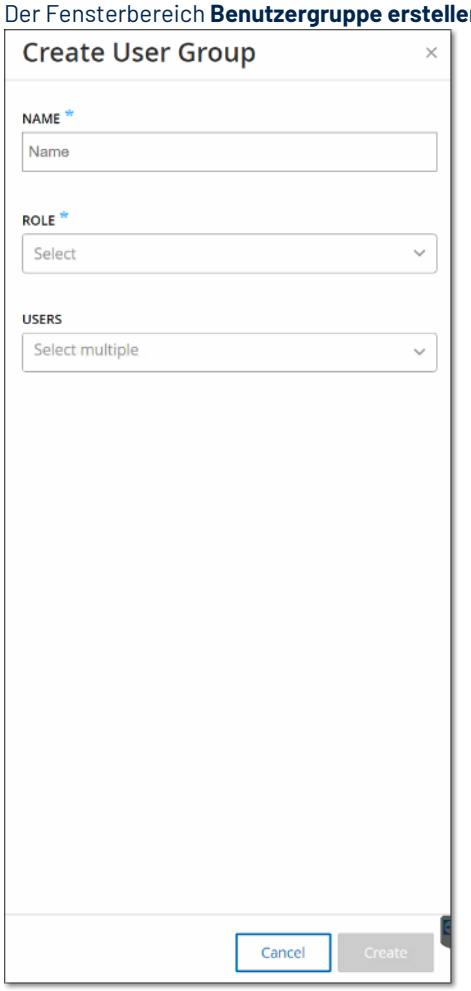
Hinzufügen von Benutzergruppen

Sie können neue Benutzergruppen erstellen und dieser Gruppe Benutzer zuweisen.

➡ So erstellen Sie ein Benutzerkonto:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Benutzergruppen**.
   Der Bildschirm **Benutzergruppen** wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Benutzergruppe erstellen**.
   Der Fensterbereich **Benutzergruppe erstellen** wird angezeigt.



3. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
4. Wählen Sie im Feld **Rolle** aus der Dropdown-Liste die Rolle aus, die Sie dieser Gruppe zuweisen möchten.
5. Wählen Sie im Feld **Benutzer** aus der Dropdown-Liste einen oder mehrere Benutzer aus, die Sie dieser Gruppe zuweisen möchten.
6. Klicken Sie auf **Erstellen**.
   Die neue Benutzergruppe wird im System erstellt und der Liste der Gruppen hinzugefügt, die im Bildschirm **Benutzergruppen** angezeigt werden.

Zusätzliche Aktionen für Benutzergruppen

Bearbeiten von Benutzergruppen

Sie können die Einstellungen bearbeiten und Mitglieder zu einer vorhandenen Benutzergruppe hinzufügen oder daraus entfernen, indem Sie die Gruppe bearbeiten.

Alternativ können Sie einen Benutzer auswählen und dann auf die Schaltfläche **Aktionen** > **Benutzer löschen** klicken.

So bearbeiten Sie eine Benutzergruppe:

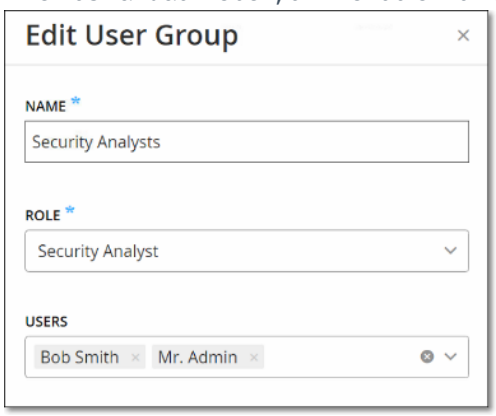
1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Benutzergruppen**.
   Der Bildschirm **Benutzergruppen** wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die gewünschte Benutzergruppe und wählen Sie **Benutzergruppe bearbeiten** im Kontextmenü aus.

Alternativ können Sie eine Benutzergruppe auswählen und dann auf die Schaltfläche **Aktionen** > **Benutzergruppe bearbeiten** klicken.

3. Der Fensterbereich **Benutzergruppen bearbeiten** wird angezeigt und zeigt die Einstellungen der Gruppe.

4. Sie können die Werte für **Name** und **Rolle** ändern. Sie können auch **Benutzer** auswählen bzw. ihre Auswahl aufheben, um Benutzer zur Gruppe hinzuzufügen bzw. daraus zu entfernen.



5. Klicken Sie auf **Speichern**.

Löschen von Benutzergruppen

Sie können nur Benutzergruppen löschen, denen derzeit keine Benutzer zugewiesen sind. Wenn einer Gruppe Benutzer zugewiesen sind, müssen Sie zuerst die Benutzer aus der Gruppe entfernen, bevor Sie die Gruppe löschen können.

So löschen Sie eine Benutzergruppe:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzerverwaltung** > **Benutzergruppen**.
   Der Bildschirm **Benutzergruppen** wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf die gewünschte Benutzergruppe und wählen Sie **Benutzergruppe löschen** aus dem Kontextmenü.
   Ein Bestätigungsfenster wird angezeigt.

Alternativ können Sie eine Benutzergruppe auswählen und dann auf die Schaltfläche **Aktionen** > **Benutzergruppe löschen** klicken.

3. Klicken Sie auf **Löschen**.
   Die Benutzergruppe wird aus dem System gelöscht.

Benutzerrollen

Im Folgenden finden Sie eine kurze Beschreibung der verfügbaren Rollen.

- **Administrator** – Verfügt über maximale Berechtigungen, um alle operativen und administrativen Aufgaben im System durchzuführen, wie zum Beispiel das Erstellen neuer Benutzerkonten.
- **Schreibgeschützt** – Kann Daten (Asset-Inventar, Ereignisse, Netzwerk-Traffic) anzeigen, aber keine Aktionen im System durchführen.
- **Sicherheitsanalyst** – Kann Daten im System anzeigen und Sicherheitsereignisse auflösen.
- **Sicherheitsmanager** – Kann alle sicherheitsbezogenen Funktionen verwalten, einschließlich Konfigurieren von Richtlinien, Anzeigen von Daten im System und Auflösen von Ereignissen.
- **Site-Operator** – Kann Daten im System anzeigen und das Asset-Inventar verwalten.
- **Supervisor** – Verfügt über vollständige Berechtigungen, um alle operativen Aufgaben im System sowie einige eingeschränkte administrative Aufgaben durchzuführen (die Erstellung neuer Benutzer oder andere sensible Aktivitäten gehören nicht dazu).

Tabelle der Benutzerrollen

Die folgende Tabelle enthält eine detaillierte Aufschlüsselung der genauen Berechtigungen, die für die einzelnen Rollen aktiviert sind.

Berechtigung	Administrator (lokal)	Administrator (extern/ AD)	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Ereignisse							
Ereignisse anzeigen	✓	✓	✓	✓	✓	✓	✓
Auflösen	✓	✓	✓	✓	✓	X	X
Erfassungsdatei herunterladen	✓	✓	✓	✓	✓	✓	✓
Aus Richtlinie ausschließen	✓	✓	✓	✓	X	X	X
Alle auflösen	✓	✓	✓	✓	✓	X	X
Exportieren	✓	✓	✓	✓	✓	✓	✓
Richtlinie auf Forti Gate erstellen	✓	✓	✓	✓	X	X	X
Aktualisieren	✓	✓	✓	✓	✓	✓	✓
Richtlinien							
Richtlinien anzeigen	✓	✓	✓	✓	✓	✓	✓
Aktivieren/ Deaktivieren	✓	✓	✓	✓	X	X	X

Berechtigung	Administrator (lokal)	Administrator (extern/AD)	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Aktion anzeigen	✓	✓	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✓	✓	X	X	X
Duplizieren	✓	✓	✓	✓	X	X	X
Löschen	✓	✓	✓	✓	X	X	X
Richtlinie erstellen	✓	✓	✓	✓	X	X	X
Exportieren	✓	✓	✓	✓	✓	✓	✓
Assets							
Assets anzeigen	✓	✓	✓	✓	✓	✓	✓
Aktion anzeigen	✓	✓	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✓	X	X	✓	X
Löschen	✓	✓	✓	X	X	✓	X
Importieren (neue Assets über CSV-Datei hochladen)	✓	✓	✓	X	X	✓	X
Ausblenden	✓	✓	✓	X	X	✓	X
Exportieren	✓	✓	✓	✓	✓	✓	✓
Erneut synchronisieren	✓	✓	✓	✓	✓	✓	X
Nessus-Scan	✓	✓	✓	✓	✓	✓	X
Snapshot erstellen (einzelnes Asset)	✓	✓	✓	✓	✓	✓	X
Offene Ports aktualisieren (einzelnes Asset)	✓	✓	✓	✓	✓	X	X
Port-Status aktualisieren (einzelnes Asset)	✓	✓	✓	✓	✓	X	X

Berechtigung	Administrator (lokal)	Administrator (extern/AD)	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Im Browser anzeigen (einzelnes Asset)	✓	✓	✓	✓	✓	✓	✓
In der Haupt-Asset-Übersicht anzeigen (einzelnes Asset)	✓	✓	✓	✓	✓	✓	✓
Angriffsvektor generieren (einzelnes Asset)	✓	✓	✓	✓	✓	✓	✓
Schwachstellen (Plugins)							
Plugin-Treffer anzeigen	✓	✓	✓	✓	✓	✓	✓
Aktion anzeigen	✓	✓	✓	✓	✓	✓	✓
Kommentar bearbeiten	✓	✓	✓	✓	✓	X	X
Plugin-Satz aktualisieren	✓	✓	✓	✓	X	X	X
Exportieren	✓	✓	✓	✓	✓	✓	✓
Netzwerk							
Paketerfassung aktivieren	✓	✓	✓	X	X	X	X
Laufende Erfassungen schließen	✓	✓	✓	✓	✓	✓	X
PCAP-Datei herunterladen	✓	✓	✓	✓	✓	✓	✓
Konversationstabelle exportieren	✓	✓	✓	✓	✓	✓	✓
Als Baseline festlegen	✓	✓	✓	✓	X	X	X
Übersicht generieren	✓	✓	✓	✓	✓	✓	✓
Übersicht aktualisieren	✓	✓	✓	✓	✓	✓	✓
Gruppen							
Gruppen anzeigen	✓	✓	✓	✓	✓	✓	✓

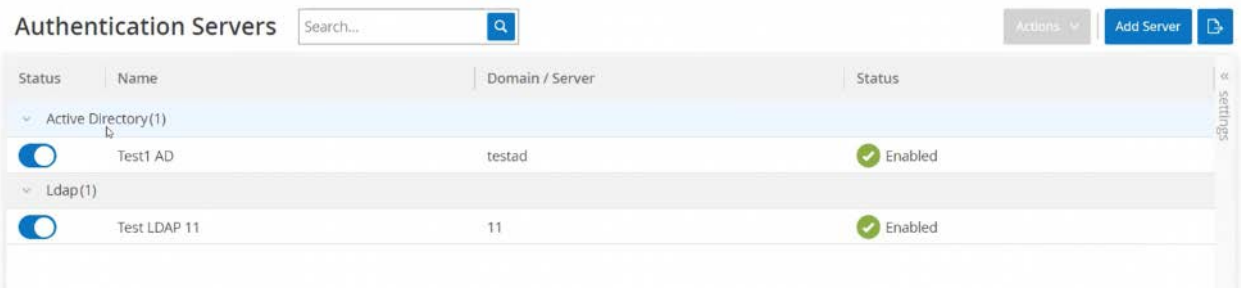
Berechtigung	Administrator (lokal)	Administrator (extern/AD)	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Aktion anzeigen	✓	✓	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✓	✓	X	X	X
Duplizieren	✓	✓	✓	✓	X	X	X
Löschen	✓	✓	✓	✓	X	X	X
Gruppe erstellen	✓	✓	✓	✓	X	X	X
Exportieren	✓	✓	✓	✓	✓	✓	✓
Bericht							
Berichte anzeigen	✓	✓	✓	✓	✓	✓	✓
Generieren	✓	✓	✓	✓	✓	✓	✓
Herunterladen	✓	✓	✓	✓	✓	✓	✓
Exportieren	✓	✓	✓	✓	✓	✓	✓
Netzwerksegmente							
Netzwerksegmente anzeigen	✓	✓	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✓	✓	X	X	X
Löschen	✓	✓	✓	✓	X	X	X
Erstellen	✓	✓	✓	✓	X	X	X
Exportieren	✓	✓	✓	✓	✓	✓	✓
Mehr erfahren	✓	✓	✓	✓	✓	✓	✓
Lokale Einstellungen							
Abfragen	✓	✓	✓	X	X	X	X
Systemkonfiguration – Gerätedetails	✓	✓	✓	X	X	X	X

Berechtigung	Administrator (lokal)	Administrator (extern/AD)	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Systemkonfiguration – Sensoren	✓	✓	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)
Systemkonfiguration – Portkonfiguration	✓	✓	✓	X	X	X	X
Systemkonfiguration – Updates	✓	✓	✓	X	X	X	X
Systemkonfiguration – Zertifikat (HTTPS)	✓	✓	X	X	X	X	X
Systemkonfiguration – API-Schlüssel	✓	X	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)
Systemkonfiguration – Lizenz	✓	✓	X	X	X	X	X
Umgebungskonfiguration – Asset-Einstellungen	✓	✓	✓	X	X	X	X
Umgebungskonfiguration – Ausgeblendete Assets	✓	✓	✓	✔ – keine Wiederherstellung	✔ – keine Wiederherstellung	✓	✔ – keine Wiederherstellung
Umgebungskonfiguration – Benutzerdefinierte Felder	✓	✓	✓	X	X	X	X
Umgebungskonfiguration – Ereigniscluster	✓	✓	✓	X	X	X	X
Umgebungskonfiguration – PCAP-Player	✓	✓	✓	X	X	X	X
Benutzer und Rollen – Benutzereinstellungen	✓	✓	✓	X	X	X	X
Benutzer und Rollen – Lokale Benutzer	✓	X	X	X	X	X	X
Benutzer und Rollen – Benutzergruppen	✓	X	X	X	X	X	X
Benutzer und Rollen – Active Directory	✓	X	X	X	X	X	X
Integrationen	✓	✓	X	X	X	X	X
Server	✓	✓	✓	✔ (Keine Aktionen)	✔ (Keine Aktionen)	✔ (Keine Aktionen)	✔ (Keine Aktionen)

Berechtigung	Administrator (lokal)	Administrator (extern/ AD)	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Systemaktionen	✓	✓ – ohne Zurücksetzung auf Werkseinstellungen	✓ – nur Sicherung und Diagnose	✓ – nur Diagnose	X	X	X
Systemprotokoll	✓	✓	✓	✓	✓	✓	✓ – kein Syslog
Aktivieren (beim Setup und nach Deaktivierung)	✓	✓	X	X	X	X	X
Assets löschen	✓	✓	✓	X	X	X	X

Authentifizierungsserver

Im Bildschirm „Authentifizierungsserver" werden Ihre vorhandenen Integrationen mit Authentifizierungsservern angezeigt. Wenn Sie einen Server hinzufügen möchten, klicken Sie auf die Schaltfläche **Server hinzufügen**.



Active Directory

Sie können Tenable.ot mit dem Active Directory Ihrer Organisation integrieren. Dies ermöglicht es Benutzern, sich mit ihren Active Directory-Zugangsdaten bei Tenable.ot einzuloggen. Im Rahmen der Konfiguration richten Sie die Integration ein und ordnen dann Gruppen in Ihrem AD zu Benutzergruppen in Tenable.ot zu.

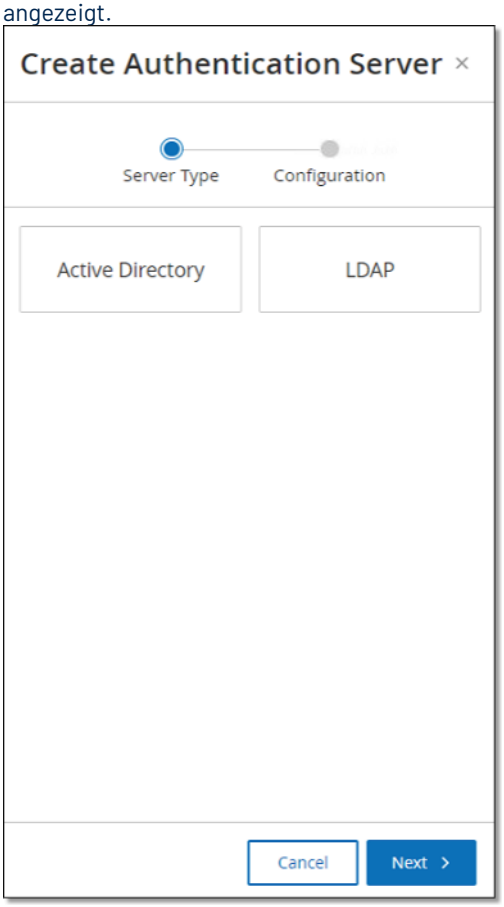
Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe *Administratoren* > Rolle *Administrator*, Benutzergruppe *Site-Operatoren* > Rolle *Site-Operator* usw. Eine Erläuterung der verfügbaren Rollen finden Sie unter **Benutzerrollen**.

So konfigurieren Sie Active Directory:

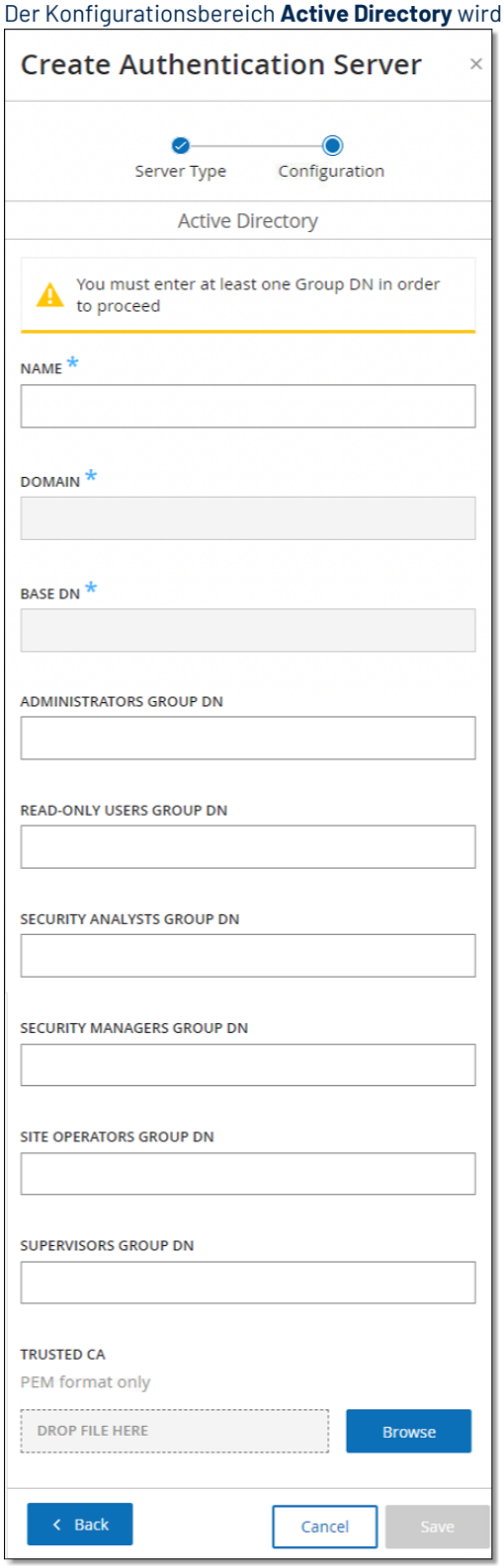
1. **Optional** können Sie ein CA-Zertifikat von der Zertifizierungsstelle Ihrer Organisation oder vom Netzwerkadministrator beziehen und es auf Ihren lokalen Rechner laden.

Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: Benutzergruppe *Administratoren* > Rolle *Administrator*, Benutzergruppe *Site-Operatoren* > Rolle *Site-Operator* usw. Eine Erläuterung der verfügbaren Rollen finden Sie unter **Benutzerrollen**.

2. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzer und Rollen** > **Authentifizierungsserver**.
3. Klicken Sie auf **Server hinzufügen**.
   Der Seitenbereich **Authentifizierungsserver erstellen** wird geöffnet und der Bereich **Servertyp** wird angezeigt.



4. Klicken Sie auf **Active Directory**.
   Der Konfigurationsbereich **Active Directory** wird angezeigt.



5. Geben Sie im Feld **Name** den Namen ein, der im Login-Bildschirm verwendet werden soll.
6. Geben Sie im Feld **Domänenname** den FQDN der Organisationsdomäne ein (z. B. firma.com).

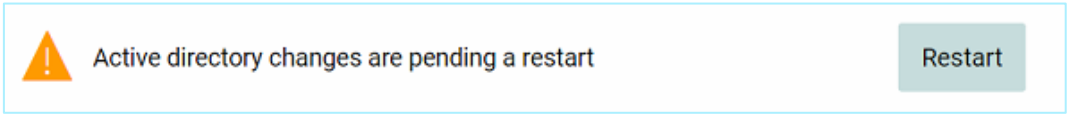
Wenn Sie Ihren Domänennamen nicht kennen, können Sie nach ihm suchen, indem Sie den Befehl „set“ in die Windows-Eingabeaufforderung/Befehlszeile eingeben. Der für das Attribut „USERDNSDOMAIN“ angegebene Wert ist der Domänenname.

7. Geben Sie im Feld **Basis-DN** den Distinguished Name der Domäne ein. Das Format für diesen Wert ist „DC={Domäne der zweiten Ebene},DC={Domäne der obersten Ebene}“ (z. B. DC=FIRMA,DC=com).
8. Geben Sie für jede der Gruppen, die Sie aus einer AD-Gruppe einer Tenable.ot-Benutzergruppe zuordnen möchten, den DN der AD-Gruppe in das entsprechende Feld ein. Um beispielsweise eine Gruppe von Benutzern der Benutzergruppe „Administratoren“ zuzuweisen, geben Sie den DN der Active Directory-Gruppe, der Sie Administratorrechte zuweisen möchten, in das Feld **Administratorgruppen-DN** ein.

Wenn Sie den DN der Gruppe, der Sie Tenable.ot-Berechtigungen zuweisen möchten, nicht kennen, können Sie eine Liste aller in Ihrem Active Directory konfigurierten Gruppen anzeigen, die Benutzer enthalten, indem Sie den Befehl „dsquery group -name Users*“ in die Windows-Eingabeaufforderung/Befehlszeile eingeben. Der Name der Gruppe, die Sie zuweisen möchten, sollte im gleichen Format in das Feld eingegeben werden, in dem er angezeigt wird (z. B. „CN=IT_Admins,OU=Gruppen,DC=Firma,DC=Com“). Der Basis-DN muss ebenfalls am Ende jedes DN enthalten sein.

Diese Felder sind keine Pflichtfelder. Wenn ein Feld nicht ausgefüllt ist, werden dieser Benutzergruppe keine AD-Benutzer zugewiesen. Sie können eine Integration ohne zugeordnete Gruppen einrichten, aber in diesem Fall können erst dann Benutzer auf das System zugreifen, nachdem Sie mindestens eine Gruppenzuordnung hinzugefügt haben.

9. Klicken Sie im Abschnitt **Vertrauenswürdige Zertifizierungsstelle** auf **Durchsuchen** und navigieren Sie zu der Datei, die das CA-Zertifikat Ihrer Organisation enthält (das Sie von Ihrer Zertifizierungsstelle oder Ihrem Netzwerkadministrator erhalten haben). (Optional)
10. Aktivieren Sie das Kontrollkästchen **Active Directory aktivieren**.
11. Klicken Sie auf **Speichern**.
    Ein Popup-Fenster fordert Sie zum Neustart des Geräts auf, um Active Directory zu aktivieren.



12. Klicken Sie auf **Neu starten**.
    Das Gerät startet neu. Beim Neustart werden die Active Directory-Einstellungen aktiviert. Jeder Benutzer, der den festgelegten Gruppen zugewiesen ist, kann mit seinen Zugangsdaten auf die Tenable.ot-Plattform zugreifen.

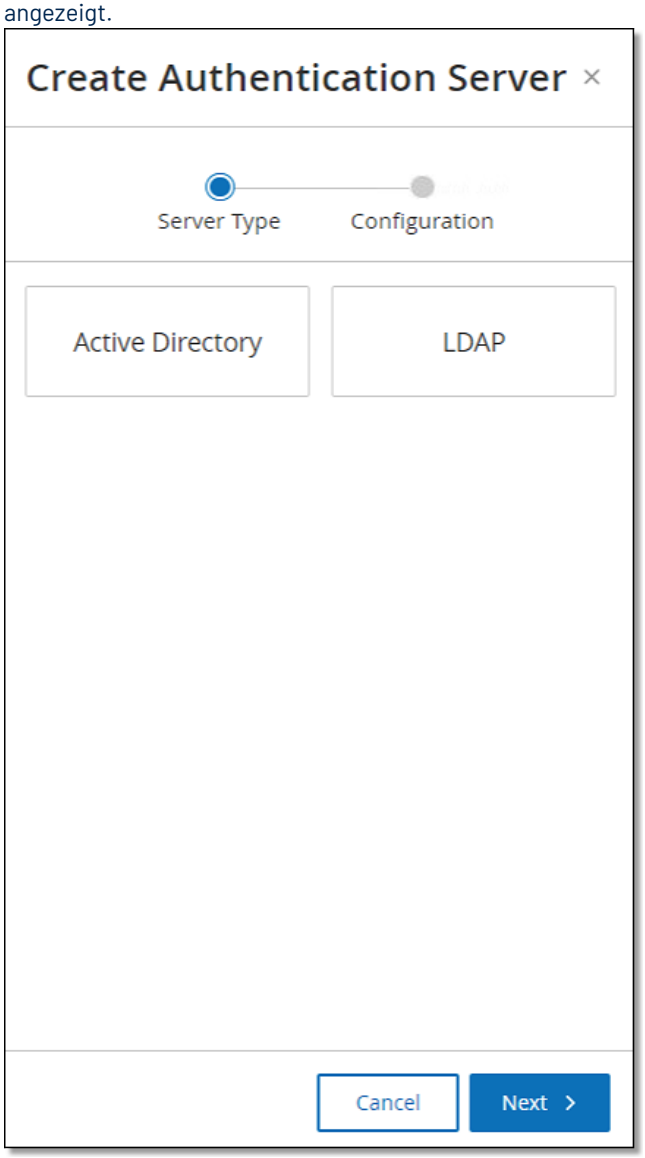
Um sich über Active Directory einzuloggen, sollte der Benutzerprinzipalname (User Principal Name, UPN) auf der Login-Seite verwendet werden. In einigen Fällen muss hierfür einfach nur „@<Domäne>.com“ zum Benutzernamen hinzugefügt werden.

LDAP

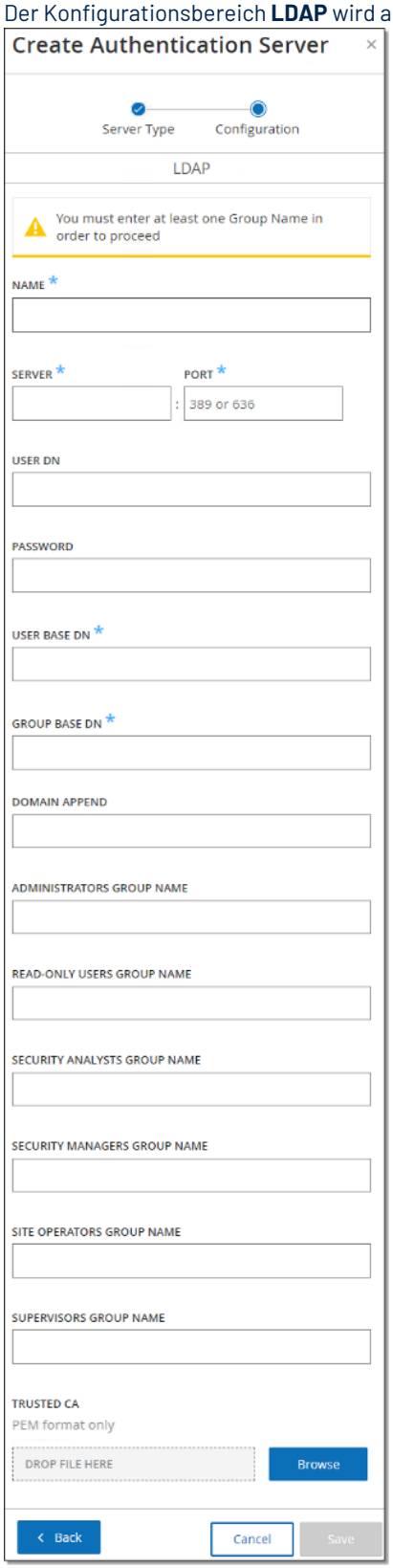
Sie können Tenable.ot mit dem LDAP Ihrer Organisation integrieren. Dies ermöglicht es Benutzern, sich mit ihren LDAP-Zugangsdaten bei Tenable.ot einzuloggen. Im Rahmen der Konfiguration richten Sie die Integration ein und ordnen dann Gruppen in Ihrem AD zu Benutzergruppen in Tenable.ot zu.

So konfigurieren Sie LDAP:

1. Gehen Sie unter „Lokale Einstellungen“ zum Bildschirm „Benutzer und Rollen“ > **Authentifizierungsserver**.
2. Klicken Sie auf **Server hinzufügen**.
   Der Seitenbereich **Authentifizierungsserver hinzufügen** wird geöffnet und der Bereich **Servertyp** wird angezeigt.



3. Wählen Sie **LDAP** aus.
   Der Konfigurationsbereich **LDAP** wird angezeigt.



4. Geben Sie im Feld **Name** den Namen ein, der im Login-Bildschirm verwendet werden soll.

Der Login-Name muss eindeutig sein und sollte darauf hinweisen, dass er für LDAP verwendet wird. Falls sowohl LDAP als auch Active Directory konfiguriert sind, unterscheiden sich die verschiedenen Konfigurationen im Login-Bildschirm nur durch den Login-Namen.

5. Geben Sie im Feld **Server** den FQDN oder die Login-Adresse ein.

Wenn Sie eine sichere Verbindung nutzen, wird empfohlen, den FQDN anstelle einer IP-Adresse zu verwenden, um sicherzustellen, dass das bereitgestellte sichere Zertifikat verifiziert wird.

Wenn ein Hostname verwendet wird, muss er in der Liste der DNS-Server im Tenable.ot-System enthalten sein. Siehe **Systemkonfiguration** > **GERÄT**.

6. Geben Sie im Feld **Port** den Wert 389 ein, um eine nicht sichere Verbindung zu verwenden, oder 636, um eine sichere SSL-Verbindung zu nutzen.

Wenn Port 636 gewählt wird, ist ein Zertifikat erforderlich, um die Integration abzuschließen.

7. Geben Sie im Feld **Benutzer-DN** den DN mit Parametern im DN-Format ein (Beispiel: für den Servernamen „AD_1.qa.com" lautet der Benutzer-DN „CN=Administrator,CN=Benutzer,DC=qa,DC=com").
8. Geben Sie im Feld **Passwort** das Passwort des Benutzer-DN ein.

Die Tenable.ot-Konfiguration mit LDAP funktioniert nur so lange, wie das Passwort des Benutzer-DN gültig ist. Falls sich das Passwort des Benutzer-DN ändert oder abläuft, muss auch die Tenable.ot-Konfiguration aktualisiert werden.

9. Geben Sie im Feld **Basis-DN des Benutzers** den Basis-Domänennamen im DN-Format ein (z. B. „DC=qa,DC=com").
10. Geben Sie im Feld **Basis-DN der Gruppe** den Basis-Domänennamen der Gruppe im DN-Format ein.
11. Geben Sie im Feld **Domänenanhang** die Standarddomäne ein, die an die Authentifizierungsanforderung angehängt wird, falls der Benutzer keine Domäne angewendet hat, in der er Mitglied ist.
12. Geben Sie in die relevanten Gruppennamenfelder die Tenable-Gruppennamen ein, die der Benutzer mit der LDAP-Konfiguration verwenden soll.
13. Wenn Sie Port 636 für die Konfiguration verwenden, klicken Sie unter **Vertrauenswürdige Zertifizierungsstelle** auf **Durchsuchen** und navigieren Sie zu einer gültigen PEM-Zertifikatdatei.
14. Klicken Sie auf **Speichern**.
    Der Server wird im Modus „Deaktiviert" gestartet.
15. Um die Konfiguration zu übernehmen, stellen Sie den Umschalter auf **EIN**.
    Das Dialogfeld **Systemneustart** wird angezeigt.
16. Klicken Sie auf **Jetzt neu starten**, um das System sofort neu zu starten und die Konfiguration anzuwenden, oder auf **Später neu starten**, um das System vorübergehend ohne die neue Konfiguration weiterzuverwenden.

Die Aktivierung/Deaktivierung der LDAP-Konfiguration wird erst abgeschlossen, wenn das System neu gestartet wird. Wenn Sie das System nicht sofort neu starten, klicken Sie im Banner am oberen Bildschirmrand auf die Schaltfläche **Neu starten**, wenn Sie zum Neustart bereit sind.

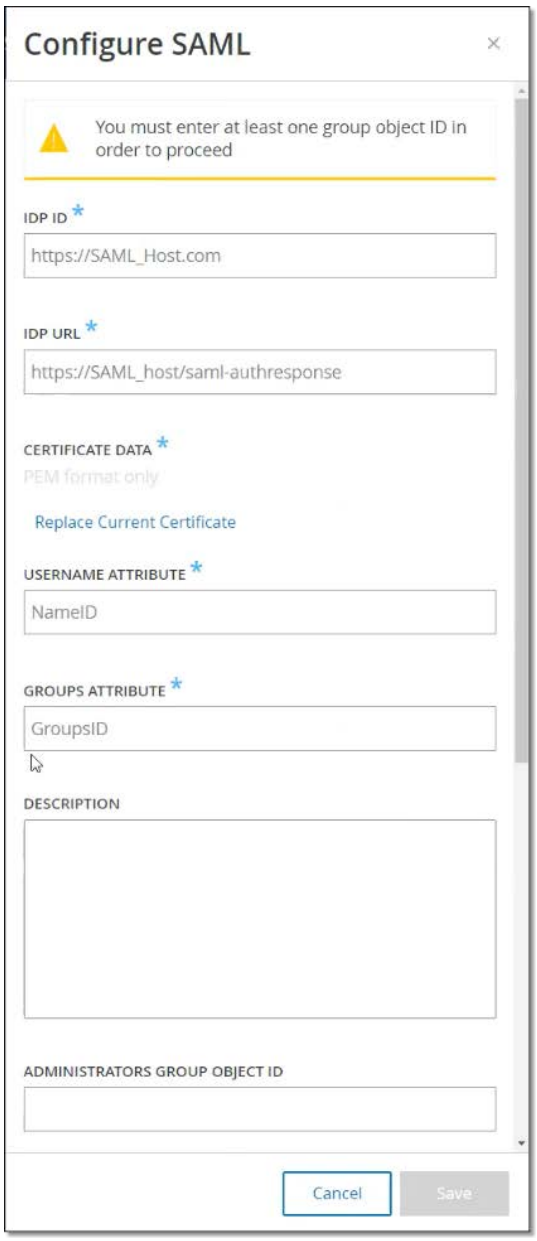
SAML

Sie können Tenable.ot mit dem Identitätsanbieter Ihrer Organisation (z. B. Microsoft Azure) integrieren. Dies ermöglicht es Benutzern, sich über ihren Identitätsanbieter zu authentifizieren. Die Konfiguration beinhaltet die Einrichtung der Integration, indem Sie eine Tenable.ot-Anwendung innerhalb Ihres Identitätsanbieters erstellen, Informationen über Ihre erstellte Tenable.ot-Anwendung eingeben, das Zertifikat Ihres Identitätsanbieters auf die Tenable.ot-Seite **SAML** hochladen und dann Gruppen von Ihrem Identitätsanbieter zu Benutzergruppen in Tenable.ot zuordnen. Ein ausführliches Tutorial zur Integration von Tenable.ot mit Microsoft Azure finden Sie in **Anhang 2 – SAML-Integration für Azure Active Directory**.

So konfigurieren Sie SAML:

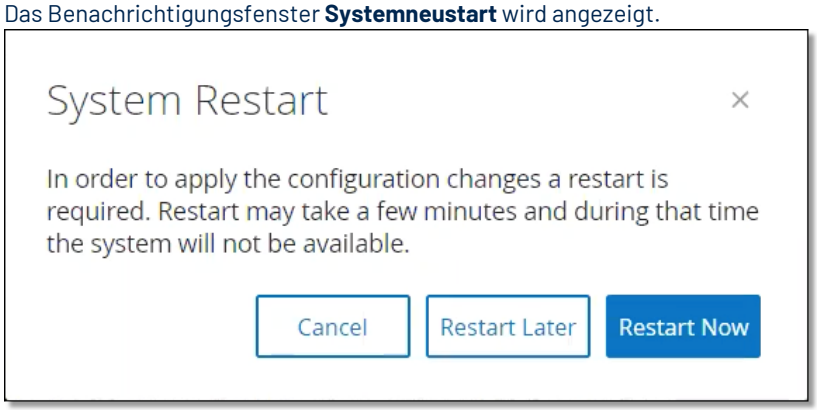
1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Benutzer und Rollen** > **SAML**.

2. Klicken Sie auf **Konfigurieren**.
   Der Seitenbereich **SAML konfigurieren** wird angezeigt.

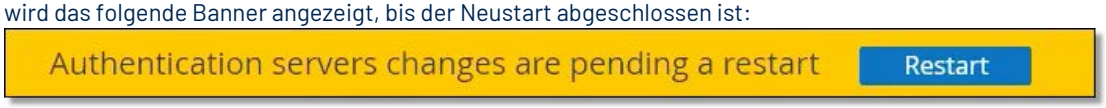


3. Geben Sie im Feld **IDP-ID** die ID des Identitätsanbieters für die Tenable.ot-Anwendung ein.
4. Geben Sie im Feld **IDP-URL** die URL des Identitätsanbieters für die Tenable.ot-Anwendung ein.
5. Klicken Sie unter **Zertifikatdaten** auf **Aktuelles Zertifikat ersetzen**, navigieren Sie zur Zertifikatdatei des Identitätsanbieters, die Sie zur Verwendung mit der Tenable.ot-Anwendung heruntergeladen haben, und öffnen Sie sie.
6. Geben Sie im Feld **Username-Attribut** das Username-Attribut vom Identitätsanbieter für die Tenable.ot-Anwendung ein.
7. Geben Sie im Feld **Groups-Attribut** das Groups-Attribut vom Identitätsanbieter für die Tenable.ot-Anwendung ein.
8. Geben Sie eine Beschreibung in das Feld **Beschreibung** ein. (Optional)
9. Rufen Sie für jede Gruppenzuordnung, die Sie konfigurieren möchten, die **Gruppenobjekt-ID** des Identitätsanbieters für eine Gruppe von Benutzern auf und geben Sie sie in Feld der gewünschten **Gruppenobjekt-ID** ein, um sie der gewünschten Tenable.ot-Benutzergruppe zuzuordnen.
10. Klicken Sie auf **Speichern**, um die Informationen im Seitenbereich zu speichern und diesen zu schließen.

11. Klicken Sie im Bildschirm **SAML** auf den Umschalter **SAML Single Sign-On-Login**, um ihn auf **EIN** zu stellen. Das Benachrichtigungsfenster **Systemneustart** wird angezeigt.



12. Klicken Sie auf **Jetzt neu starten**, um das System sofort neu zu starten und die SAML-Konfiguration anzuwenden, oder klicken Sie auf **Später neu starten**, um die Anwendung der SAML-Konfiguration auf den nächsten Neustart des Systems zu verschieben. Wenn Sie sich für einen späteren Neustart entscheiden, wird das folgende Banner angezeigt, bis der Neustart abgeschlossen ist:



Beim Neustart werden die Einstellungen aktiviert und alle Benutzer, die den festgelegten Gruppen zugewiesen sind, können mit den Zugangsdaten ihres Identitätsanbieters auf die Tenable.ot-Plattform zugreifen.

Integrationen

Sie können Integrationen mit anderen unterstützten Plattformen einrichten, damit Tenable.ot mit Ihren anderen Cybersecurity-Plattformen synchronisiert werden kann.

Tenable-Produkte

Sie können Tenable.ot mit Tenable.sc und Tenable.io integrieren. Dadurch kann Tenable.ot Daten mit den anderen Plattformen austauschen. Die synchronisierten Daten umfassen sowohl OT-Schwachstellen als auch Daten, die durch IT-bezogene Nessus-Scans erfasst wurden, die über Tenable.ot initiiert wurden.

Daten für Assets, die in Tenable.ot „ausgeblendet“ wurden, werden nicht über die Integration an Tenable.sc und Tenable.io gesendet.

Um die Plattformen zu integrieren, muss Tenable.ot in der Lage sein, Tenable.sc und/oder Tenable.io über Port 443 zu erreichen. Es wird empfohlen, einen speziellen Benutzer auf Tenable.sc und/oder Tenable.io zu erstellen, der als Integrationsbenutzer für Tenable.ot fungiert.

Tenable.sc

Um Tenable.sc zu integrieren, erstellen Sie ein neues Agent-Repository für Tenable.ot-Daten. Notieren Sie sich die Repository-ID. Erstellen Sie in Tenable.ot eine neue Integration, geben Sie die IP oder den Hostnamen Ihres Tenable.sc-Systems sowie Ihre Kontozugangsdaten und die Repository-ID ein und legen Sie dann die Synchronisierungsfrequenz fest. Klicken Sie dann mit der rechten Maustaste auf die neu hinzugefügte Integration und wählen Sie „Synchronisieren“.

Es wird empfohlen, einen bestimmten Benutzer in Tenable.sc zu erstellen, der für die Integration in Tenable.ot verwendet wird. Der Benutzer sollte über die Rolle *Sicherheitsmanager*/*Sicherheitsanalyst* oder *Schwachstellenanalyst* verfügen und der Gruppe „Vollzugriff“ zugewiesen sein.

Tenable.io

Geben Sie für die Integration in Tenable.io Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel ein und legen Sie dann die Synchronisierungsfrequenz fest.

Sie müssen zuerst einen API-Schlüssel in der Tenable.io-Konsole generieren (**Einstellungen** (Settings) > **Mein Konto** (My Account) > **API-Schlüssel** (API Keys) > **Generieren** (Generate)). Sie erhalten einen Zugriffsschlüssel und einen geheimen Schlüssel, die Sie beim Konfigurieren der Integration in der Tenable.ot-Konsole eingeben.

Palo Alto Networks – Next Generation Firewall

Sie können von Tenable.ot erfasste Asset-Inventarisierungsdaten an Ihr Palo Alto-System übertragen.

Um Tenable.ot mit Ihrer Palo Alto NGFW zu integrieren, geben Sie die IP oder den Hostnamen Ihrer Palo Alto NGRW sowie die Zugangsdaten für Ihr NGRW-Konto ein.

Aruba – ClearPass-Richtlinienmanager

Sie können von Tenable.ot erfasste Asset-Inventarisierungsdaten an Ihr Aruba-System übertragen.

Um Tenable.ot mit Ihrem Aruba ClearPass-System zu integrieren, geben Sie die IP oder den Hostnamen Ihres Aruba ClearPass-Systems sowie die Zugangsdaten für Ihr Aruba ClearPass-Konto ein.

Server

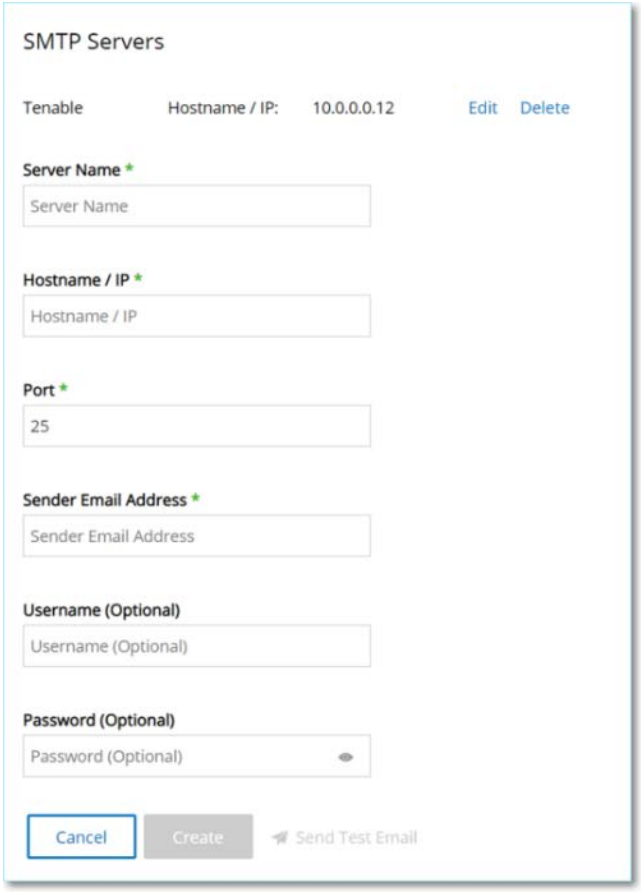
Sie können SMTP-Server und Syslog-Server im System einrichten, damit Ereignisbenachrichtigungen per E-Mail gesendet und/oder in einem SIEM-System protokolliert werden können. Sie können auch FortiGate-Firewalls einrichten, um FortiGate auf Grundlage von Tenable.ot-Netzwerkereignissen Vorschläge zu Firewall-Richtlinien zu senden.

SMTP-Server

Damit Ereignisbenachrichtigungen per E-Mail an die entsprechenden Parteien gesendet werden können, müssen Sie einen *SMTP-Server* im System einrichten. Wenn Sie keinen SMTP-Server einrichten, können die vom System generierten Ereignisse nicht per E-Mail versendet werden. In jedem Fall können alle Ereignisse in der Verwaltungskonsole (UI) im Bildschirm „Ereignisse“ eingesehen werden.

➡ So richten Sie einen SMTP-Server ein:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Server** > **SMTP-Server**.
2. Klicken Sie auf **SMTP-Server hinzufügen**.
   Das Konfigurationsfenster **SMTP-Server** wird angezeigt.



3. Geben Sie im Feld **Servername** den Namen eines SMTP-Servers ein, der für E-Mail-Benachrichtigungen verwendet werden soll.
4. Geben Sie im Feld **Hostname/IP** einen Hostnamen oder eine IP-Adresse des SMTP-Servers ein.
5. Geben Sie im Feld **Port** die Portnummer ein, an der der SMTP-Server nach Ereignissen lauschen soll (Standard: 25).
6. Geben Sie im Feld **E-Mail-Adresse des Absenders** eine E-Mail-Adresse ein, die als Absender der Ereignisbenachrichtigungs-E-Mail angezeigt wird.
7. Geben Sie in die Felder **Benutzername** und **Passwort** einen Benutzernamen und ein Passwort für den Zugriff auf den SMTP-Server ein. Diese Felder sind optional.
8. An dieser Stelle können Sie versuchen, eine Test-E-Mail zu senden, um zu überprüfen, ob die Konfiguration erfolgreich war. Klicken Sie auf **Test-E-Mail senden**, geben Sie die E-Mail-Adresse ein, an die gesendet

werden soll, und überprüfen Sie den Posteingang, um festzustellen, ob die E-Mail angekommen ist. Wenn die E-Mail nicht angekommen ist, führen Sie eine Fehlerbehebung durch, um die Ursache des Problems zu ermitteln und es zu beheben.

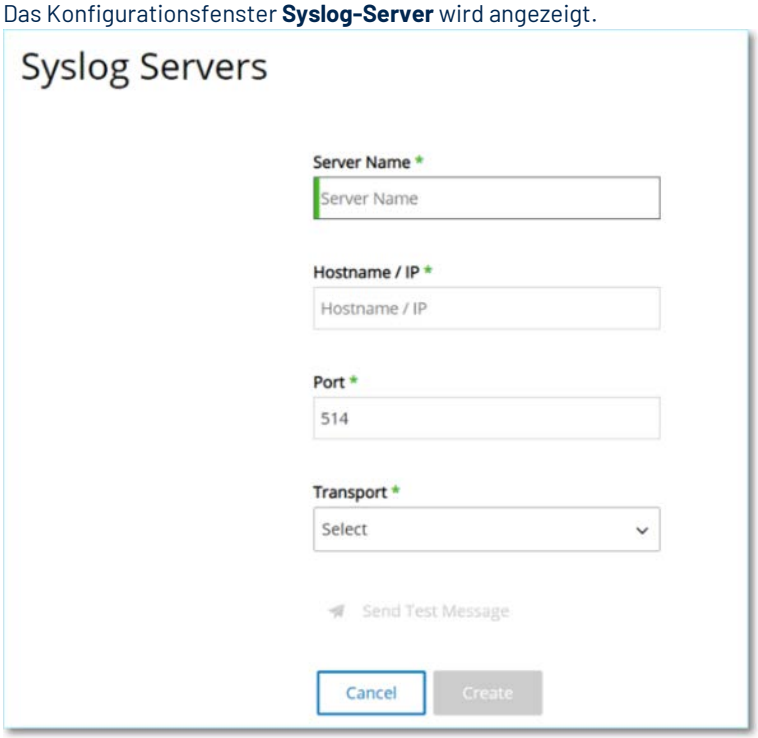
9. Klicken Sie auf **Speichern**.
   Sie können weitere SMTP-Server einrichten, indem Sie den oben beschriebenen Vorgang wiederholen.

Syslog-Server

Damit Ereignisprotokolle auf einem externen Server gesammelt werden können, müssen Sie einen *Syslog-Server* im System einrichten. Wenn Sie keinen Syslog-Server einrichten möchten, werden die Ereignisprotokolle nur auf der Tenable.ot-Plattform gespeichert.

So richten Sie einen Syslog-Server ein:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Server** > **Syslog-Server**.
2. Klicken Sie auf **+ Syslog-Server hinzufügen**.
   Das Konfigurationsfenster **Syslog-Server** wird angezeigt.



3. Geben Sie im Feld **Servername** den Namen eines Syslog-Servers ein, der zum Protokollieren von Systemereignissen verwendet werden soll.
4. Geben Sie im Feld **Hostname/IP** einen Hostnamen oder eine IP-Adresse des Syslog-Servers ein.
5. Geben Sie im Feld **Port** die Portnummer auf dem Syslog-Server ein, an die Ereignisse gesendet werden. (Standard: 514)
6. Wählen Sie im Feld **Transport** das gewünschte Transportprotokoll in der Dropdown-Liste aus. Verfügbare Optionen: *TCP* oder *UDP*.

7. Wenn Sie eine Testnachricht senden möchten, um zu überprüfen, ob die Konfiguration erfolgreich war, klicken Sie auf **Testnachricht senden** und prüfen Sie, ob die Nachricht angekommen ist. Wenn die Nachricht nicht angekommen ist, führen Sie eine Fehlerbehebung durch, um die Ursache des Problems zu ermitteln und es zu beheben.
8. Klicken Sie auf **Speichern**.
   Sie können weitere Syslog-Server einrichten, indem Sie den oben beschriebenen Vorgang wiederholen.

FortiGate-Firewalls

So richten Sie einen FortiGate-Server ein:

1. Gehen Sie unter **Lokale Einstellungen** zum Bildschirm **Server** > **FortiGate-Firewalls**.
2. Klicken Sie auf die Schaltfläche **Firewall hinzufügen**.
   Das Konfigurationsfenster **FortiGate-Firewall hinzufügen** wird angezeigt.

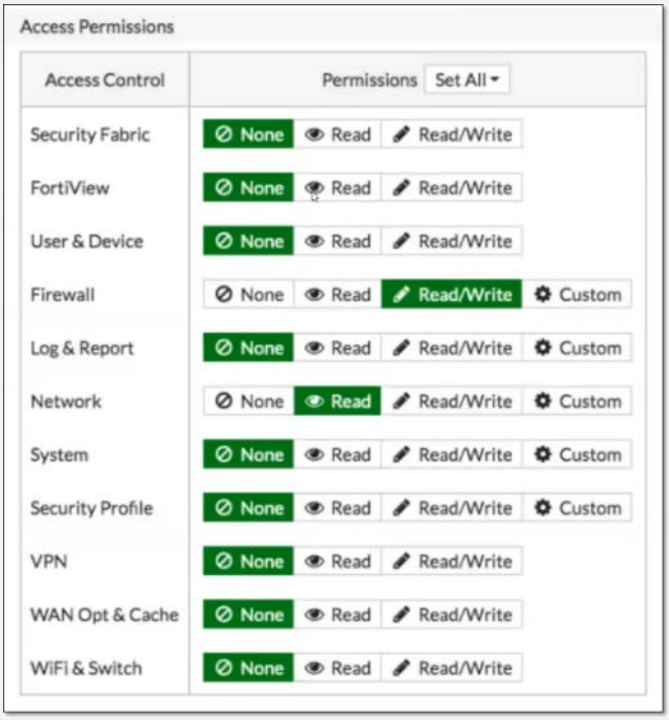
3. Geben Sie im Feld **Servername** den Namen eines FortiGate-Servers ein, der verwendet werden soll.
4. Geben Sie im Feld **Host/IP** einen Hostnamen oder eine IP-Adresse des FortiGate-Servers ein.
5. Geben Sie im Feld **API-Schlüssel** das **API-Token** ein, das Sie in FortiGate generiert haben. Weitere Informationen finden Sie im nachfolgenden Hinweis.
6. Klicken Sie auf **Hinzufügen**.
   Der FortiGate-Firewall-Server wird erstellt.

Die Anweisungen zum Generieren eines FortiGate-API-Tokens finden Sie auf folgender Seite: https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

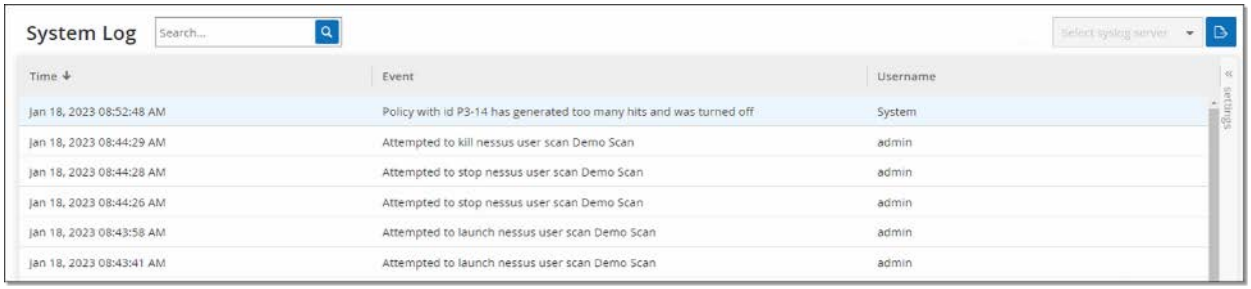
Hinweis:

- Verwenden Sie als Quelladresse (die erforderlich ist, um sicherzustellen, dass das API-Token nur von vertrauenswürdigen Hosts verwendet werden kann) die IP-Adresse Ihres Tenable.ot-Geräts.

Stellen Sie beim Erstellen eines Administratorprofils für Tenable.ot sicher, dass Sie Zugriffsberechtigungen gemäß den folgenden Einstellungen anwenden:



Systemprotokoll



Der Bildschirm **Systemprotokoll** zeigt eine Liste aller Systemereignisse (z. B. Richtlinie aktiviert, Richtlinie bearbeitet, Ereignis aufgelöst usw.), die im System aufgetreten sind. Dieses Protokoll enthält sowohl vom Benutzer initiierte Ereignisse als auch automatisch auftretende Systemereignisse (z. B. Richtlinie aufgrund zu vieler Treffer automatisch deaktiviert). Dieses Protokoll enthält **keine** von einer Richtlinie generierten Ereignisse, die im Bildschirm *Ereignisse* angezeigt werden. Die Protokolle können als CSV-Datei exportiert werden. Sie können das System auch so konfigurieren, dass die Systemprotokollereignisse an einen Syslog-Server gesendet werden.

Die für die einzelnen protokollierten Ereignisse angezeigten Informationen werden in der folgenden Tabelle beschrieben:

Parameter	Beschreibung
Uhrzeit	Die Uhrzeit und das Datum des Ereignisses.
Ereignis	Eine kurze Beschreibung des aufgetretenen Ereignisses.
Benutzername	Der Name des Benutzers, der das Ereignis initiiert hat. Bei automatisch auftretenden Ereignissen wird kein Benutzername vergeben.

Senden des Systemprotokolls an einen Syslog-Server

➡ So konfigurieren Sie das System zum Senden von Systemereignissen an einen Syslog-Server:

1. Gehen Sie zum Bildschirm **Lokale Einstellungen** > **Systemprotokoll**.
2. Klicken Sie in der Kopfleiste auf **Syslog-Server auswählen**.
   Eine Dropdown-Liste mit Servern wird angezeigt.

> Informationen zum Hinzufügen eines Syslog-Servers finden Sie unter **Syslog-Server**.

3. Wählen Sie den gewünschten Server aus.
   Die Systemprotokollereignisse werden an den angegebenen Syslog-Server gesendet.

ANHANG 1 – INSTALLIEREN EINES SENSORS (VERSION 3.13 UND NIEDRIGER)

Das folgende Verfahren erläutert den vollständigen Ablauf zum Konfigurieren eines Sensors der Version 3.13 und niedriger. Einige der anfänglichen Schritte sind auch für neuere Sensoren relevant. Der Setup-Assistent wurde jedoch durch das unter **Koppeln des Sensors** beschriebene Kopplungsverfahren ersetzt.

Schritt 1 – Einrichten des Sensors

Der Sensor ist in zwei Ausführungen erhältlich, als Rack-Montage-Sensor und als konfigurierbarer Sensor, wie im Abschnitt **Tenable.ot Sensor** beschrieben. Das Rack-Montage-Modell kann in einem standardmäßigen 19-Zoll-Rack montiert oder auf einer ebenen Fläche aufgestellt werden. Das konfigurierbare Modell kann auf einer DIN-Schiene installiert oder in einem standardmäßigen 19-Zoll-Rack montiert werden (unter Verwendung des Montagelaschen-Adapterkits).

Einrichten eines Rack-Montage-Sensors

Ein Rack-Montage-Sensor kann in einem standardmäßigen 19-Zoll-Rack montiert oder auf einer ebenen Fläche (z. B. einem Schreibtisch) aufgestellt werden.

Rack-Montage (für Rack-Montage-Modell)

➡ **So montieren Sie die Tenable.ot Appliance in einem Standard-Rack (19 Zoll):**

1. Befestigen Sie die L-förmigen Halterungen an den Schraubenlöchern auf jeder Seite des Sensors, wie in der Abbildung unten gezeigt.

2. Setzen Sie zwei Schrauben auf jeder Seite ein und ziehen Sie sie mit einem Schraubendreher fest, um die Halterungen zu sichern.
3. Setzen Sie den Sensor mit den Halterungen in einen freien 1-HE-Steckplatz im Rack ein.
4. Sichern Sie das Gerät am Rack, indem Sie die Rack-Montage-Halterungen (mitgeliefert) am Rack-Rahmen befestigen. Verwenden Sie dabei geeignete Schrauben für die Rack-Montage (nicht mitgeliefert).

Stellen Sie sicher, dass das Rack geerdet ist. Vergewissern Sie sich, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

5. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss an der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Ebene Oberfläche

So installieren Sie den Tenable.ot Sensor auf einer ebenen Oberfläche:

1. Legen Sie den Sensor auf eine trockene, ebene Oberfläche (z. B. einen Schreibtisch).

Stellen Sie sicher, dass die Tischplatte eben und trocken ist.
Vergewissern Sie sich, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

2. Wenn das Gerät zusammen mit anderen Elektrogeräten aufgestellt wird, vergewissern Sie sich, dass hinter dem Lüfter (in der Rückwand) genügend Platz ist, um eine ausreichende Belüftung und Kühlung zu gewährleisten.
3. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss an der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Einrichten eines konfigurierbaren Sensors

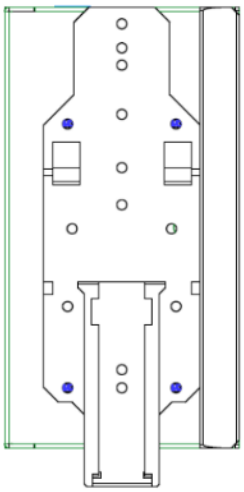
Ein konfigurierbarer Sensor kann auf einer DIN-Schiene oder in einem standardmäßigen 19-Zoll-Rack montiert werden (unter Verwendung des Montagelaschen-Adapterkits).

Montage auf DIN-Schiene

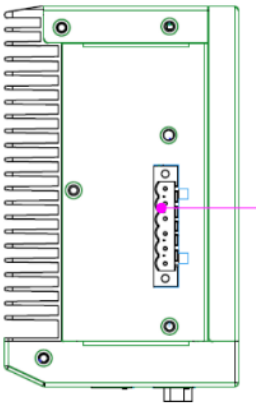
Das konfigurierbare Modell kann mit dem folgenden Verfahren auf einer DIN-Schiene montiert werden.

➡ So montieren Sie den konfigurierbaren Tenable.ot Sensor auf einer Standard-DIN-Schiene:

1. Verwenden Sie die Halterung auf der Rückseite des Sensors, um den Sensor auf einer DIN-Schiene zu montieren.



2. Schließen Sie die Stromversorgung mit einer der folgenden Methoden an:
   - **Gleichstromversorgung** – Schließen Sie das Gleichstromkabel an den Sensor an, indem Sie den 6-poligen 12–36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen. Schließen Sie dann das andere Ende des Kabels an eine Gleichstromquelle an.



- **Wechselstromversorgung** – Schließen Sie die Wechselstromversorgung an den Sensor an, indem Sie den 6-poligen 12–36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen.

Stecken Sie dann das eine Ende des Wechselstromkabels (mitgeliefert) in das Netzteil und das andere Ende in eine Netzsteckdose.

Rack-Montage (für konfigurierbares Modell)

Ein konfigurierbarer Sensor kann mit den mitgelieferten „Montagelaschen" an einem Montage-Rack befestigt werden.

➡ So montieren Sie den konfigurierbaren Sensor in einem Standard-Rack (19 Zoll):

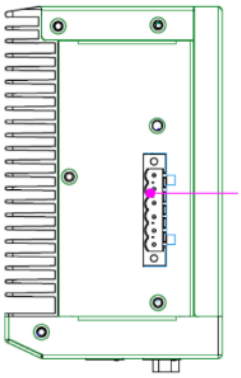
1. Bereiten Sie das Gerät wie folgt für die Rack-Montage vor:
   a. Entfernen Sie drei Schrauben auf jeder Seite des Geräts.
   b. Befestigen Sie die „Montagelaschen" mit neuen Schrauben (mitgeliefert) auf beiden Seiten des Geräts.

2. Setzen Sie die Servereinheit in einen freien 1-HE-Steckplatz im Rack ein.

Stellen Sie sicher, dass das Rack geerdet ist. Stellen Sie sicher, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.

3. Befestigen Sie das Gerät am Rack, indem Sie die „Montagelaschen" mit den Montageschrauben (mitgeliefert) am Rack-Rahmen befestigen.

4. Schließen Sie die Stromversorgung mit einer der folgenden Methoden an:
   - **Gleichstromversorgung** – Schließen Sie das Gleichstromkabel an den Sensor an, indem Sie den 6-poligen 12–36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen. Schließen Sie dann das andere Ende des Kabels an eine Gleichstromquelle an.



   - **Wechselstromversorgung** – Schließen Sie die Wechselstromversorgung an den Sensor an, indem Sie den 6-poligen 12–36-V-DC-Phoenix-Contact-Stecker in die Seite des Sensorgeräts stecken und die integrierten Schrauben oben und unten am Stecker festziehen.

Stecken Sie dann das eine Ende des Wechselstromkabels (mitgeliefert) in das Netzteil und das andere Ende in eine Netzsteckdose.

Schritt 2 – Verbinden des Sensors mit dem Netzwerk

Der Tenable.ot Sensor wird verwendet, um Netzwerk-Traffic zu erfassen und an die Tenable.ot Appliance weiterzuleiten. Um eine Netzwerküberwachung durchzuführen, müssen Sie das Gerät an einen Spiegelport am Netzwerk-Switch anschließen, der mit den relevanten Controllern/SPS verbunden ist.

Um den Sensor zu verwalten, müssen Sie das Gerät mit einem Netzwerk verbinden (kann ein anderes Netzwerk sein als das für die Netzwerküberwachung verwendete sein).

➡ So verbinden Sie den Tenable.ot Rack-Montage-Sensor mit dem Netzwerk:

1. Schließen Sie am Tenable.ot Sensor das Ethernet-Kabel (mitgeliefert) an **Port 1** an.
2. Schließen Sie das Kabel an einen regulären Anschluss am Netzwerk-Switch an.
3. Schließen Sie am Gerät ein weiteres Ethernet-Kabel (mitgeliefert) an **Port 2** an.
4. Schließen Sie das Kabel an einen Spiegelport am Netzwerk-Switch an.

➡ So verbinden Sie den konfigurierbaren Tenable.ot Sensor mit dem Netzwerk:

1. Schließen Sie am Tenable.ot Sensor das Ethernet-Kabel (mitgeliefert) an **Port 1** an.
2. Schließen Sie das Kabel an einen regulären Anschluss am Netzwerk-Switch an.
3. Schließen Sie am Gerät ein weiteres Ethernet-Kabel (mitgeliefert) an **Port 3** an.
4. Schließen Sie das Kabel an einen Spiegelport am Netzwerk-Switch an.

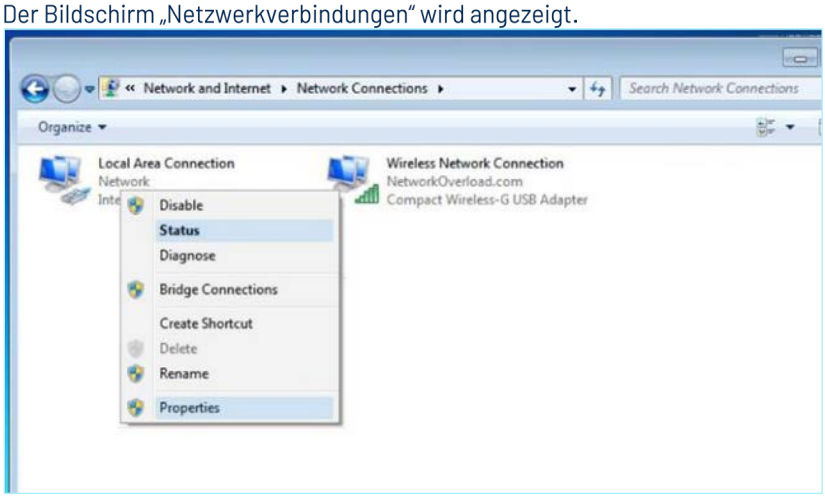
Schritt 3 – Aufrufen des Sensor-Setup-Assistenten

➡ **So loggen Sie sich bei der Verwaltungskonsole ein:**

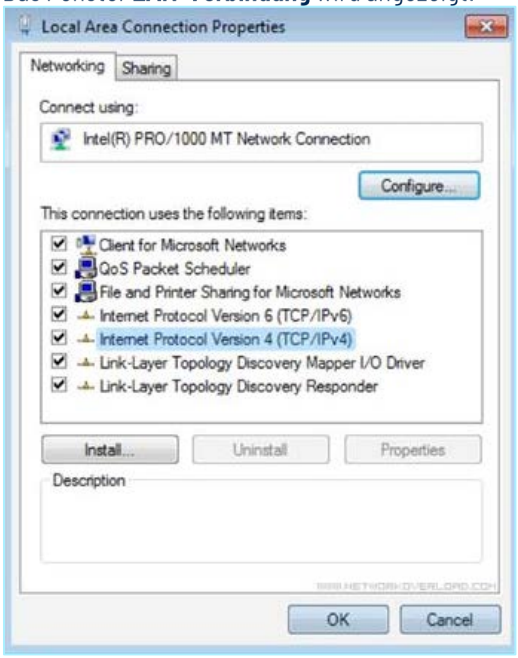
1. Führen Sie einen der folgenden Schritte aus:
   - Verbinden Sie die Workstation der Verwaltungskonsole (z. B. PC, Laptop usw.) über das Ethernet-Kabel direkt mit Port 1 des Tenable.ot Sensors ODER
   - Verbinden Sie die Workstation der Verwaltungskonsole mit dem Netzwerk-Switch.
2. Stellen Sie sicher, dass die Workstation der Verwaltungskonsole Teil desselben Subnetzes ist wie der Tenable.ot Sensor (d. h. 192.168.1.5) oder an das Gerät umgeleitet werden kann.
3. Verwenden Sie das folgende Verfahren, um eine statische IP-Adresse einzurichten (Sie müssen eine statische IP einrichten, um eine Verbindung zum Tenable.ot Sensor herzustellen):
   a. Gehen Sie zu **Netzwerk und Internet** > **Netzwerk- und Freigabecenter** > **Adaptereinstellungen ändern**.

Die Navigation kann bei den verschiedenen Windows-Versionen leicht variieren.

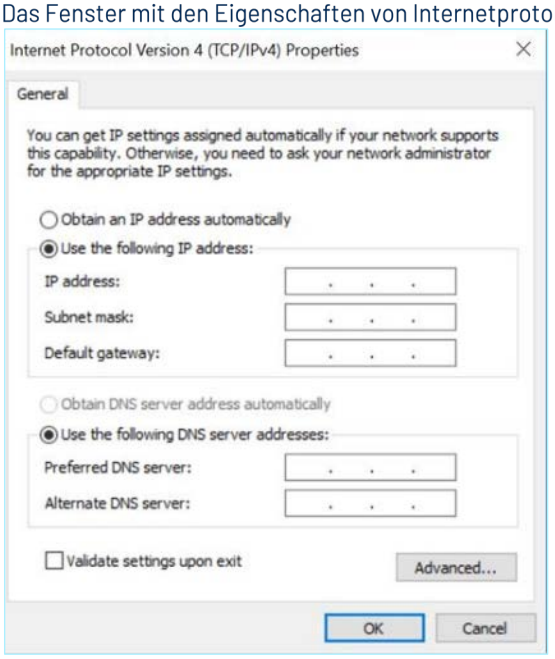
Der Bildschirm „Netzwerkverbindungen“ wird angezeigt.



   b. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung** und wählen Sie **Eigenschaften**. Das Fenster **LAN-Verbindung** wird angezeigt.



c. Wählen Sie **Internetprotokoll, Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.
Das Fenster mit den Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) wird angezeigt.



d. Wählen Sie „Folgende IP-Adresse verwenden“ aus.
e. Geben Sie im Feld „IP-Adresse“ *192.168.1.10* ein.
f. Geben Sie im Feld „Subnetzmaske“ *255.255.255.0* ein.
g. Klicken Sie auf **OK**.
Die neuen Einstellungen werden übernommen.

4. Navigieren Sie im Chrome-Webbrowser zu „192.168.1.5“.

> Auf die Benutzeroberfläche kann nur über einen Chrome-Browser zugegriffen werden. Zudem muss die neueste Version von Chrome verwendet werden.

Der Begrüßungsbildschirm des Setup-Assistenten wird geöffnet.

5. Klicken Sie auf **Setup starten**.
Der Setup-Assistent wird geöffnet und zeigt die Seite **Benutzerinformationen** an.

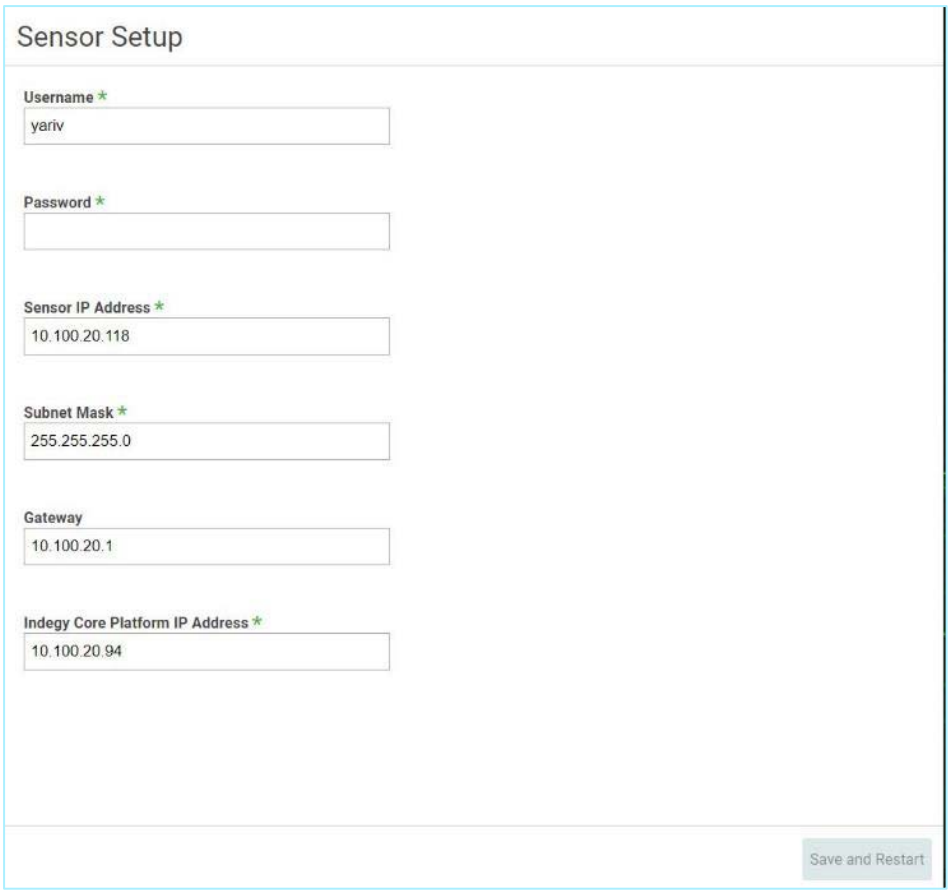
Schritt 4 – Sensor-Setup-Assistent

Der Setup-Assistent von Tenable.ot führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

Wenn Sie die Konfiguration später ändern möchten, können Sie dies im Bildschirm **Einstellungen** in der Verwaltungskonsole (UI) tun.

So richten Sie den Sensor ein:

1. Klicken Sie im Begrüßungsbildschirm auf **Setup starten** (Start Setup).
   Der Setup-Bildschirm wird angezeigt.



2. Geben Sie im Feld **Benutzername** einen Benutzernamen ein, der für den Login beim System verwendet werden soll. Der Benutzername kann bis zu 12 Zeichen lang sein und darf nur Kleinbuchstaben und Zahlen enthalten.
3. Geben Sie im Feld **Passwort** ein Passwort ein, das für das Einloggen beim System verwendet werden soll. Mindestanforderungen für Passwörter:
   - 12 Zeichen
   - Ein Großbuchstabe
   - Ein Kleinbuchstabe
   - Eine Zahl
   - Ein Sonderzeichen
4. Geben Sie im Feld **Passwort erneut eingeben** das gleiche Passwort erneut ein.

5. Geben Sie im Feld **Sensor-IP-Adresse** (Sensor IP Address) eine IP-Adresse (innerhalb des Netzwerk-Subnetzes) ein, die auf den Tenable.ot Sensor angewendet werden soll. Es wird dringend empfohlen, die Standard-IP-Adresse zu ändern.
6. Geben Sie im Feld **Subnetzmaske** die Subnetzmaske des Netzwerks ein.
7. Wenn Sie ein Gateway einrichten möchten (optional), geben Sie die Gateway-IP für das Netzwerk in das Feld **Gateway** ein.
8. Geben Sie im Feld **IP-Adresse** die IP-Adresse der Tenable.ot-Plattform ein.
9. Klicken Sie auf **Speichern und neu starten** (Save and Restart).
   Der Sensor führt einen Neustart durch:

10. Nach dem Neustart wird der Netzwerk-Traffic an die Tenable.ot-Plattform weitergeleitet. Wenn Sie die Konfiguration ändern möchten, können Sie sich mit der konfigurierten IP-Adresse und den von Ihnen konfigurierten Zugangsdaten beim Sensor einloggen:

ANHANG 2 – SAML-INTEGRATION FÜR AZURE ACTIVE DIRECTORY

Tenable.ot unterstützt die Integration mit Microsoft Azure Active Directory über das SAML-Protokoll. Dies ermöglicht es Azure-Benutzern, die Tenable.ot zugewiesen wurden, sich über SSO bei Tenable.ot einzuloggen. Mithilfe der Gruppenzuordnung können Sie Rollen in Tenable.ot entsprechend den Gruppen zuzuweisen, denen Benutzer in Azure zugewiesen sind.

Einrichten der Integration

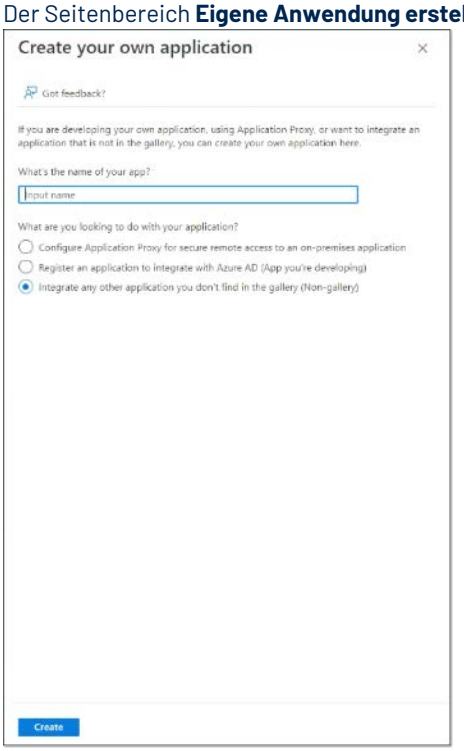
In diesem Abschnitt wird der vollständige Ablauf für die Einrichtung einer Single Sign-on (SSO)-Integration für Tenable.ot mit Microsoft Azure Active Directory erläutert. Die Konfiguration beinhaltet die Einrichtung der Integration, indem Sie eine Tenable.ot-Anwendung in Azure Active Directrory erstellen, Informationen über Ihre erstellte Tenable.ot-Anwendung eingeben, das Zertifikat Ihres Identitätsanbieters auf die SAML-Seite in Tenable.ot-Seite hochladen und dann Gruppen von Ihrem Identitätsanbieter zu Benutzergruppen in Tenable.ot zuordnen.

Um die Konfiguration einzurichten, müssen Sie sowohl bei Azure Active Directory als auch bei Tenable.ot als Administrator eingeloggt sein.

Schritt 1 – Erstellen der Tenable-Anwendung in Azure

➡ So erstellen Sie die Tenable-Anwendung in Azure:

1. Gehen Sie in **Microsoft Azure Active Directory** zu **Azure Active Directory** > **Unternehmensanwendungen**, klicken Sie auf **+ Neue Anwendung**, um das Dialogfeld **Azure AD-Katalog durchsuchen** anzuzeigen, und klicken Sie auf **+ Eigene Anwendung erstellen.**
   Der Seitenbereich **Eigene Anwendung erstellen** wird angezeigt.



2. Geben Sie im Feld **Wie lautet der Name der App?** einen Namen für die Anwendung ein (z. B. Tenable_OT) und wählen Sie **Hiermit wird eine beliebige andere Anwendung integriert, die Sie nicht im Katalog finden (Nicht-Katalog)** aus (standardmäßig deaktiviert). Klicken Sie dann auf **Erstellen**, um die Anwendung hinzuzufügen.

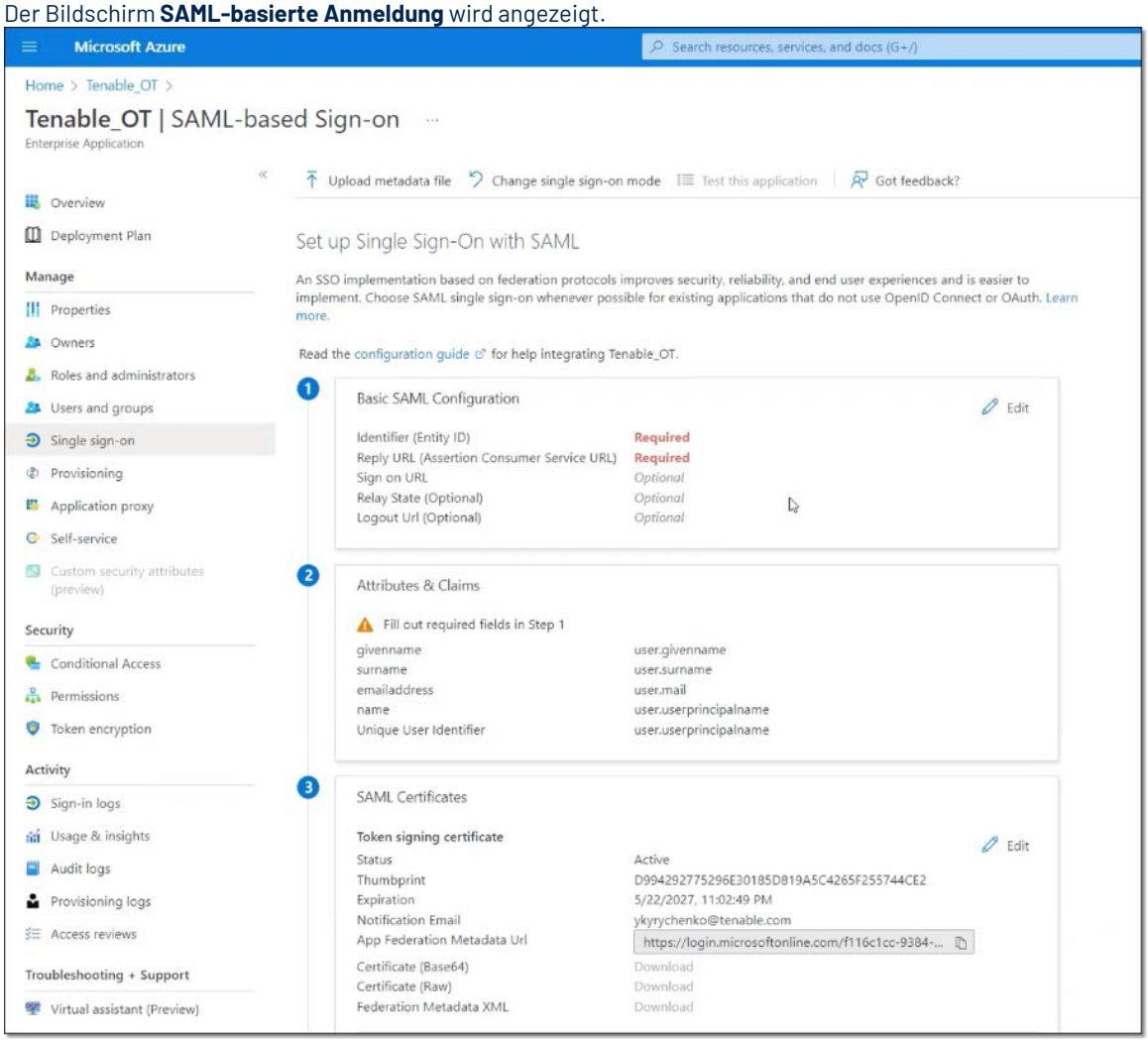
Schritt 2 – Erstkonfiguration

In diesem Schritt erfolgt die Erstkonfiguration der Tenable.ot-Anwendung in Azure. Dies umfasst das Erstellen temporärer Werte für die Werte „Bezeichner" und „Antwort-URL" der grundlegenden SAML-Konfiguration, um das erforderliche Zertifikat herunterladen zu können.

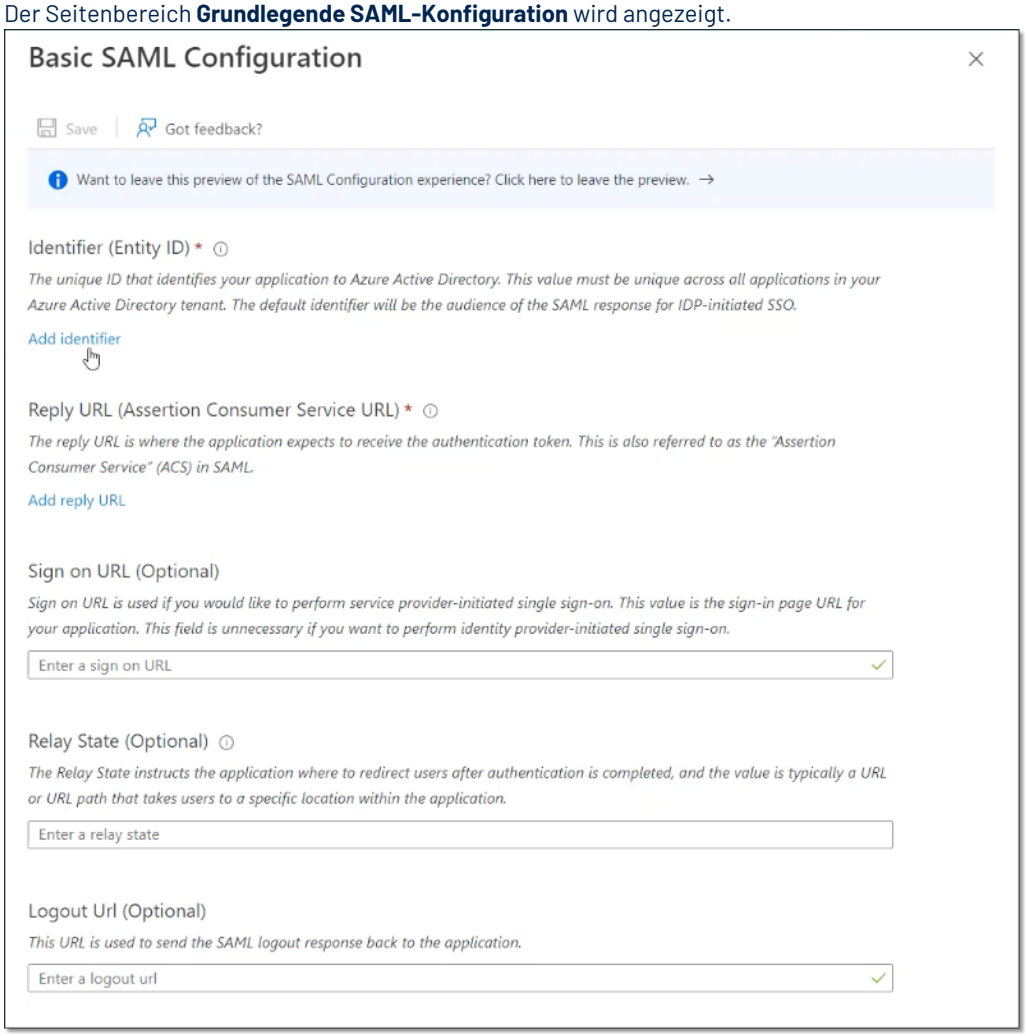
> Nur die in dieser Vorgehensweise angegebenen Felder müssen konfiguriert werden. Für andere Felder können die Standardwerte übernommen werden.

So führen Sie die Erstkonfiguration durch:

1. Klicken Sie im Navigationsmenü **Microsoft Azure Active Directory** auf **Einmaliges Anmelden** und wählen Sie dann **SAML** als Methode für einmaliges Anmelden (Single Sign-On, SSO) aus.
   Der Bildschirm **SAML-basierte Anmeldung** wird angezeigt.



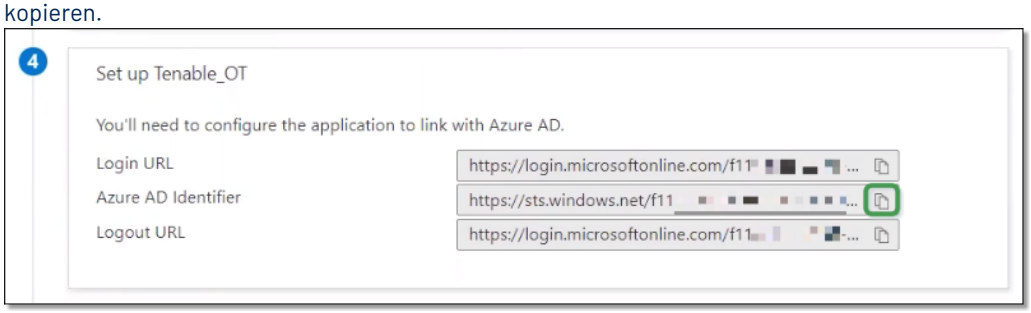
2. Klicken Sie in Abschnitt 1, **Grundlegende SAML-Konfiguration**, auf „Bearbeiten“.
Der Seitenbereich **Grundlegende SAML-Konfiguration** wird angezeigt.



3. Geben Sie im Feld **Bezeichner (Entitäts-ID)** eine temporäre ID für die Tenable-Anwendung ein (z. B. tenable_ot).
4. Geben Sie im Feld **Antwort-URL (Assertionsverbraucherdienst-URL)** eine gültige URL ein (z. B. https://tenable.ot).

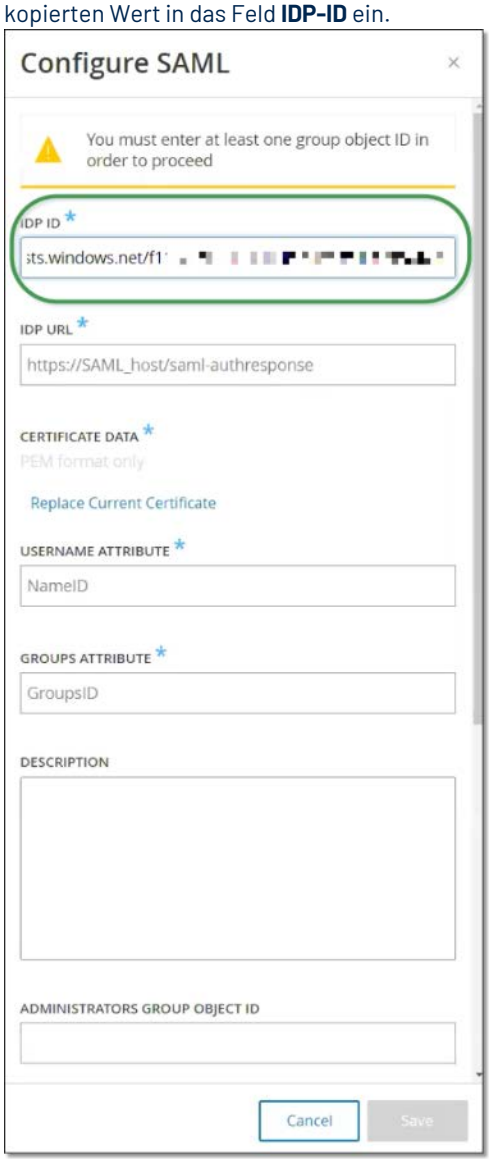
> Sowohl der Bezeichner als auch die Antwort-URL werden später im Konfigurationsprozess geändert.

5. Klicken Sie auf **Speichern**, um die temporären Werte zu speichern und den Seitenbereich **Grundlegende SAML-Konfiguration** zu schließen.
6. Klicken Sie in Abschnitt 4, **Einrichten**, auf das Symbol **Kopieren**, um den **Azure AD-Bezeichner** zu kopieren.



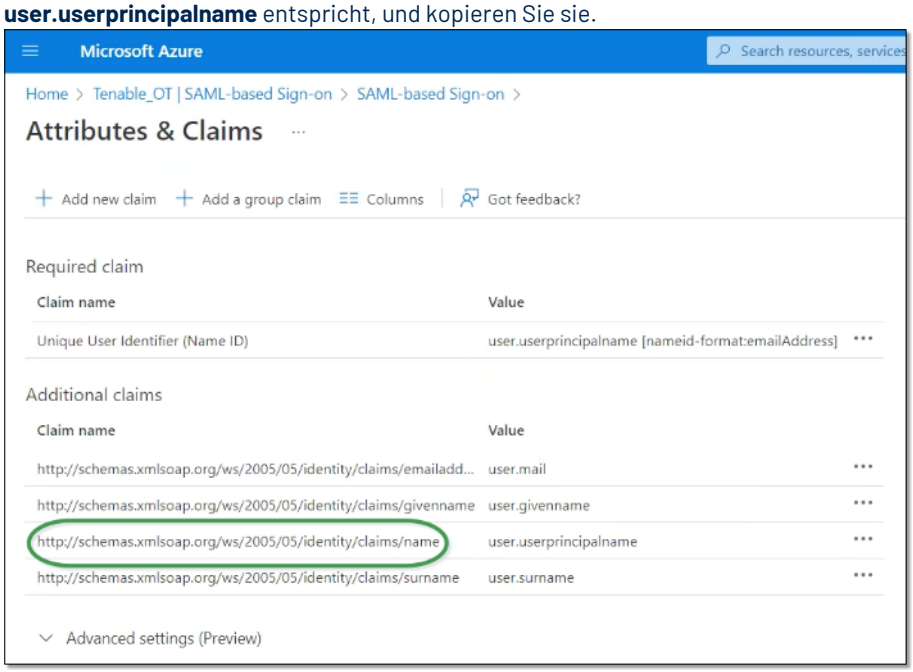
7. Wechseln Sie zur **Tenable.ot**-Konsole und gehen Sie zu **Benutzer und Rollen > SAML**.

8. Klicken Sie auf **Konfigurieren**, um den Seitenbereich **SAML konfigurieren** anzuzeigen, und fügen Sie den kopierten Wert in das Feld **IDP-ID** ein.

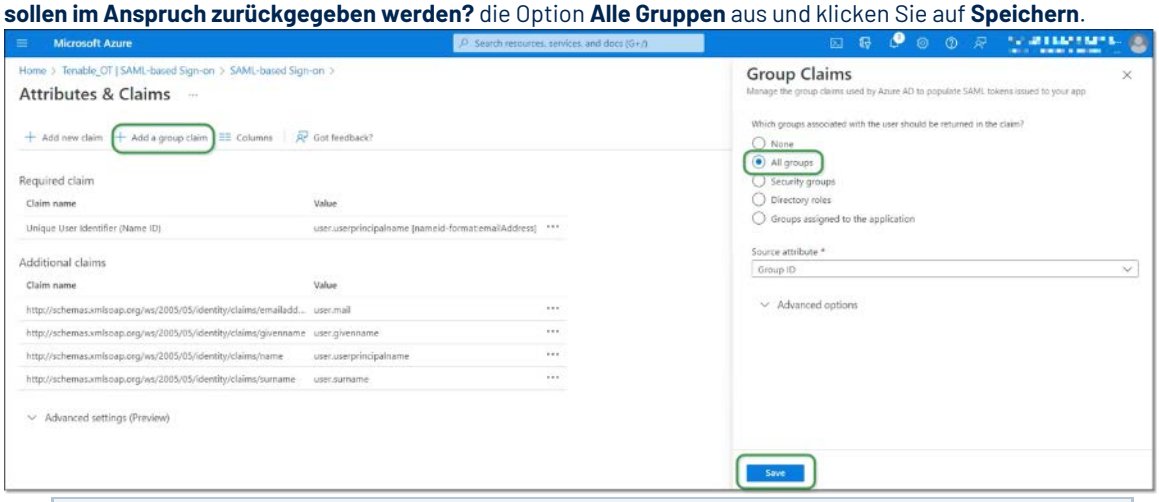


9. Klicken Sie in der **Azure**-Konsole auf das Symbol, um die **Anmelde-URL** zu kopieren.
10. Kehren Sie zur **Tenable.ot**-Konsole zurück und fügen Sie den kopierten Wert in das Feld **IDP-URL** ein.
11. Klicken Sie in der **Azure**-Konsole in Abschnitt 3, **SAML-Zertifikate**, für **Zertifikat (Base64)** auf **Herunterladen**.
12. Kehren Sie zur **Tenable.ot**-Konsole zurück und klicken Sie unter **Zertifikatdaten** auf **Durchsuchen**, navigieren Sie zur Sicherheitszertifikatdatei und wählen Sie sie aus.
13. Klicken Sie in der **Azure**-Konsole in Abschnitt 2, **Attribute & Ansprüche**, auf **Bearbeiten**.

14. Wählen Sie unter **Zusätzliche Ansprüche** die URL unter **Anspruchsname** aus, die dem Wert **user.userprincipalname** entspricht, und kopieren Sie sie.

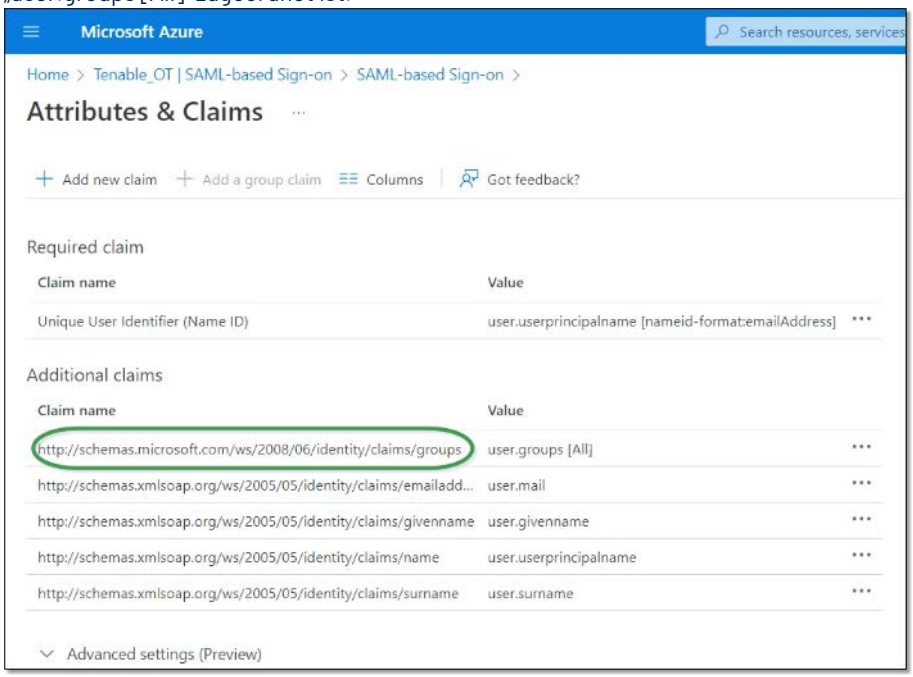


15. Kehren Sie zur **Tenable**-Konsole zurück und fügen Sie diese URL in das Feld **Username-Attribut** ein.
16. Klicken Sie in der Azure-Konsole auf **+ Gruppenanspruch hinzufügen**, um den Seitenbereich **Gruppenansprüche** anzuzeigen. Wählen Sie dann unter **Welche dem Benutzer zugeordneten Gruppen sollen im Anspruch zurückgegeben werden?** die Option **Alle Gruppen** aus und klicken Sie auf **Speichern**.



Wenn die Gruppeneinstellung in Microsoft Azure aktiviert ist, können Sie **Der Anwendung zugewiesene Gruppen** anstelle von **Alle Gruppen** wählen. Azure stellt dann nur die Benutzergruppen bereit, die der Anwendung zugewiesen sind.

17. Markieren und kopieren Sie unter **Zusätzliche Ansprüche** die URL unter **Anspruchsname**, die dem Wert „user.groups [All]“ zugeordnet ist.



18. Kehren Sie zur **Tenable**-Konsole zurück und fügen Sie die kopierte URL in das Feld **Groups-Attribut** ein.
19. Wenn Sie eine Beschreibung der SAML-Konfiguration hinzufügen möchten, geben Sie diese in das Feld **Beschreibung** ein.

Schritt 3 – Zuordnen von Azure-Benutzern zu Tenable-Gruppen

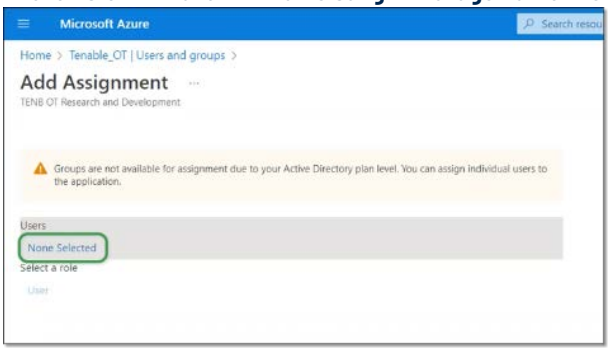
In diesem Schritt werden Azure Active Directory-Benutzer der Tenable.ot-Anwendung zugewiesen. Die jedem Benutzer gewährten Berechtigungen werden festgelegt, indem die Azure-Gruppen, denen die Benutzer zugewiesen sind, einer vordefinierten Tenable.ot-Benutzergruppe zugeordnet werden, die eine zugeordnete Rolle und einen Satz von Berechtigungen hat. Die vordefinierten Benutzergruppen von Tenable.ot sind folgende: *Administratoren*, *Schreibgeschützt* (Benutzer mit reinen Leseberechtigungen), *Sicherheitsanalysten*, *Sicherheitsmanager*, *Site-Operatoren* und *Supervisoren*. Weitere Informationen finden Sie unter **Benutzergruppen**. Jeder Azure-Benutzer muss mindestens einer Gruppe zugewiesen werden, die einer Tenable.ot-Benutzergruppe zugeordnet ist.

Administratorbenutzer, die über SAML eingeloggt sind, werden als externe Administratoren betrachtet und erhalten nicht alle Berechtigungen lokaler Administratoren.

Benutzern, die mehreren Benutzergruppen zugewiesen sind, werden die höchstmöglichen Berechtigungen aus ihren Gruppen gewährt.

So ordnen Sie Azure-Benutzer zu Tenable.ot zu:

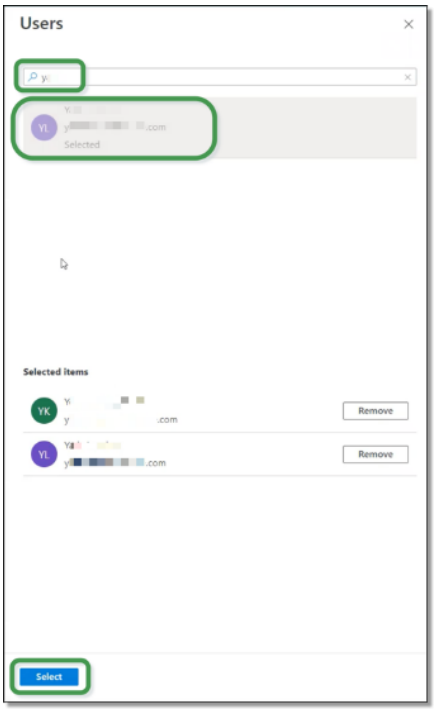
1. Navigieren Sie in **Microsoft Azure** zur Seite **Benutzer und Gruppen** und klicken Sie auf **+ Benutzer/Gruppe hinzufügen**.
2. Klicken Sie im Bildschirm **Zuweisung hinzufügen** unter **Benutzer** auf **Keine ausgewählt**.



Der Seitenbereich **Benutzer** wird angezeigt.

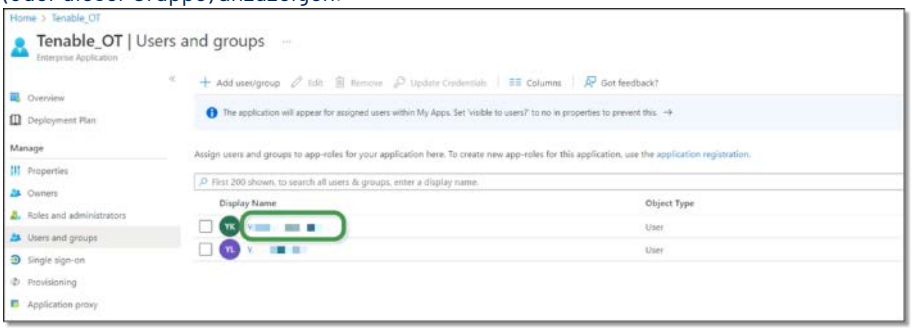
> Wenn die Gruppeneinstellung in Microsoft Azure aktiviert ist und Sie zuvor **Der Anwendung zugewiesene Gruppen** anstelle von „Alle Gruppen“ ausgewählt haben, können Sie Gruppen anstelle von einzelnen Benutzern zuweisen.

3. Suchen Sie nach allen gewünschten Benutzern, und klicken Sie auf sie. Klicken Sie anschließend auf **Auswählen** und dann auf **Zuweisen**, um die Benutzer der Anwendung zuzuweisen.



Die Seite **Benutzer und Gruppen** wird angezeigt.

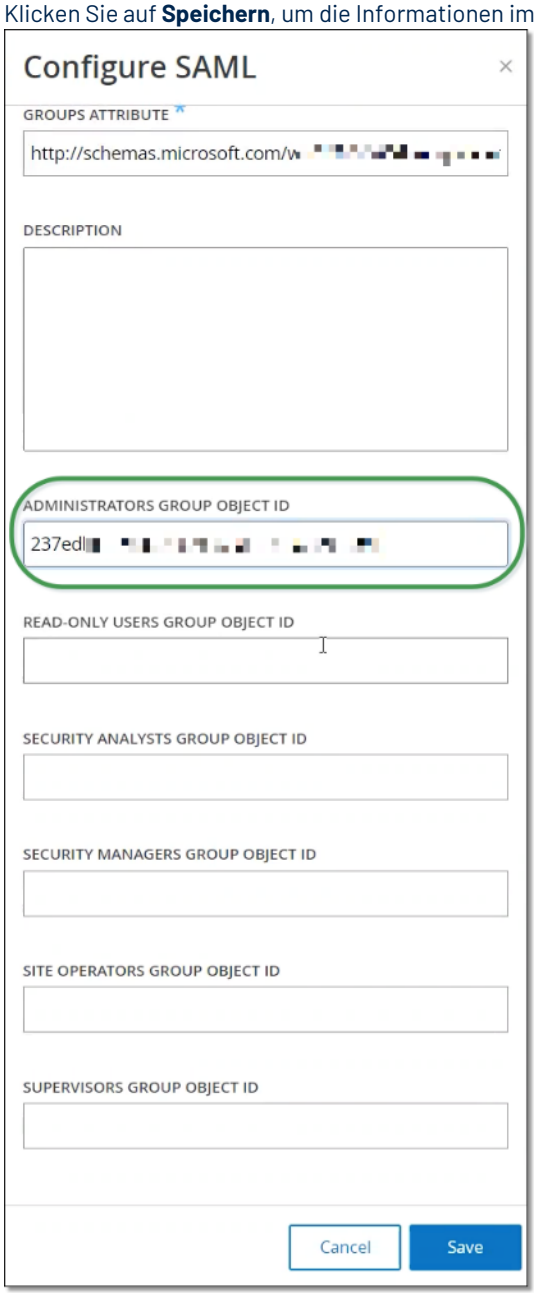
4. Klicken Sie auf den **Anzeigenamen** eines Benutzers (oder einer Gruppe), um das Profil dieses Benutzers (oder dieser Gruppe) anzuzeigen.



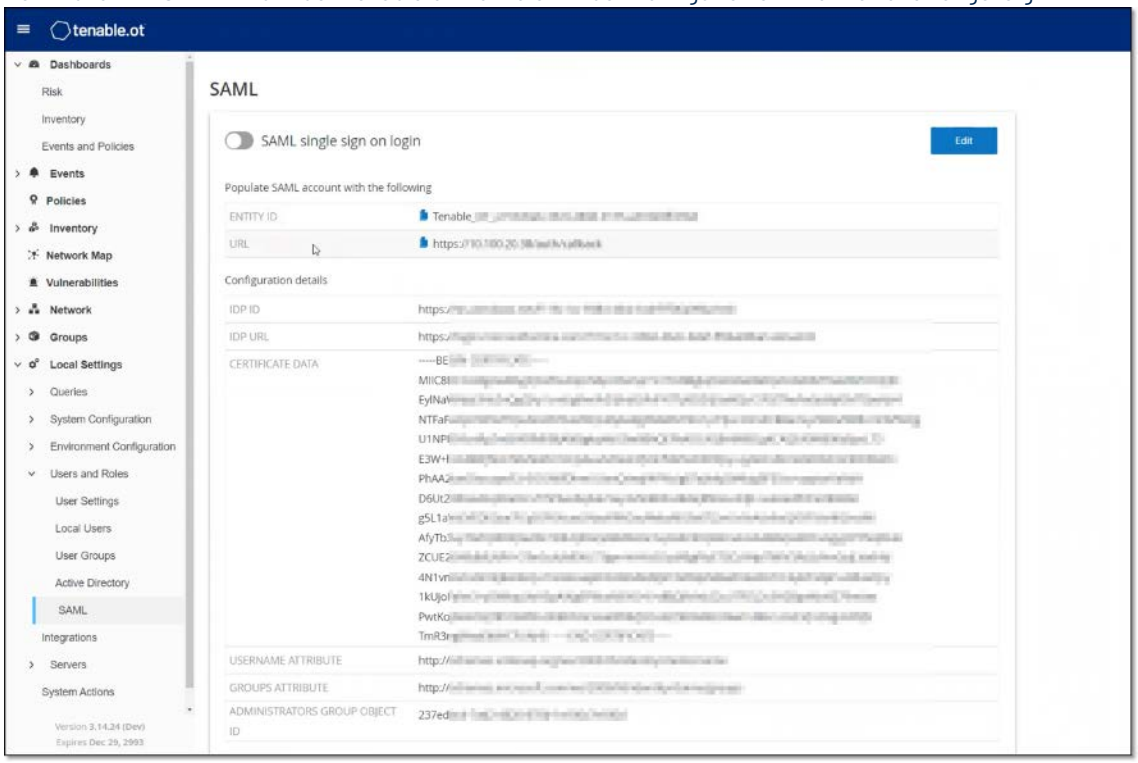
5. Wählen Sie im Bildschirm **Profil** in der linken Navigationsleiste **Gruppen** aus, um den Bildschirm **Gruppen** anzuzeigen.
6. Markieren und kopieren Sie unter **Objekt-ID** den Wert für die Gruppe, die Tenable zugeordnet wird.

7. Kehren Sie zur **Tenable.ot**-Konsole zurück und fügen Sie den kopierten Wert in das Feld der gewünschten **Gruppenobjekt-ID** ein (z. B. Gruppenobjekt-ID für Administratoren).
8. Wiederholen Sie die Schritte 1 bis 7 für jede Gruppe, die Sie einer bestimmten Benutzergruppe in Tenable.ot zuordnen möchten.

9. Klicken Sie auf **Speichern**, um die Informationen im Seitenbereich zu speichern und diesen zu schließen.



Der Bildschirm **SAML** wird in der Tenable.ot-Konsole mit den konfigurierten Informationen angezeigt.



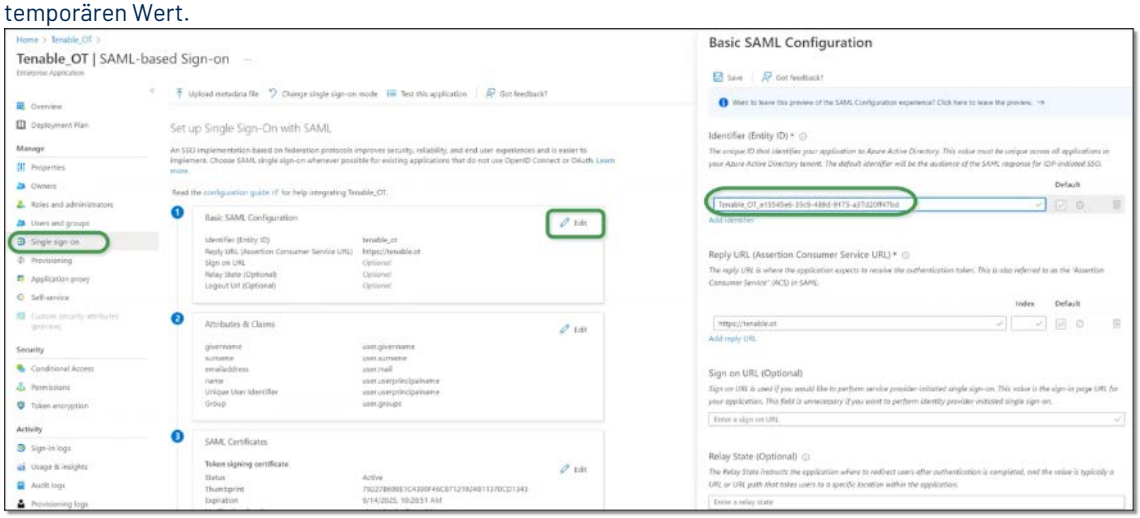
Schritt 4 – Abschließen der Konfiguration in Azure

➡ So schließen Sie die Konfiguration in Azure ab:

1. Klicken Sie im Tenable.ot-Bildschirm **SAML** unter **Entitäts-ID** auf das Symbol „Kopieren“.

2. Wechseln Sie zum **Azure**-Bildschirm und klicken Sie im Navigationsmenü auf der linken Seite auf **Einmaliges Anmelden**, um die Seite **SAML-basierte Anmeldung** zu öffnen.
3. Klicken Sie in Abschnitt 1, **Grundlegende SAML-Konfiguration**, auf **Bearbeiten** und fügen Sie den kopierten Wert in das Feld **Bezeichner (Entitäts-ID)** ein. Ersetzen Sie dabei den zuvor eingegebenen

temporären Wert.



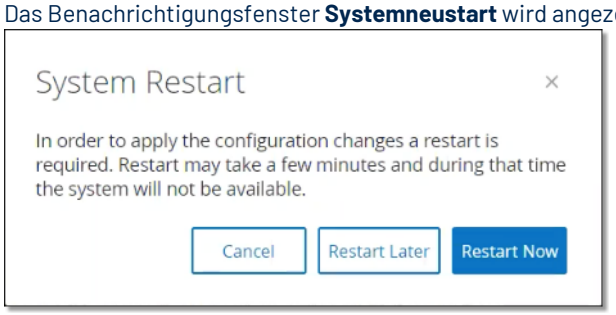
4. Kehren Sie zum Tenable.ot-Bildschirm **SAML** zurück und klicken Sie unter **Entitäts-ID** auf das Symbol „Kopieren“.
5. Fügen Sie in der **Azure**-Konsole im Seitenbereich **Grundlegende SAML-Konfiguration** unter **Antwort-URL (Assertionsverbraucherdienst-URL)** die kopierte URL ein. Ersetzen Sie dabei die zuvor eingegebene temporäre URL.
6. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern, und schließen Sie den Seitenbereich. Die Konfiguration ist abgeschlossen und die Verbindung wird im Bildschirm **Azure-Unternehmensanwendungen** angezeigt.

Schritt 5 – Aktivieren der Integration

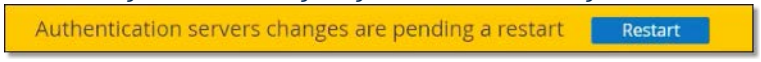
Um die SAML-Integration zu aktivieren, muss Tenable.ot neu gestartet werden. Der Benutzer kann das System sofort oder später neu starten.

So aktivieren Sie die Integration:

1. Klicken Sie in der Tenable.ot-Konsole im Bildschirm **SAML** auf den Umschalter **SAML Single Sign-On-Login**, um ihn auf **EIN** zu stellen.
   Das Benachrichtigungsfenster **Systemneustart** wird angezeigt.



2. Klicken Sie auf **Jetzt neu starten**, um das System sofort neu zu starten und die SAML-Konfiguration anzuwenden, oder klicken Sie auf **Später neu starten**, um die Anwendung der SAML-Konfiguration auf den nächsten Neustart des Systems zu verschieben. Wenn Sie sich für einen späteren Neustart entscheiden, wird das folgende Banner angezeigt, bis der Neustart abgeschlossen ist:



Einloggen mit SSO

Nach dem Neustart enthält das **Tenable.ot**-Login-Fenster unter der Schaltfläche „Einloggen“ einen neuen Link **Über SSO einloggen**. Azure-Benutzer, die Tenable.ot zugewiesen wurden, können sich mit ihrem Azure-Konto bei Tenable.ot einloggen.

So loggen Sie sich mit SSO ein:

1. Klicken Sie im Login-Bildschirm von **Tenable.ot** auf den Link **Über SSO einloggen**.

Wenn Sie bereits bei Azure eingeloggt sind, gelangen Sie direkt zur Tenable.ot-Konsole, andernfalls werden Sie zur Login-Seite von Azure weitergeleitet.
Benutzer mit mehr als einem Konto werden auf die Microsoft-Seite **Konto auswählen** umgeleitet, auf der sie das gewünschte Konto für die Anmeldung auswählen können.