Tenable OT Security 3.17 Benutzerhandbuch

Letzte Überarbeitung: 24 Juni 2025

Inhalt

Willkommen bei Tenable OT Security

Tenable OT Security (OT Security) (früher 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 OT Security maximieren die Transparenz, Sicherheit und Kontrolle Ihrer Betriebsumgebung.

OT Security bietet umfassende Sicherheitstools und Berichte für IT-Sicherheitspersonal und OT-Ingenieure. Es bietet einen Einblick in konvergente IT/OT-Segmente und ICS-Aktivitäten und macht auf Situationen an allen Sites und bei ihren jeweiligen OT-Assets aufmerksam – von Windows-Servern bis hin zu SPS-Backplanes – in einer zentralen, einheitlichen Ansicht.

OT Security weist die folgenden wichtigen Leistungsmerkmale auf:

- **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. OT Security lässt sich auch nativ in 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, in dem all Ihre Sicherheitsprodukte als Einheit zusammenarbeiten können, um Ihre Umgebung zu schützen.
- **Bedrohungserkennung und -entschärfung** – OT Security 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** – OT Security nutzt patentierte Technologie und bietet einen 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 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 OT Security mithilfe

von Predictive Prioritization Schwachstellen- und Risikostufen für jedes Asset in Ihrem ICS-Netzwerk (Industrial Control Systems, industrielle Steuerungssysteme). Diese Berichte enthalten Risikobewertungen und detaillierte Einblicke sowie Vorschläge zur Risikominderung.

- **Konfigurationskontrolle** – OT Security bietet einen detaillierten Verlauf der Änderungen an der Gerätekonfiguration im Zeitverlauf, einschließlich spezifischer Kontaktplan-Segmente, Diagnosepuffer, Tag-Tabellen und mehr. Auf diese Weise können Administratoren einen Backup-Snapshot mit dem „letzten als funktionierend bekannten Zustand" für eine schnellere Wiederherstellung und Einhaltung von Branchenvorschriften erstellen.

Tipp: Das *Tenable OT Security-Benutzerhandbuch* und die Benutzeroberfläche sind auf Englisch, Japanisch, Deutsch, Französisch und vereinfachtem Chinesisch verfügbar. Informationen zum Ändern der Sprache der Benutzeroberfläche finden Sie unter Lokale Einstellungen.

Weitere Informationen zu Tenable OT Security finden Sie in den folgenden Materialien für Kundenschulungen:

- Einführung in Tenable OT Security (Tenable University)

Erste Schritte mit OT Security

Befolgen Sie die unter Erste Schritte mit OT Security genannten Schritte, um mit OT Security zu beginnen.

OT Security-Technologien

Die umfassende OT Security-Lösung umfasst zwei zentrale Erfassungstechnologien:

- **Netzwerkerkennung** – Die Netzwerkerkennungstechnologie von OT Security ist eine passive Deep-Packet Inspection Engine, die 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 OT Security überwacht Geräte im Netzwerk, indem sie regelmäßig die Metadaten von Kontrollgeräten im ICS-Netzwerk abfragt. Diese Funktionalität verbessert die Fähigkeit von OT Security, 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 sicher und hat keine Auswirkungen auf die Geräte. Abfragen können regelmäßig nach einem vordefinierten Zeitplan oder nach Bedarf durch den Benutzer ausgeführt werden.

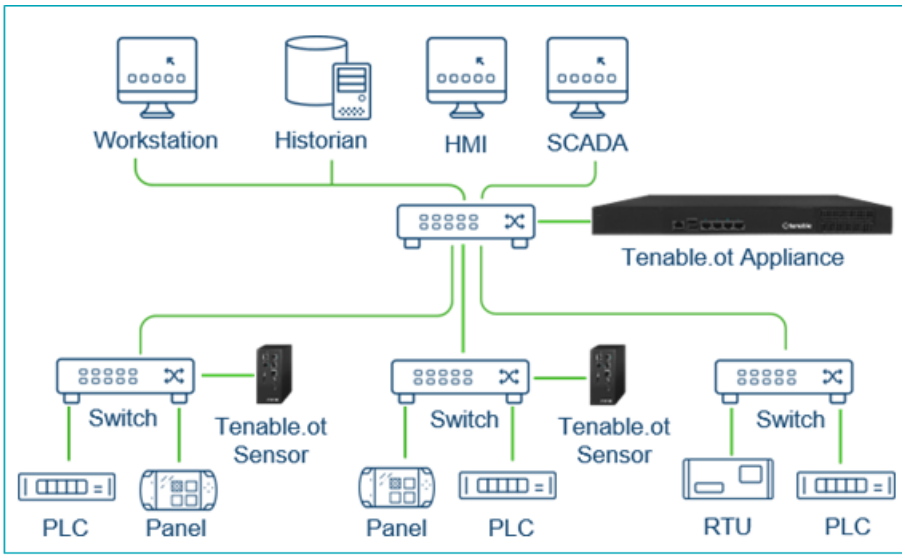
Lösungsarchitektur

Komponenten der OT Security-Plattform

> **Hinweis**: In diesem Dokument wird die OT Security Appliance als ICP (Industrial Core Platform) bezeichnet.

Die OT Security-Lösung setzt sich aus diesen Komponenten zusammen:

- **ICP** (**OT Security 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 vom Tenable OT Security Sensor (OT Security Sensor). Die ICP-Appliance führt sowohl die Netzwerkerkennung als auch aktive Abfragen aus.
- **OT Security Sensoren** – Hierbei handelt es sich um kleine Geräte, die in Netzwerksegmenten von Interesse bereitgestellt werden, bis zu einem Sensor pro Managed Switch. OT Security Sensoren bieten einen vollständigen Einblick in diese Netzwerksegmente, indem sie den gesamten Traffic erfassen, die Daten komprimieren und die Informationen dann an die OT Security Appliance übermitteln. Sie können Sensoren der Version 3.14 und höher auch so konfigurieren, dass sie aktive Abfragen an die Netzwerksegmente senden, in denen sie bereitgestellt werden.



Netzwerkkomponenten

OT Security unterstützt die Interaktion mit den folgenden Netzwerkkomponenten:

- **OT Security-Benutzer (Verwaltung)** – Sie können Benutzerkonten erstellen, um den Zugriff auf die OT Security-Verwaltungskonsole zu steuern. Sie können mit einem Browser (Google Chrome) über Secure Socket-Layer-Authentifizierung (HTTPS) auf die Verwaltungskonsole zugreifen.

Hinweis: Der Zugriff auf die OT Security-Benutzeroberfläche ist nur mit der neuesten Version von Chrome möglich.

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

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

Tenable OT Security – Hardwarespezifikationen

ICP-Spezifikationen

Im Folgenden finden Sie die Spezifikationen für die OT Security Hardware-Appliances für die Industrial Core Platform (ICP):

IEI-ICP

Kategorie	IEI-ICP

	
CPU	Xeon®D-2177
Kerne	14
RAM	64 GB
Speicher	256 GB SSD 800 GB NVMe 2 TB HDD
Netzwerk (Kupfer-Ethernet)	8 x 2,5 Gbit/s
Netzwerk (Glasfaser-Ethernet)	4 x 10 GB SFP+
Stromversorgung	Redundant, 110–220 V
Formfaktor	1 HE, halbe Tiefe
Abmessungen (BxHxT)	430 x 426 x 44.2 mm
Gewicht	7 kg
Betriebstemperatur	0 bis 40 °C (32 bis 104 °F)
Lagertemperatur	-10 bis 50 °C (14 bis 122 °F)
Relative Luftfeuchtigkeit	5 % bis 90 %, nicht kondensierend
Zertifizierungen	CE/FCC/RoHS, Klasse A CB, CCC, UL, RCM, NOM
Max. SPAN-Durchsatz	500 Mbit/s

Lanner-ICP

Kategorie	Lanner-ICP

	
CPU	Intel®Xeon™D-1577, 1,3 GHz
Kerne	16
RAM	64 GB
Speicher	1 TB SSD 2 TB SSD
Netzwerk (Kupfer-Ethernet)	4 x 1 Gbit/s
Netzwerk (Glasfaser-Ethernet)	N/A
Stromversorgung	Eine, 110–220 V
Formfaktor	1 HE, halbe Tiefe
Abmessungen (BxHxT)	438 x 44 x 321 mm 17.2 x 1.73 x 12.64 in
Gewicht	7.5 Kg
Betriebstemperatur	0 bis 40 °C (32 bis 104 °F)
Lagertemperatur	-20 bis 70 °C (-4 bis 158 °F)
Relative Luftfeuchtigkeit	5 % bis 90 %, nicht kondensierend
Zertifizierungen	CE/FCC-Klasse A, RoHS
Max. SPAN-Durchsatz	500 Mbit/s

Lenovo-ICP

Kategorie	Lenovo-ICP

	
CPU	Intel®Xeon™D-2183dIT, 2,0 GHz
Kerne	16
RAM	64 GB
Speicher	1 TB SATA M.2 2 TB SATA M.2
Netzwerk (Kupfer-Ethernet)	6 x 1 Gbit/s
Netzwerk (Glasfaser-Ethernet)	2 x 10 Gbit/s SFP+
Stromversorgung	Redundant, 2 x 240-W-AC-Netzteil
Formfaktor	1 HE, halbe Tiefe
Abmessungen (BxHxT)	209 x 43 x 376 mm 8.2 x 1.7 x 14.8 in
Gewicht	3.6 Kg
Betriebstemperatur	5 bis 45 °C (41 bis 113 °F)
Lagertemperatur	-20 bis 60 °C (-4 bis 140 °F)
Relative Luftfeuchtigkeit	8 % bis 90 %, nicht kondensierend
Zertifizierungen	CE/FCC/RoHS, Klasse A CB, CCC, UL, RCM, NOM
Max. SPAN-Durchsatz	500 Mbit/s

Dell-ICP-XL

Kategorie	Dell-ICP-XL

	
CPU	2 x Xeon®Silver 4314
Kerne	2 x 16
RAM	256 GB
Speicher	960 GB SSD SAS FIPS-140 SED 960 GB SSD SAS FIPS-140 SED 2 x 2,4 TB SAS HDD FIPS-140 SED **Hinweis**: Die Hardware ist vollständig verschlüsselt und FIPS-140-konform.
Netzwerk (Kupfer)	6 x 1 Gbit/s
Netzwerk (Glasfaser)	2 x 10 Gbit/s SFP+
Stromversorgung	Redundant, 110–220 V, 165 W
Formfaktor	1 HE, volle Tiefe
Abmessungen (BxHxT)	Höhe: 42,8 mm (1,69 in) x Breite*: 482,0 mm (18,98 in) x Tiefe*: 698 mm/ (27,5 in) * Maße einschließlich Blende.
Gewicht	22 kg
Betriebstemperatur	0 bis 40 °C (32 bis 104 °F)
Lagertemperatur	-10 bis 50 °C (14 bis 122 °F)
Relative Luftfeuchtigkeit	5 % bis 90 %, nicht kondensierend
Zertifizierungen	CE/FCC/RoHS CB, CCC, UL, RCM, NOM

Max. SPAN-Durchsatz	1 Gbit/s

IEI-ICP-Mini

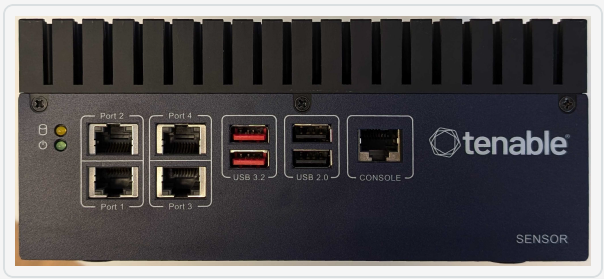
Kategorie	IEI-ICP-Mini
	
CPU	Intel®Core™i7-1185G7E, 1,8 GHz
Kerne	4
RAM	32 GB
Speicher	480 GB SSD
Netzwerk (Kupfer)	4 x 2,5 Gbit/s
Netzwerk (Glasfaser)	N/A
Stromversorgung	Verteiler, 12–28 VDC
Formfaktor	DIN-Schiene
Abmessungen (mm)	150 x 190 x 81 mm
Gewicht	1,9 kg
Betriebstemperatur	0 bis 40 °C (32 bis 104 °F)
Lagertemperatur	-10 bis 50 °C (14 bis 122 °F)
Relative Luftfeuchtigkeit	10 % bis 95 %, nicht kondensierend
Zertifizierung	CE/FCC/RoHS, Klasse A CB, CCC, UL, RCM, NOM

Max. SPAN-Durchsatz	150 Mbit/s

Sensorspezifikationen

IEI-Sensor

Im Folgenden finden Sie die Spezifikationen für die OT Security Hardware-Appliances für Sensoren:

Kategorie	IEI-Sensor (4 Ports)
	
CPU	Celeron 630S5E (2 x 1,8 GHz)
Kerne	2
RAM	4 GB
Speicher	128 GB
Netzwerk (Kupfer)	4 x 2,5 Gbit/s
Netzwerk (Glasfaser)	N/A
Stromversorgung	Verteiler, 12–28 VDC
Formfaktor	DIN-Schiene
Abmessungen (BxHxT) (mm)	150 x 190 x 81 mm
Gewicht	1,9 kg
Betriebstemperatur	0 bis 40 °C (32 bis 104 °F)
Lagertemperatur	-10 bis 50 °C (14 bis 122 °F)
Relative Luftfeuchtigkeit	10 % bis 95 %, nicht kondensierend

Zertifizierung	CE-Klasse A, FCC-Klasse A, RoHS-Klasse A CB, CCC, UL, RCM, NOM
Max. SPAN-Durchsatz	N/A

Lanner-Sensor

Kategorie	Lanner-Sensor
	
CPU	Intel®Atom™E3845, 1,91 GHz
Kerne	4
RAM	4 GB
Speicher	64 GB SSD
Netzwerk (Kupfer)	5 x 1 Gbit/s
Netzwerk (Glasfaser)	N/A
Stromversorgung	Verteiler, 12–28 VDC
Formfaktor	DIN-Schiene
Abmessungen (BxHxT)	78 x 146 x 127 mm 3 x 5.75 x 5 in
Gewicht	1,25 kg
Betriebstemperatur	-40 bis 70 °C (-40 bis 158 °F)
Lagertemperatur	-40 bis 85 °C (-40 bis 185 °F)

Relative Luftfeuchtigkeit	5 % bis 95 %, nicht kondensierend
Zertifizierungen	CE/FCC-Klasse A, RoHS
Max. SPAN-Durchsatz	N/A

Lenovo-Sensor

Kategorie	Lenovo-Sensor
	
CPU	Intel®Core™13-8145UE, 2,2 GHz
Kerne	2
RAM	8 GB
Speicher	128 GB SATA M.2
Netzwerk (Kupfer)	2 x 1Gbit/s
Netzwerk (Glasfaser)	N/A
Stromversorgung	36 W; 2/6-poliger Phoenix Contact-Steckverbinder mit Push-Lock oder externes 36-W-Netzteil, 100–240 V
Formfaktor	Extra kleiner Formfaktor (ESFF)
Abmessungen (BxHxT)	179 x 88 x 34.5 mm 7.05 x 3.46 x 1.36 in
Gewicht	0,72 kg
Betriebstemperatur	0 bis 50 °C (32 bis 122 °F)
Lagertemperatur	-40 bis 60 °C (-40 bis 140 °F)
Relative Luftfeuchtigkeit	20 % bis 80 %, nicht kondensierend

Zertifizierungen	RoHS, WEEE, REACH, ErP Lot 3, MIL-STD-810H
Max. SPAN-Durchsatz	N/A

Systemelemente

Assets

Assets sind die Hardwarekomponenten in Ihrem Netzwerk, wie beispielsweise Controller, Engineering-Stationen, Server usw. Die automatisierte Asset-Erfassung, -Klassifizierung und -Verwaltung von OT Security bietet eine genaue 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

OT Security wendet hochentwickelte 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 im Netzwerk, die sich auf das Gerät ausgewirkt haben (gewichtet nach dem Schweregrad des Ereignisses und und wie lange das Ereignis zurückliegt).

  > **Hinweis**: 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 Bedrohungen, die in Ihrem Netzwerk identifiziert wurden (z. B. veraltete Betriebssysteme, Verwendung anfälliger Protokolle, anfällige offene Ports usw.). In OT Security 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.

Hinweis: 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 definieren bestimmte Arten von Ereignissen, 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, generiert OT Security ein Ereignis. OT Security protokolliert das Ereignis und sendet Benachrichtigungen gemäß den für die Richtlinien konfigurierten Richtlinienaktionen.

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)** – Eine HMI sollte 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** – Zwischen zwei Netzwerk-Assets wurde ein unzulässiges Kommunikationsprotokoll 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** – Es wurde ein neues Asset entdeckt oder ein Asset kommuniziert nicht mehr im Netzwerk.
- **Anomale oder nicht autorisierte Änderungen an Asset-Eigenschaften** – Die Firmware oder der Status eines Assets haben sich 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 Baseline für den Netzwerk-Traffic**: Der Benutzer definiert eine Baseline für „normalen“ Netzwerk-Traffic basierend auf der Traffic-Karte während eines bestimmten Zeitraums und generiert Warnungen für Abweichungen von der Baseline. 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 Richtlinien für Konfigurationsereignise:
    - **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 OT Security 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.

Lizenzkomponenten von OT Security

In diesem Thema wird das Verfahren zur Lizenzierung von Tenable OT Security als eigenständiges Produkt beschrieben. Außerdem wird erläutert, wie Assets gezählt werden, welche Add-On-Komponenten Sie erwerben können, wie Lizenzen zurückgefordert werden und was geschieht, wenn Lizenzen überschritten werden oder ablaufen.

> **Tipp**: Informationen zur Aktualisierung oder erneuten Initialisierung Ihrer Lizenz finden Sie unter OT Security – Lizenz-Workflow.

Lizenzierung von Tenable OT Security

Sie können Tenable OT Security als Subscription oder als unbefristete Version/Wartungsversion erwerben.

Um Tenable OT Security zu lizenzieren, erwerben Sie Lizenzen, die auf den Anforderungen Ihres Unternehmens und den Umgebungsdetails basieren. Tenable OT Security weist diese Lizenzen dann Ihren *Assets* zu: allen erkannten Geräten mit IP-Adressen, eine Lizenz für jede IP-Adresse.

Wenn Ihre Umgebung größer wird, steigt auch die Anzahl Ihrer Assets. Um dieser Änderung Rechnung zu tragen, erwerben Sie zusätzliche Lizenzen. Für Tenable-Lizenzen gilt eine progressive Preisgestaltung: Je mehr Lizenzen Sie erwerben, desto geringer ist der Preis pro Einheit. Informationen zu Preisen erhalten Sie von dem für Sie zuständigen Tenable-Mitarbeiter.

Zählung von Assets

In Tenable OT Security basiert die Anzahl Ihrer Lizenzen auf der Anzahl eindeutiger IP-Adressen in Ihrer Umgebung. Assets werden ab dem Zeitpunkt lizenziert, zu dem sie erkannt werden.

Hinweis: Assets in internen Netzwerken hinter Live-IP-Adressen werden nicht auf Ihre Lizenz angerechnet. Beispielsweise werden in einem redundant verbundenen PLC-Chassis (speicherprogrammierbare Steuerung) mit zwei Live-IP-Adressen und zehn Modulen dahinter nur die beiden Live-IP-Adressen auf Ihre Lizenz angerechnet.

Hinweis: Sie können zwar eine separat erworbene Version von OT Security mit Ihrer Instanz von Tenable Oneverbinden, dies hat jedoch keinen Einfluss auf die Lizenzierung dieser Assets. Tenable One-Kunden verfügen über eine Vielzahl von Tenable-Lösungen, die für sie lizenziert sind, einschließlich OT Security. Die Lizenzen müssen jedoch zuerst Teil der Tenable One-Lizenz sein. Sie können das Konto gemeinsam mit Ihren CSMs (Customer Success Manager) aktualisieren.

Komponenten von Tenable OT Security

Sie können Tenable OT Security an Ihren Anwendungsfall anpassen, indem Sie Komponenten hinzufügen. Bei einigen Komponenten handelt es sich um Add-ons, die Sie erwerben müssen.

Im Lieferumfang enthalten	Add-on-Komponente
• Virtual Core Appliance • Tenable Security Center.	• Tenable OT Security Enterprise Manager. • Tenable OT Security – Konfigurierbarer Sensor • Tenable OT Security – Zertifizierter konfigurierbarer

	Sensor • Tenable OT Security – Zertifizierte Core-Plattform • Tenable OT Security – Core-Plattform • Tenable OT Security – XL Core-Plattform

Lizenzen zurückfordern

Wenn Sie Lizenzen erwerben, bleibt die Gesamtzahl Ihrer Lizenzen für die Dauer Ihres Vertrags unverändert, es sei denn, Sie erwerben weitere Lizenzen. Tenable OT Security fordert jedoch Lizenzen in Echtzeit zurück, wenn sich die Anzahl Ihrer Assets ändert.

Die folgenden Assets werden von Tenable OT Security zurückgefordert:

- Ausgeblendete Assets
- Assets, die länger als 30 Tage offline waren
- Assets, die Sie in der Benutzeroberfläche entfernen oder ausblenden

Überschreitung der maximalen Lizenzanzahl

In Tenable OT Security können Sie nur die Ihnen zugeteilte Anzahl an Lizenzen verwenden, es sei denn, Sie erwerben weitere Lizenzen.

Die Überschreitung der maximalen Lizenzanzahl bewirkt Folgendes:

- Benutzer ohne Administratorrechte können nicht mehr auf Tenable OT Security zugreifen.
- In der Benutzeroberfläche wird eine Meldung angezeigt, dass Ihre Lizenzanzahl überschritten wurde.
- Sie können Assets nicht mehr über die Tenable OT Security-Einstellungen wiederherstellen.
- Sie können Schwachstellen-Plugins oder IDS-Signaturen (Feed-Updates) nicht mehr aktualisieren.

Hinweis: Wenn Sie Ihre maximale Lizenzanzahl überschreiten, kann Tenable OT Security weiterhin neue Assets erkennen und hinzufügen.

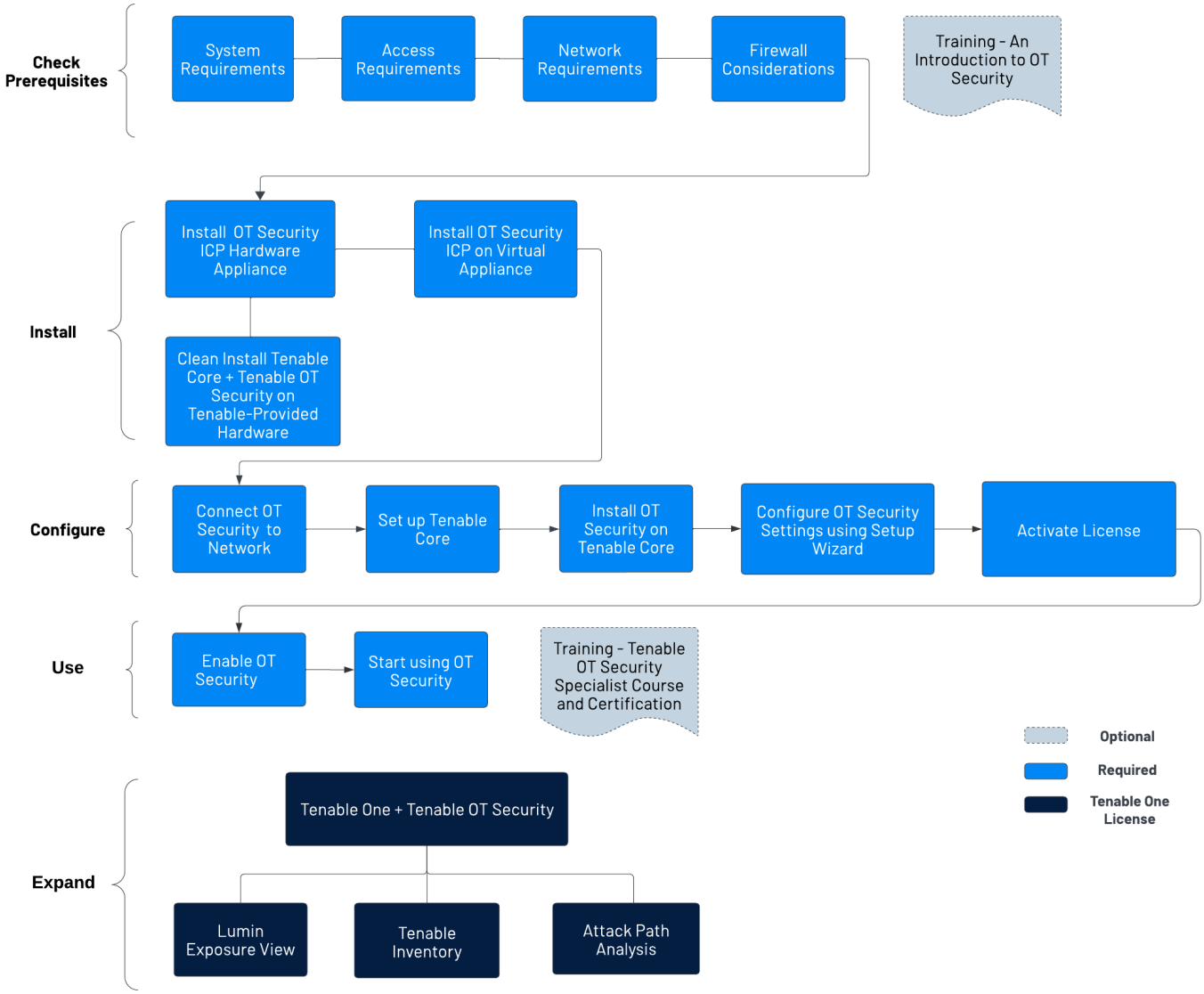
Abgelaufene Lizenzen

Die von Ihnen erworbenen Tenable OT Security-Lizenzen sind für die Dauer Ihres Vertrags gültig. 30 Tage vor Ablauf Ihrer Lizenz wird eine Warnung in der Benutzeroberfläche angezeigt. Setzen Sie sich während dieses Verlängerungszeitraums mit dem für Sie zuständigen Tenable-Mitarbeiter in Verbindung, um Produkte hinzuzufügen oder zu entfernen oder die Anzahl Ihrer Lizenzen zu ändern.

Nach Ablauf Ihrer Lizenz wird Tenable OT Security deaktiviert und Sie können das Tool nicht verwenden.

Erste Schritte mit OT Security

Verwenden Sie die folgende Einstiegssequenz, um die Installation zu starten und OT Security zu verwenden.



Voraussetzungen überprüfen

- Voraussetzungen – Informieren Sie sich über die System-, Hardware-, virtuellen und Lizenzanforderungen für OT Security.
    - Systemanforderungen – Informieren Sie sich über die Anforderungen für die Installation und Ausführung von Tenable Core + OT Security.
    - Zugriffsanforderungen – Informieren Sie sich über die Internet- und Portanforderungen für die Ausführung von Tenable Core + OT Security.

- Überlegungen zum Netzwerk – Informieren Sie sich über die Netzwerkschnittstellen, die zum Verbinden von OT Security benötigt werden.
- Überlegungen zur Firewall – Informieren Sie sich über die Ports, die offen sein müssen, damit OT Security ordnungsgemäß funktioniert.
- Einführung in Tenable OT Security – Gehen Sie das Schulungsmaterial durch, um detaillierte Informationen zu OT Security zu erhalten.

OT Security ICP installieren

OT Security ist eine Anwendung, die auf dem Betriebssystem Tenable Core ausgeführt wird und den Basisanforderungen von Tenable Core unterliegt. Beachten Sie die folgenden Richtlinien, um Tenable Core + OT Security zu installieren und zu konfigurieren.

So installieren Sie OT Security:

1. OT Security ICP installieren
   - OT Security ICP-Hardware-Appliance installieren – Richten Sie OT Security als Hardware-Appliance ein.

     > **Hinweis**: Auf der von Tenable bereitgestellten Tenable Core-Hardware ist Tenable Core + OT Security vorinstalliert. Wenn Sie eine ältere oder veraltete Appliance installieren, sollten Sie sich möglicherweise für eine Neuinstallation entscheiden. Weitere Informationen finden Sie unter Neuinstallation von Tenable Core + Tenable OT Security auf von Tenable bereitgestellter Hardware.

   - Virtuelle OT Security ICP-Appliance installieren – Stellen Sie Tenable Core + OT Security als virtuelle Maschine bereit, indem Sie die vorkonfigurierte `OVA`-Datei mit der Standardkonfiguration der virtuellen Maschine verwenden, oder passen Sie Ihre Appliance mit der `ISO`-Installationsdatei an.
2. OT Security mit dem Netzwerk verbinden – Verbinden Sie die OT Security Hardware- und virtuelle Appliance mit dem Netzwerk.
3. OT Security ICP konfigurieren

a. Tenable Core einrichten – Konfigurieren Sie Tenable Core über die CLI oder die Benutzeroberfläche.

b. OT Security unter Tenable Core installieren – Schließen Sie die Installation von Tenable OT Security in Tenable Core manuell ab.

c. Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren – Konfigurieren Sie die grundlegenden Einstellungen in OT Security mit dem Setup-Assistenten.

   - Loggen Sie sich bei der OT Security-Konsole ein und konfigurieren Sie die Einstellungen für Benutzerinformationen, Gerät, Systemzeit und Port-Trennung.

4. OT Security-Lizenz aktivieren – Aktivieren Sie Ihre Lizenz, nachdem Sie die Installation von OT Security abgeschlossen haben.

OT Security verwenden

Starten OT Security

1. OT Security aktivieren – Aktivieren Sie OT Security, nachdem Sie Ihre Lizenz aktiviert haben.
2. verwendenOT Security – Konfigurieren Sie Ihre überwachten Netzwerke, die Port-Trennung, Benutzer, Gruppen, Authentifizierungsserver usw. so, dass sie OT Security verwenden.

> **Tipp**: Um praktische Erfahrungen zu sammeln und die Tenable OT Security Specialist-Zertifizierung zu erhalten, absolvieren Sie den Tenable OT Security Specialist-Kurs.

OT Security zu Tenable One erweitern

> **Hinweis**: Hierzu ist eine Tenable One-Lizenz erforderlich. Weitere Informationen zum Testen von Tenable One finden Sie unter Tenable One.

Integrieren Sie OT Security mit Tenable One und nutzen Sie die folgenden Funktionen:

- In Lumin Exposure View können Sie konvergierende Risikostufen aufzeigen und versteckte Schwächen über die IT-OT-Grenze hinweg aufdecken. Mit erweiterten OT-Daten können Sie potenzielle Schwachstellen kontinuierlich überwachen und verfolgen:

- Auf der Exposure-Karte **Global** finden Sie Informationen zu Ihrem gesamtheitlichen Risikowert. Klicken Sie auf **Per Exposure**, um zu verstehen, welche Faktoren sich in welchem Umfang auf Ihren Risikowert auswirken.
- Sehen Sie sich die Exposure-Karte **Operational Technologies** an.
- Konfigurieren Sie die Einstellungen der Exposure-Ansicht, um benutzerdefinierte Kartenziele festzulegen und Ihr **SLA für Behebungsmaßnahmen** und die **SLA-Effizienz** basierend auf Ihrer Unternehmensrichtlinie zu konfigurieren.
- Erstellen Sie eine benutzerdefinierte Exposure-Karte auf der Grundlage des geschäftlichen Kontexts und nutzen Sie das neue Tag, das Sie in Tenable Inventory erstellt haben.

- In Tenable Inventory können Sie die Asset-Erfassung mit OT-spezifischen Informationen anreichern, wie z. B. Firmware-Versionen, Anbieter, Modelle und Betriebsstatus. Rufen Sie OT-Informationen ab, die Standard-IT-Sicherheitstools nicht bieten können:
  - Überprüfen Sie Ihre OT-Assets, um die strategischen Aspekte der Benutzeroberfläche zu verstehen. Dies sollte Ihnen eine Vorstellung davon vermitteln, welche Funktionen Sie in Tenable Inventory wann verwenden können.
  - Überprüfen Sie die **Tenable-Abfragen**, die Sie verwenden, bearbeiten und mit Lesezeichen versehen können.
  - Machen Sie sich mit dem Global Search Query Builder und seinen Objekten und Eigenschaften vertraut. Versehen Sie benutzerdefinierte Abfragen für die spätere Verwendung mit Lesezeichen.

    Tipp: So verschaffen Sie sich einen schnellen Überblick über die verfügbaren Eigenschaften:
    - Geben Sie im Query Builder *has* ein. Es erscheint eine Liste mit vorgeschlagenen Asset-Eigenschaften.
    - Passen Sie die Liste an, indem Sie eine Spalte hinzufügen. Es erscheint eine Liste der verfügbaren Spalten/Eigenschaften.
  - Schlüsseln Sie die Seite mit Asset-Details auf, um Asset-Eigenschaften und alle zugehörigen Kontextansichten anzuzeigen.
  - Erstellen Sie ein neues dynamisches Tag für Ihre OT-Assets. Dabei gilt:

        - Operator = **Typ des Hostsystems**
        - Wert = **SPS**
    - (Optional) Erstellen Sie ein Tag, das verschiedene Asset-Klassen kombiniert.
- In Attack Path Analysis können Sie anfällige Netzwerkpfade aufdecken, die wichtige betriebliche Abläufe in Produktionslinien oder Rechenzentren stören könnten. Sie können OT-Kommunikationspfade und nicht autorisierte Änderungen nachverfolgen:
    - Rufen Sie das **Attack Path Analysis Dashboard** auf, um einen allgemeinen Überblick über Ihre anfälligen Assets zu erhalten, wie z. B. die Anzahl der Angriffspfade, die zu diesen kritischen Assets führen, die Anzahl der offenen Feststellungen und deren Schweregrad, eine Matrix zur Anzeige von Pfaden mit unterschiedlichem Quellknoten-Exposure-Score und ACR-Ziel-Wert-Kombinationen sowie eine Liste mit häufigen Angriffspfaden.
        - Sehen Sie sich die **Top Attack Path Matrix** an und klicken Sie auf die Kachel **Top Attack Paths**, um weitere Informationen zu Ihren „Kronjuwelen“ oder Assets mit einem ACR von 7 oder höher anzuzeigen.

      Sie können diese bei Bedarf anpassen, um sicherzustellen, dass Daten und Erkenntnisse zu den kritischsten Angriffspfaden angezeigt werden.
    - Zeigen Sie auf der Seite **Findings** alle Angriffstechniken an, die in einem oder mehreren Angriffspfaden, die zu einem oder mehreren kritischen Assets führen, verwendet werden. Kombinieren Sie dazu Ihre Daten mit hochentwickelten Diagrammanalysen und dem MITRE ATT&CK® Framework, um Erkenntnisse zu gewinnen, die es Ihnen ermöglichen, die unbekannten Faktoren zu verstehen, die die Auswirkungen von Bedrohungen auf Ihre Assets und Daten auslösen und verstärken, und entsprechend zu handeln.
    - Wählen Sie in der **Mitre Att&ck Heatmap** die **ICS**-Heatmap-Option aus, um sich auf die Taktiken und Techniken für industrielle Steuerungssysteme (ICS) zu konzentrieren.
    - Generieren Sie auf der Seite **Discover** Angriffspfad-Abfragen, um Ihre Assets als Teil potenzieller Angriffspfade zu betrachten:

- Generate an Attack Path using a Built-in Query
- Generate an Asset Query using the Asset Query Builder
- Generate an Attack Path Query using the Attack Path Query Builder

Anschließend können Sie die Daten der Angriffspfad-Abfrage (Attack Path Query) und der Asset-Abfrage (Asset Query) über die Abfrageergebnisliste und das interaktive Diagramm anzeigen und mit ihnen interagieren.

Voraussetzungen

Ziel: Sicherstellen, dass Sie alles für eine erfolgreiche ICP-Installation besitzen.

Tenable OT Security ist eine Anwendung, die auf dem Betriebssystem Tenable Core ausgeführt wird und den Basisanforderungen von Tenable Core unterliegt.

Tenable Core + Tenable OT Security ist für die Bereitstellung sowohl auf Hardware als auch als VM-Appliance verfügbar. Für eine Bereitstellung als virtuelle Maschine müssen die in Hardwareanforderungen genannten Mindestanforderungen erfüllt sein.

Hardwareanforderungen

Dedizierte Tenable Core + Tenable OT Security Hardware-Appliances sind in mehreren Größen verfügbar (separat erhältlich). Hardwarespezifikationen finden Sie im Tenable OT Security-Datenblatt zu physischer Hardware.

Das Betriebssystem Tenable Core und die Anwendung Tenable OT Security sind auf allen verfügbaren Hardware-Appliances vorinstalliert.

Sie können Tenable Core + Tenable OT Security auch auf benutzerdefinierter Hardware installieren, die die Anforderungen erfüllt. Wenden Sie sich an Tenable Support oder Ihren Customer Success Manager, um Anweisungen zu erhalten.

Informationen zu den Anforderungen für Tenable Core + Tenable OT Security finden Sie in folgenden Ressourcen:

- Systemanforderungen
- Zugriffsanforderungen

Virtuelle Appliance – Anforderungen

Tenable Core + Tenable OT Security kann auf folgende Weise bereitgestellt werden:

- Mithilfe der `OVA`-Datei – Diese Datei kann sofort bereitgestellt werden und enthält die gesamte standardmäßige und unterstützte Konfiguration der virtuellen Maschine.
- Mithilfe der `ISO`-Datei – Dies ist ein universelles Image des Installationsdatenträgers. Stellen Sie diese Datei auf einer ordnungsgemäß konfigurierten virtuellen Maschine bereit, die die Anforderungen erfüllt.

Lizenzanforderungen

Allgemeine Informationen zur Lizenzierung für OT Security finden Sie unter Lizenzkomponenten von OT Security.

Informationen zum Lizenzierungs-Workflow finden Sie unter Lizenzaktivierung für OT Security.

Systemanforderungen

Um Tenable Core + OT Security oder OT Security Sensor zu installieren und auszuführen, müssen die Anwendung und das System die folgenden Anforderungen erfüllen.

Tipp: OT Security bietet einsatzfertige Appliances an, die direkt mit vorinstalliertem Image geliefert werden. Diese Option ist viel einfacher zu verwenden und bereitzustellen und bietet eine kürzere Amortisationszeit. Sie können jedoch auch Ihre eigene Hardware beschaffen und unser ISO-Image darauf anwenden. Wenn Sie Ihre eigene Hardware bereitstellen oder unsere Hardware verwenden möchten, finden Sie Anleitungen und bewährte Methoden in unseren Tenable OT-Hardwarespezifikationen. Alle Komponenten von OT Security, der ICP-EM und der Sensor können auf jeder Hardware ausgeführt werden, die die Spezifikationen erfüllt.

Hinweis: Tenable rät davon ab, mehrere Anwendungen auf einer einzigen Instanz von Tenable Core bereitzustellen. Wenn Sie mehrere Anwendungen auf Tenable Core bereitstellen möchten, stellen Sie für jede Anwendung eine eigene Instanz bereit.

Hinweis: Tenable-Support bietet keine Unterstützung bei Problemen im Zusammenhang mit dem Host-Betriebssystem, selbst wenn diese während der Installation oder Bereitstellung auftreten.

Umgebung	Tenable Core-	Weitere Informationen

Dateiformat			
Virtuelle Maschine	VMware	OVA-Datei	Tenable Core in VMware bereitstellen
	Microsoft Hyper-V	ZIP-Datei	
Hardware Von Tenable bereitgestellte Hardware		ISO-Image	Tenable Core auf Hardware installieren

Hinweis: Sie könnten die Pakete verwenden, um Tenable Core in anderen Umgebungen auszuführen, Tenable bietet jedoch keine Dokumentation für diese Verfahren.

OT Security – Hardwareanforderungen

Weitere Informationen zu spezifischen Hardwareanforderungen für OT Security oder OT Security Sensor finden Sie unter Tenable OT Security Hardware Specifications im Leitfaden *General Requirements*.

OT Security – Anforderungen an virtuelle Hardware

Unternehmensnetzwerke können in puncto Leistung, Kapazität, Protokollen und Gesamtaktivität variieren. Für Bereitstellungen müssen unter anderem folgende Ressourcenanforderungen berücksichtigt werden: reale Netzwerkgeschwindigkeit, Größe des zu überwachenden Netzwerks und Konfiguration der Anwendung.

Die folgende Tabelle enthält grundlegende Richtlinien für den Einsatz von Tenable Core + OT Security in einer virtuellen Umgebung.

Tenable Core + OT Security erfordert CPUs mit AVX und AVX2 (z. B. Intel Haswell oder neuer).

Installationsszenario	CPU-Kerne	Arbeitsspeicher	Festplattenspeicher
Virtuelle Maschine	8 Kerne	16 GB RAM	200 GB

Speicheranforderungen

Tenable empfiehlt, OT Security auf DAS-Geräten (Direct Attached Storage) zu installieren, vorzugsweise auf Solid-State-Laufwerken (SSD), um eine optimale Leistung zu erzielen. Tenable empfiehlt nachdrücklich die Verwendung von Solid-State-Speicher (SSS), der über eine hohe DWPD-Rate (Laufwerksschreibvorgänge pro Tag) verfügt, um eine lange Lebensdauer zu gewährleisten.

Die Installation von OT Security auf NAS-Geräten (Network-Attached Storage) wird von Tenable nicht unterstützt. In diesen Fällen sind Speichernetzwerke (SAN) mit einer Speicherlatenz von maximal 10 Millisekunden oder Tenable Hardware-Appliances eine gute Alternative.

Anforderungen an den Festplattenspeicher

Unternehmensnetzwerke können in puncto Leistung, Kapazität, Protokollen und Gesamtaktivität variieren. Für Bereitstellungen müssen unter anderem folgende Ressourcenanforderungen berücksichtigt werden: reale Netzwerkgeschwindigkeit, Größe des zu überwachenden Netzwerks und Konfiguration der Anwendung. Die Auswahl von Prozessoren, Arbeitsspeicher und Netzwerkkarte hängt stark von diesen Bereitstellungskonfigurationen ab. Die Anforderungen an den Festplattenspeicher hängen von der Nutzung auf Basis der Datenmenge und der Dauer der Datenspeicherung im System ab.

OT Security muss vollständige Paketerfassungen des überwachten Traffics durchführen, und die Größe der von OT Security gespeicherten Richtlinienereignisdaten hängt von der Anzahl der Geräte und dem Typ der Umgebung ab.

Sie können die Speicheranforderungen pro Tag (GB/Tag) berechnen, indem Sie die Traffic-Rate (Mbps) * 2,7 multiplizieren – basierend auf einem Komprimierungsfaktor von 0,25.

In einem Beispiel mit zwei Sensoren, die jeweils 23 Mbps SPAN-Traffic empfangen, wird der Speicherbedarf pro Tag (GB/Tag) berechnet als (23*2)*2,7=124 GB Speicherplatz pro Tag für die Traffic-Speicherung.

> **Hinweis**: Wenn Sie gemäß Compliance- oder Sicherheitsvorschriften Traffic von bis zu 30 Tagen speichern müssen, benötigen Sie ein PCAP-Speicherlaufwerk (Paketerfassung) mit 3,75 TB, um diese Anforderung zu erfüllen. Sobald die gespeicherten Traffic-Daten die maximale Größe erreicht haben, überschreibt OT Security die ältesten PCAP-Daten und ersetzt sie durch neuen Traffic.

Richtlinien für ICP-Systemanforderungen

Maximaler SPAN/TAP-Durchsatz (Mbit/s)	CPU-Kerne[1]	Arbeitsspeicher (DDR4)	Speicheranforderungen	Netzwerkschnittstellen
50 Mbit/s oder weniger	4	16 GB RAM	128 GB	Mindestens 4 x 1 Gbit/s
50–150 Mbit/s	16	32 GB RAM	512 GB	Mindestens 4 x 1 Gbit/s
150–300 Mbit/s	32	64 GB RAM	1 TB	Mindestens 4 x 1 Gbit/s
300 Mbit/s bis 1 GB	32-64	128 GB RAM oder mehr	2 TB oder mehr	Mindestens 4 x 1 Gbit/s

Anforderungen an Festplattenpartitionen

OT Security verwendet die folgenden bereitgestellten Partitionen:

Partition	Inhalt
/	Betriebssystem
/opt	Anwendungs- und Datenbankdateien
/var/pcap	Paketerfassungen (vollständige Paketerfassung, Ereignis, Abfrage)

Im Standardinstallationsprozess werden diese Partitionen auf demselben Datenträger abgelegt. Tenable empfiehlt, diese zu Partitionen auf separaten Festplatten zu verschieben, um den Durchsatz zu erhöhen. OT Security ist eine festplattenintensive Anwendung. Die Verwendung von Festplatten mit hohen Lese-/Schreibgeschwindigkeiten, wie z. B. SSDs, ermöglicht die beste Leistung. Tenable empfiehlt, eine SSD mit hohen DWPD-Raten auf vom Kunden bereitgestellter Hardware zu verwenden, wenn die Paketerfassungsfunktion in OT Security genutzt wird.

Tipp: Durch die Bereitstellung von OT Security auf einer Hardwareplattform, die mit einem redundanten Array unabhängiger Festplatten (RAID 0) konfiguriert ist, kann die Leistung erheblich verbessert werden.

Tipp: Tenable erfordert selbst für unsere größten Kunden keine RAID-Laufwerke. In einem Fall änderten sich jedoch für einen Kunden mit mehr als einer Million verwalteter Schwachstellen die Antwortzeiten für Abfragen mit einer schnelleren RAID-Festplatte von einigen Sekunden auf weniger als eine Sekunde.

Anforderungen an Netzwerkschnittstellen

Bevor Sie OT Security installieren, müssen zwei (oder mehr) Netzwerkschnittstellen auf Ihrem Gerät vorhanden sein. Tenable empfiehlt die Verwendung von Gigabit-Schnittstellen. Die VMWare OVA-Datei erstellt diese Schnittstellen automatisch. Erstellen Sie diese Schnittstellen manuell, wenn Sie die ISO-Datei installieren (z. B. Hyper-V).

Hinweis: Tenable bietet keine SR-IOV-Unterstützung für die Verwendung von 10-G-Netzwerkkarten und garantiert bei Verwendung von 10-G-Netzwerkkarten keine 10-G-Geschwindigkeiten.

Anforderungen an Netzwerkschnittstellen-Controller

- OT Security erfordert nur eine NIC für EM.
- OT Security erfordert mindestens zwei NICs für die ICP und die Sensoren.
- OT Security erfordert die Verwendung statischer IP-Adressen für ICP/EM/Sensoren.
- Sowohl der Sensor als auch die ICP können so konfiguriert werden, dass sie mehrere SPAN-Schnittstellen überwachen.

Hinweis: Ab OT Security 4.1lauten die Profilnamen für Netzwerkschnittstellen wie folgt:

- nic0 – Systemport 1
- nic1– Systemport 2
- nic2 – Systemport 3
- nic3 – Systemport 4

nic0 oder **Systemport 1**(192.168.1.5) und **nic3** oder **Systemport 4** (192.168.3.3) haben statische IP-Adressen, wenn Sie Tenable Core + OT Security in einer Hardware- oder virtuellen Umgebung installieren. Andere Netzwerkschnittstellen-Controller (Network Interface Controllers, NICs) verwenden DHCP.

nic3 oder **Systemport 4** (192.168.3.3) hat eine statische IP-Adresse, wenn Sie Tenable Core + OT Security auf VMware bereitstellen. Andere NICs verwenden DHCP. Bestätigen Sie, dass die MAC-Adresse von **nic1**oder **Systemport 2** in Tenable Core + OT Security mit der MAC-Adresse des NIC in Ihrer VMware-Konfiguration für passives Scannen übereinstimmt. Ändern Sie bei Bedarf Ihre VMware-Konfiguration so, dass sie mit Ihrer MAC-Adresse in Tenable Core übereinstimmt.

Weitere Informationen finden Sie unter Manually Configure a Static IP Address, Manage System Networking und in der *VMware-Dokumentation*.

[1]„CPU-Kerne“ bezieht sich auf PHYSISCHE Kerne und setzt CPUs der Serverklasse voraus (Xeon, Opteron).

Zugriffsanforderungen

Ihre Bereitstellung muss die folgenden Anforderungen erfüllen.

- Internetanforderungen
- Portanforderungen

Internetanforderungen

Sie müssen über Internetzugriff verfügen, um Tenable Core-Dateien herunterzuladen und Online-Installationen durchzuführen.

Nachdem Sie eine Datei auf Ihren Computer übertragen haben, variieren die Internetzugriffsanforderungen zum Bereitstellen oder Aktualisieren von Tenable Core je nach Umgebung.

Hinweis: Sie müssen `Appliance.cloud.tenable.com` erreichen, um die Online-ISOs für Installationen verwenden zu können (und um Online-Updates zu erhalten) und `sensor.cloud.tenable.com`, um Scan-Jobs auszuwählen.

Umgebung		Tenable Core-Format	Internetanforderungen
Virtuelle Maschine	VMware	OVA-Datei	Für die Bereitstellung oder Aktualisierung von Tenable Core ist kein Internetzugriff

			erforderlich.
Hardware		`ISO`-Image	Für die Installation und Aktualisierung von Tenable Core ist Internetzugriff erforderlich.

Tipp: Sie benötigen keinen Zugriff auf das Internet, wenn Sie Updates über eine Offline-`ISO`-Datei installieren. Weitere Informationen finden Sie unter Update Tenable Core Offline.

Portanforderungen

Ihre Tenable Core-Bereitstellung erfordert Zugriff auf bestimmte Ports für ein- und ausgehenden Traffic. Tenable Security Center erfordert außerdem anwendungsspezifischen Portzugriff. Weitere Informationen finden Sie unter Portanforderungen im (missing or bad snippet).OT Security erfordert außerdem anwendungsspezifischen Portzugriff. Weitere Informationen finden Sie unter Überlegungen zur Firewall.

Eingehender Traffic

Lassen Sie eingehenden Traffic zu folgenden Ports zu:

Hinweis: Eingehender Traffic bezieht sich auf Traffic von Benutzern, die Tenable Core konfigurieren.

Port	Traffic
TCP 22	Eingehende SSH-Verbindungen.
TCP 443	Eingehende Kommunikation an die OT Security-Schnittstelle.
TCP 8000	Eingehende HTTPS-Kommunikation an die Tenable Core-Schnittstelle.

Ausgehender Traffic

Lassen Sie ausgehenden Traffic an die folgenden Ports zu:

Port	Traffic
TCP 22	Ausgehende SSH-Verbindungen, einschließlich Remotespeicher-Verbindungen.
TCP 443	Ausgehende Kommunikation an die Server `appliance.cloud.tenable.com`

	und `sensor.cloud.tenable.com` für System-Updates.
UDP 53	Ausgehende DNS-Kommunikation für OT Security und Tenable Core.

Überlegungen zum Netzwerk

Die OT Security Appliance (sowohl physisch als auch virtuell) muss diese Netzwerkschnittstellen erreichen:

Schnittstelle für Verwaltung und aktive Abfragen

- Eine Schnittstelle, die mit einer IP-Adresse konfiguriert ist, über die das Netzwerk erreicht werden kann, um die Appliance zu verwalten und zu konfigurieren.
- Ermöglicht der Appliance, Assets im Netzwerk zur Durchführung von aktiven Abfragen zu erreichen (empfohlen, aber optional).
- Ermöglicht die Aufteilung auf zwei separate Netzwerkschnittstellen. Siehe Separaten Verwaltungsport verbinden (Port-Trennung).

Überwachungsschnittstelle

- Überwacht und erfasst passiv Traffic zu Analysezwecken.
- Muss mit einer Spiegelungs-, Switch Port Analyzer (SPAN)- oder Remote Switch Port Analyzer (RSPAN)-Zielschnittstelle eines Switch verbunden sein.
- (Optional) Verwendet Sensoren und ERSPAN-Konfiguration (Encapsulated Remote SPAN), um Traffic zu überwachen, der nicht direkt in die Appliance-Oberfläche gespiegelt werden kann.

Überlegungen zur Firewall

Beim Einrichten Ihres OT Security-Systems ist es wichtig, die offenen Ports zu bestimmen, damit das Tenable-System ordnungsgemäß funktioniert. Die folgenden Tabellen geben die Ports an, die für die Verwendung mit OT Security ICP und den OT Security Sensoren reserviert werden müssen, sowie die Ports, die für die Ausführung von aktiven Abfragen und für die Integration mit Tenable Vulnerability Management und Tenable Security Center benötigt werden.

Hinweis: Informationen zur Liste der Tenable-Websites und -Domänen, die Sie in der Firewall zulassen müssen, finden Sie im Wissensdatenbankartikel.

OT Security Core-Plattform

Die folgenden Ports sollten für die Kommunikation mit der OT Security Core-Plattform offen bleiben.

Flussrichtung	Port	Kommuniziert mit	Zweck
Eingehend	TCP 443 und TCP 28304	OT-Sensor	Sensorauthentifizierung, Kopplung und Empfang von Sensorinformationen.
Eingehend	TCP 8000	Weboberfläche für Tenable Core	Browserzugriff auf Tenable Core
Eingehend	TCP 28304	ICP/OT Security	Sensorkommunikation
Eingehend	TCP 22	Appliance für SSH-Zugriff	Befehlszeilenzugriff auf Betriebssystem oder Appliance
Ausgehend	TCP 443	Tenable Security Center	Sendet Daten zur Integration
Ausgehend*	TCP 443	cloud.tenable.com	Sendet Daten zur Integration
Ausgehend*	Verschiedene Industrieprotokolle	SPS/Steuerungen	Aktive Abfrage
Ausgehend*	TCP 25 oder 587	E-Mail-Server für Warnmeldungen	SMTP (Warn-E-Mails, Berichte)
Ausgehend*	UDP 514	Syslog-Server	Sendet Richtlinien-Ereigniswarnungen und Syslog-Meldungen

Ausgehend*	UDP 53	DNS-Server	Namensauflösung
Ausgehend*	UDP 123	NTP-Server	Zeitdienst
Ausgehend*	TCP 389 oder 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 *.nessus.org	Automatische Plugin-, Anwendungs- und Betriebssystem-Updates**
Ausgehend	TCP 10146 (sicherer Port)	IoT-Connector	Verbindet ICP mit dem IoT-Connector-Agent

* Optionale Dienste

** Offline-Verfahren verfügbar

OT Security Sensoren

Die folgenden Ports sollten für die Kommunikation mit OT Security Sensoren offen bleiben.

Flussrichtung	Port	Kommuniziert mit	Zweck
Eingehend	TCP 8000	Weboberfläche	Browserzugriff auf Benutzer-GUI
Eingehend	TCP 22	Appliance für SSH-Zugriff	Befehlszeilenzugriff auf Betriebssystem oder Appliance
Ausgehend*	TCP 25	E-Mail-Server für	SMTP (Warn-E-Mails,

		Warnmeldungen	Berichte)
Ausgehend*	UDP 53	DNS-Server	Namensauflösung
Ausgehend*	UDP 123	NTP-Server	Zeitdienst
Ausgehend*	UDP 161	SNMP-Server	SNMP-Überwachung an Tenable Core
Ausgehend	TCP 28303	ICP/OT Security Sendet Kommunikation vom Sensor, empfängt auf ICP/OT Security	Nicht authentifizierte/nur passive Sensorverbindung
Ausgehend	TCP 443 und TCP 28304	ICP/OT Security Sendet Kommunikation vom Sensor, empfängt auf ICP/OT Security	Authentifizierter/sicherer Tunnel zwischen Sensor und ICP

* Optionale Dienste

Aktive Abfrage

Die folgenden Ports sollten offen bleiben, um die aktiven 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	UDP/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

Hinweis: Die von den Geräten verwendeten Ports variieren je nach Anbieter und Produktreihe. Eine Liste der relevanten Ports und Protokolle, die erforderlich sind, um den Erfolg aktiver Abfragen sicherzustellen, finden Sie unter Identifizierungs- und Detailabfrage.

OT Security-Integrationen

Die folgenden Ports sollten für die Kommunikation mit der Tenable Vulnerability Management- und der Tenable Security Center-Integration offen bleiben.

Flussrichtung	Port	Kommuniziert mit	Zweck
Ausgehend	TCP 443	cloud.tenable.com	Tenable Vulnerability Management-Integration
Ausgehend	TCP 443	Tenable Security Center	Tenable Security Center-Integration

Identifizierungs- und Detailabfrage

Sie können die folgenden Ports für Identifizierungs- und Detailabfragen verwenden:

Hinweis: Möglicherweise müssen Sie die Ports in der Firewall für OT Security oder dessen Sensoren öffnen, um den relevanten Port für Ihre Assets zu erreichen.

Port	Port-Name
21	FTP
80	HTTP
102	Step 7/S7+

111	Emerson OVATION
135	WMI
161	SNMP
443	HTTPS
502	MODBUS/MMS
1911	Niagara FOX
2001	Profibus
2222	PCCC_AB-ETH
2404	IEC 60870-5
3500	Bachmann
4000	Emerson ROC
4911	Niagara FOX TLS
5002	Mitsubishi MELSEC
5007	Mitsubishi MELSEC
5432	PSQL/SEL
18245	SRTP
20000	DNP3
20256	PCOM
44818	EthernetIP/CIP
47808	BACNET (udp)
48898	ADS
55553	Honeywell CEE
55565	Honeywell FTE

OT Security ICP installieren

Ziel: Installation und Betriebsbereitschaft des ICP für OT Security.

Bevor Sie beginnen

- Siehe Voraussetzungen.

Führen Sie nach Bedarf diese Schritte aus, um OT Security ICP zu installieren und eine Verbindung mit dem Netzwerk herzustellen:

- OT Security ICP-Hardware-Appliance installieren

  Hinweis: Auf der von Tenable bereitgestellten Tenable Core-Hardware ist Tenable Core + OT Security vorinstalliert. Wenn Sie eine ältere oder veraltete Appliance installieren, sollten Sie sich möglicherweise für eine Neuinstallation entscheiden. Weitere Informationen finden Sie unter Neuinstallation von Tenable Core + Tenable OT Security auf von Tenable bereitgestellter Hardware.

- Virtuelle OT Security ICP-Appliance installieren

Nächster Schritt

- OT Security mit dem Netzwerk verbinden

OT Security ICP-Hardware-Appliance installieren

Sie können die OT Security Appliance entweder in einem Rack montieren oder einfach auf eine ebene Oberfläche wie einen Schreibtisch stellen.

Tipp: Tenable empfiehlt, dass Sie die unter Tenable Core einrichten beschriebene grundlegende Konfiguration und Einrichtung und den OT Security-Setup-Assistenten bequem von Ihrem Schreibtisch aus ausführen, bevor Sie die Appliance in ein Rack oder an einen anderen Remote-Standort verschieben.

Rack-Montage

So montieren Sie die OT Security Appliance in einem 19-Zoll-Standard-Rack:

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

   Hinweis:

   - 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 in der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Ebene Oberfläche

So installieren Sie die OT Security Appliance auf einer ebenen Oberfläche:

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

   Hinweis:

   - Stellen Sie sicher, dass die Tischplatte eben und trocken ist.
   - Stellen Sie sicher, dass der Lufteinlass des Lüfters (in der Rückwand) und die Belüftungsöffnungen (an der Oberseite) nicht blockiert sind.
   - Wenn Sie ein Gerät zusammen mit anderen Elektrogeräten aufstellen, vergewissern Sie sich, dass hinter dem Lüfter (in der Rückwand) genügend Platz ist, um eine ausreichende Belüftung und Kühlung zu gewährleisten.

2. Stecken Sie das eine Ende des Wechselstromkabels (mitgeliefert) in den Stromversorgungsanschluss in der Rückwand und das andere Ende in die Wechselstromversorgung (Netz).

Weitere Informationen zur Konnektivität finden Sie unter Überlegungen zum Netzwerk.

Nächste Schritte

OT Security mit dem Netzwerk verbinden

Neuinstallation von Tenable Core + Tenable OT Security auf von Tenable bereitgestellter Hardware

Tenable Core + OT Security sind auf einsatzfertiger, offiziell von Tenable bereitgestellter Hardware vorinstalliert. In einigen Fällen wird eine Neuinstallation (auch als erneutes Flashen bezeichnet) empfohlen.

> **Hinweis**: Wenn Sie vor Kurzem eine neue Appliance erhalten haben, können Sie dieses Verfahren überspringen.

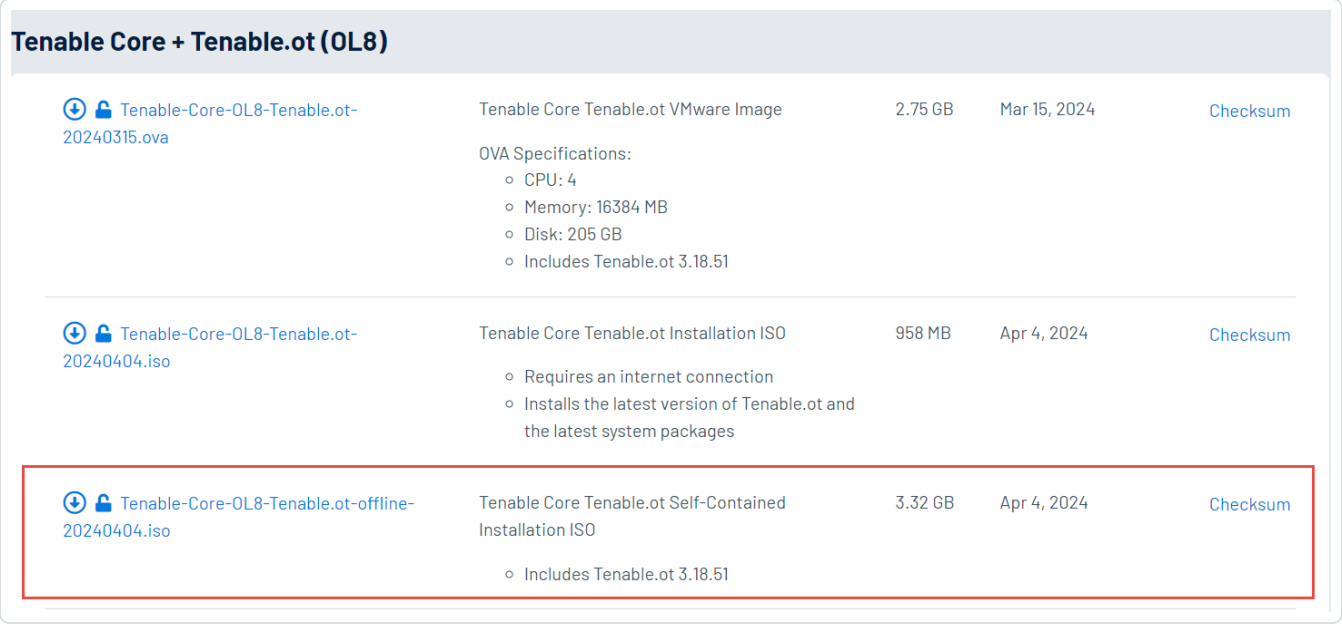
Bevor Sie beginnen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

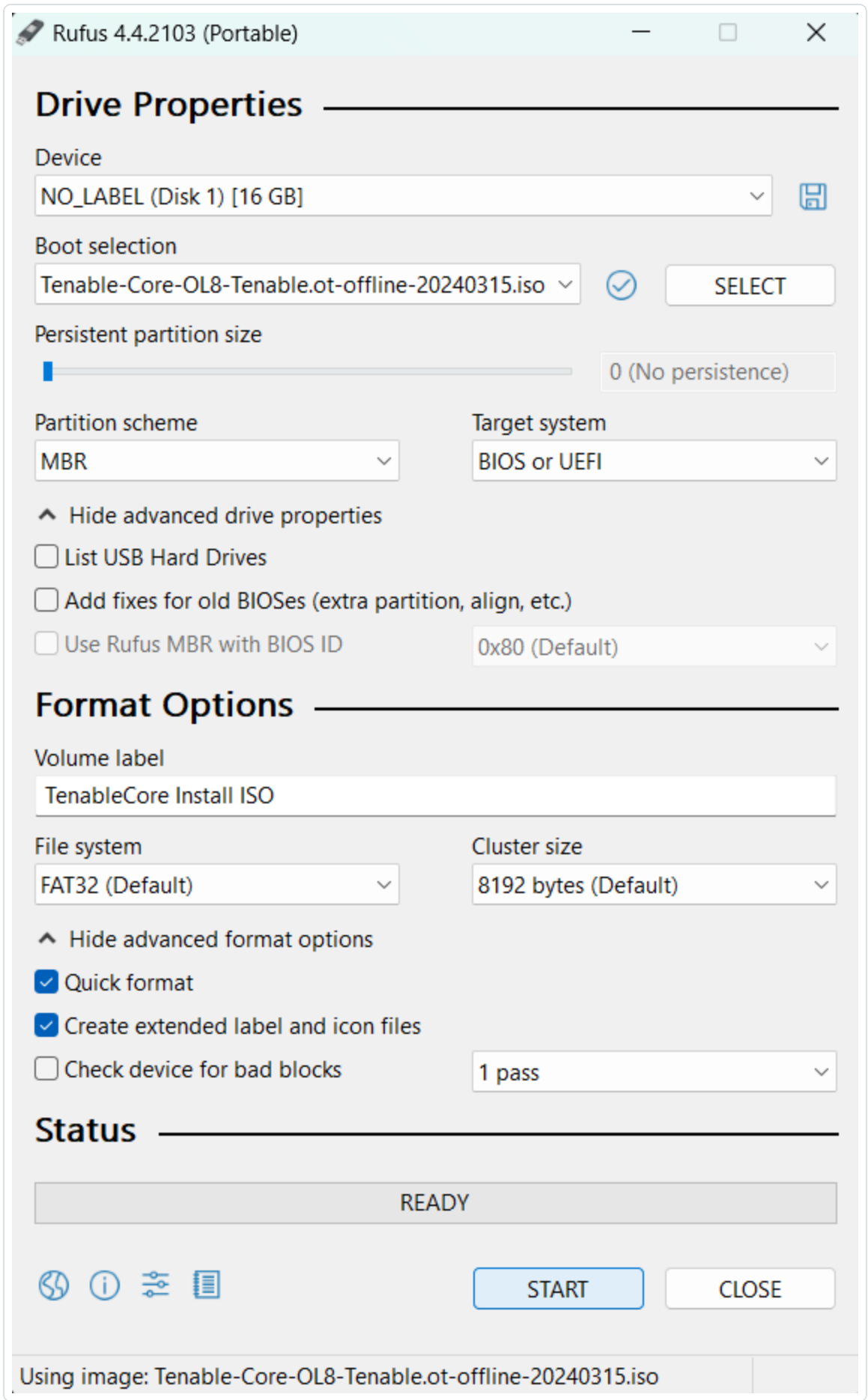
- Eine Anwendung zum Formatieren und Erstellen bootfähiger USB-Flash-Laufwerke wie Rufus.
- Ein serielles Kabel.
- Eine serielle Terminalanwendung, wie z. B. PuTTY.
- Einen USB-Speicherstick mit ca. 8 GB+.

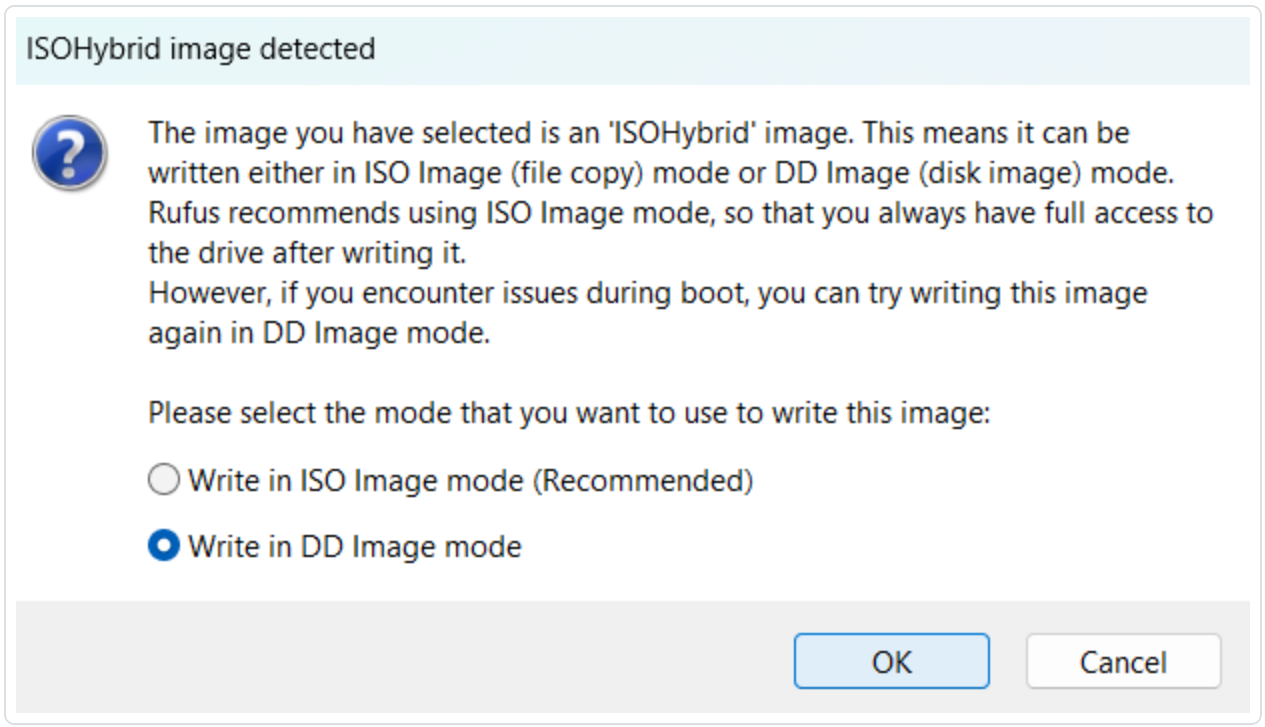
So installieren Sie die ISO-Datei von Tenable Core + OT Security:

1. Laden Sie die neueste Offline-ISO-Datei unter Tenable Downloads herunter.

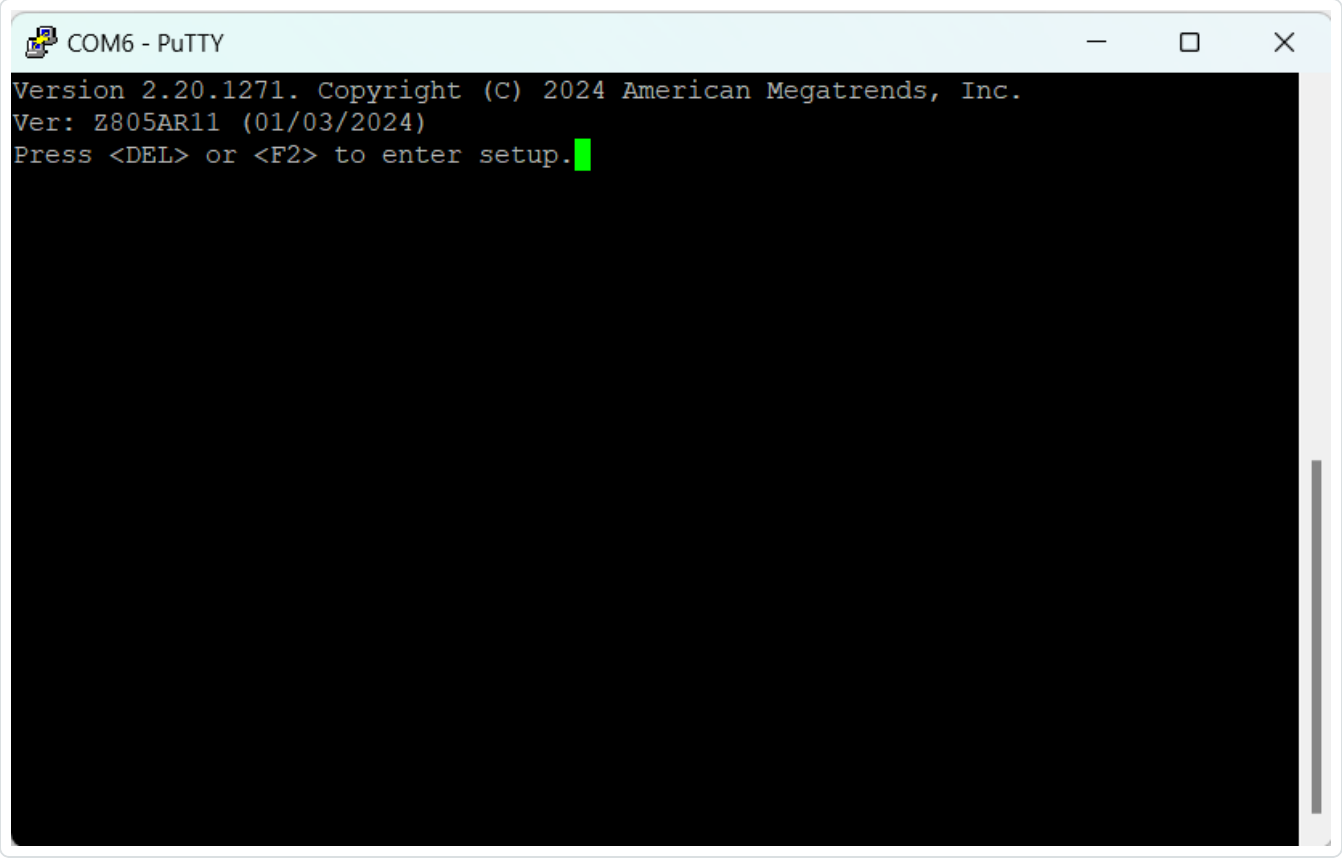


2. Stecken Sie den USB-Speicherstick in einen PC und flashen Sie die ISO im DD-Modus auf den Speicherstick.

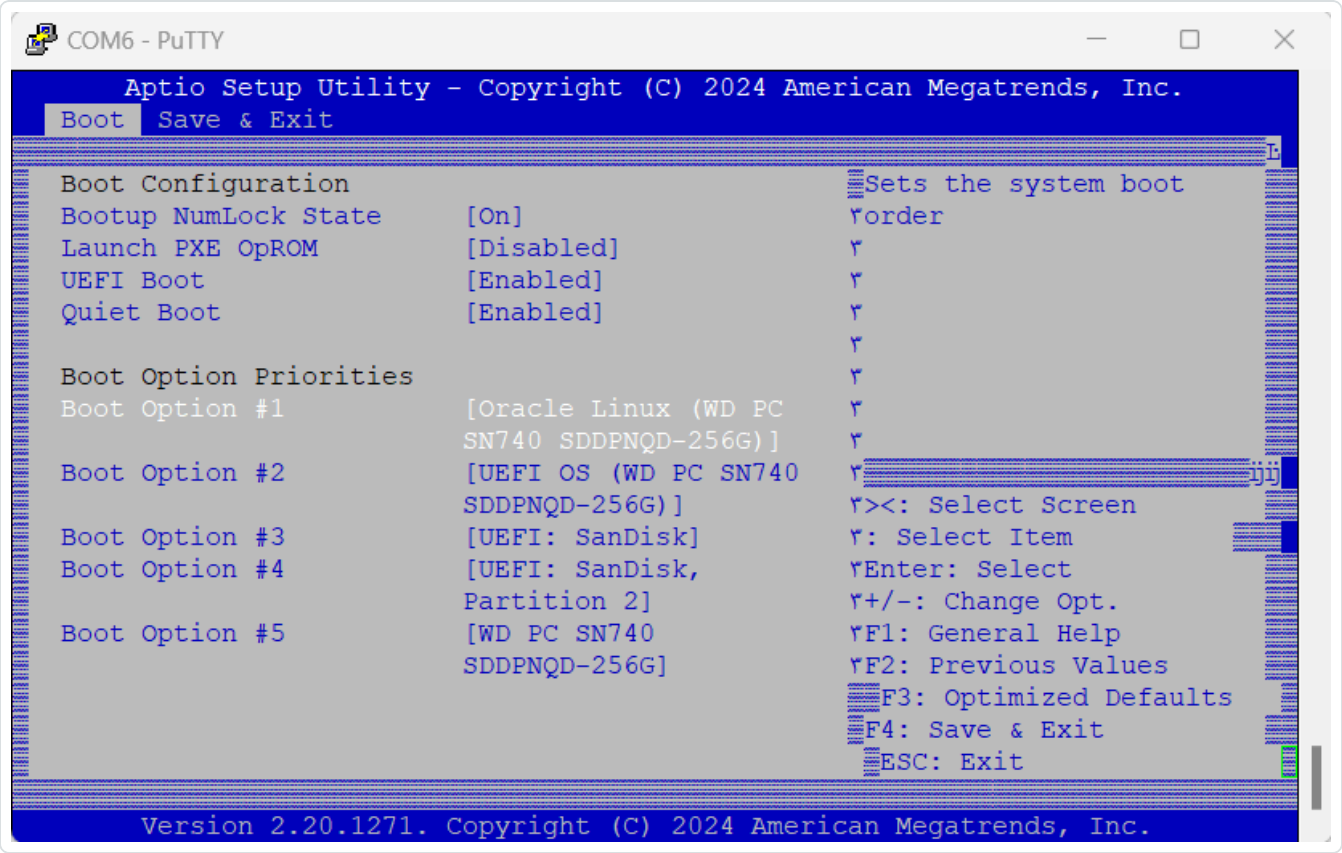

Rufus 4.4.2103 (Portable)
Drive Properties
Device
NO_LABEL (Disk 1) [16 GB]
Boot selection
Tenable-Core-OL8-Tenable.ot-offline-20240315.iso
SELECT
Persistent partition size
0 (No persistence)
Partition scheme
MBR
Target system
BIOS or UEFI
Hide advanced drive properties
List USB Hard Drives
Add fixes for old BIOSes (extra partition, align, etc.)
Use Rufus MBR with BIOS ID
0x80 (Default)
Format Options
Volume label
TenableCore Install ISO
File system
FAT32 (Default)
Cluster size
8192 bytes (Default)
Hide advanced format options
Quick format
Create extended label and icon files
Check device for bad blocks
1 pass
Status
READY
START
CLOSE
Using image: Tenable-Core-OL8-Tenable.ot-offline-20240315.iso



3. Wenn Sie fertig sind, stecken Sie den USB-Speicherstick in einen USB-Port der OT Security Appliance.
4. Stellen Sie über die serielle Schnittstelle der Konsole eine Verbindung zur Appliance her (Baudrate 115.200 Bit/s mit einer 8N1-Konfiguration) und schalten Sie die Appliance ein.

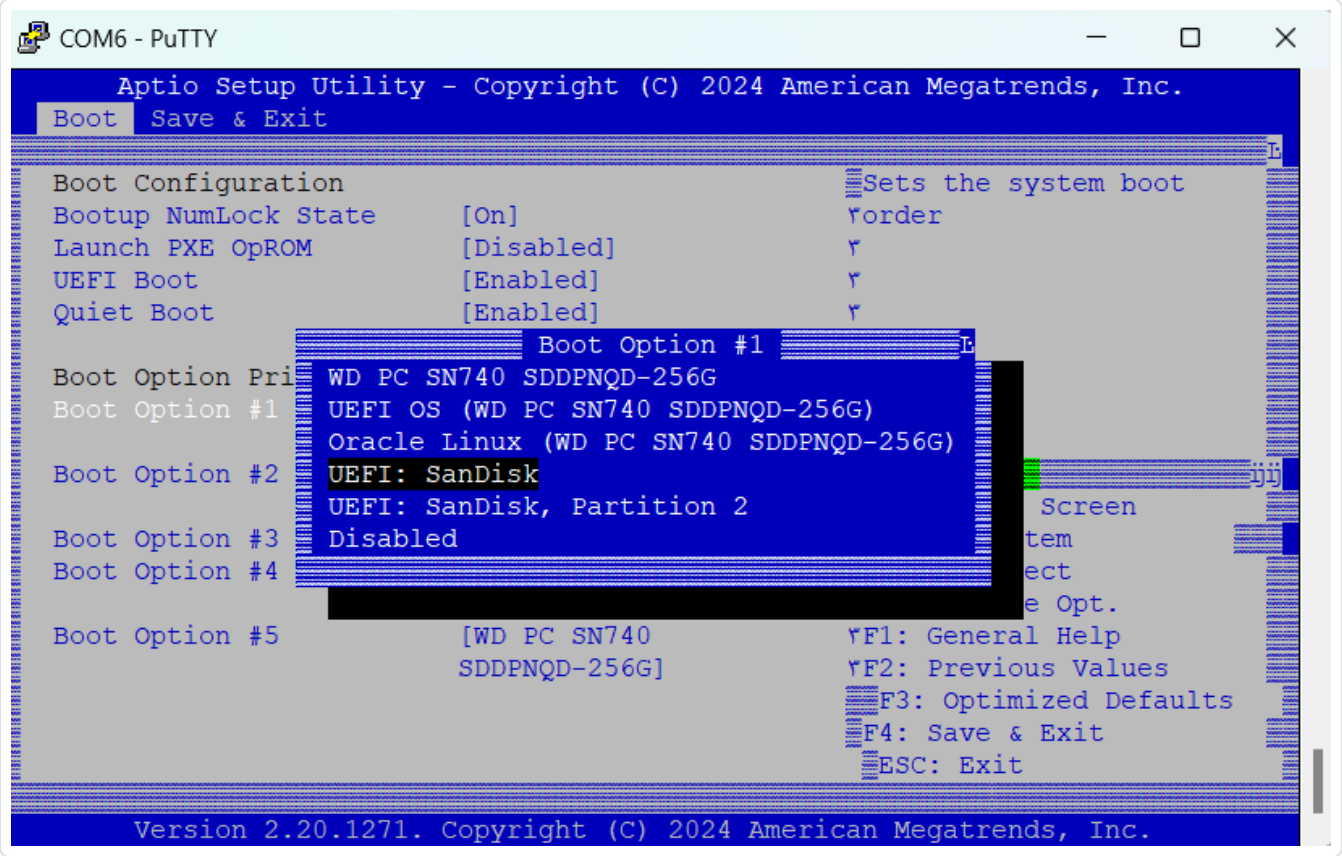


5. Wenn Sie dazu aufgefordert werden, drücken Sie <DEL>, um das Setup zu starten.
6. Navigieren Sie im System-Setup mit den Pfeiltasten zum Abschnitt **Boot** (Start).



7. Wählen Sie **Boot-Option #1** (Startoption 1) aus und legen Sie sie auf Ihren USB-Speicherstick fest.

> **Hinweis**: Verwenden Sie die UEFI-Option (Unified Extensible Firmware Interface).

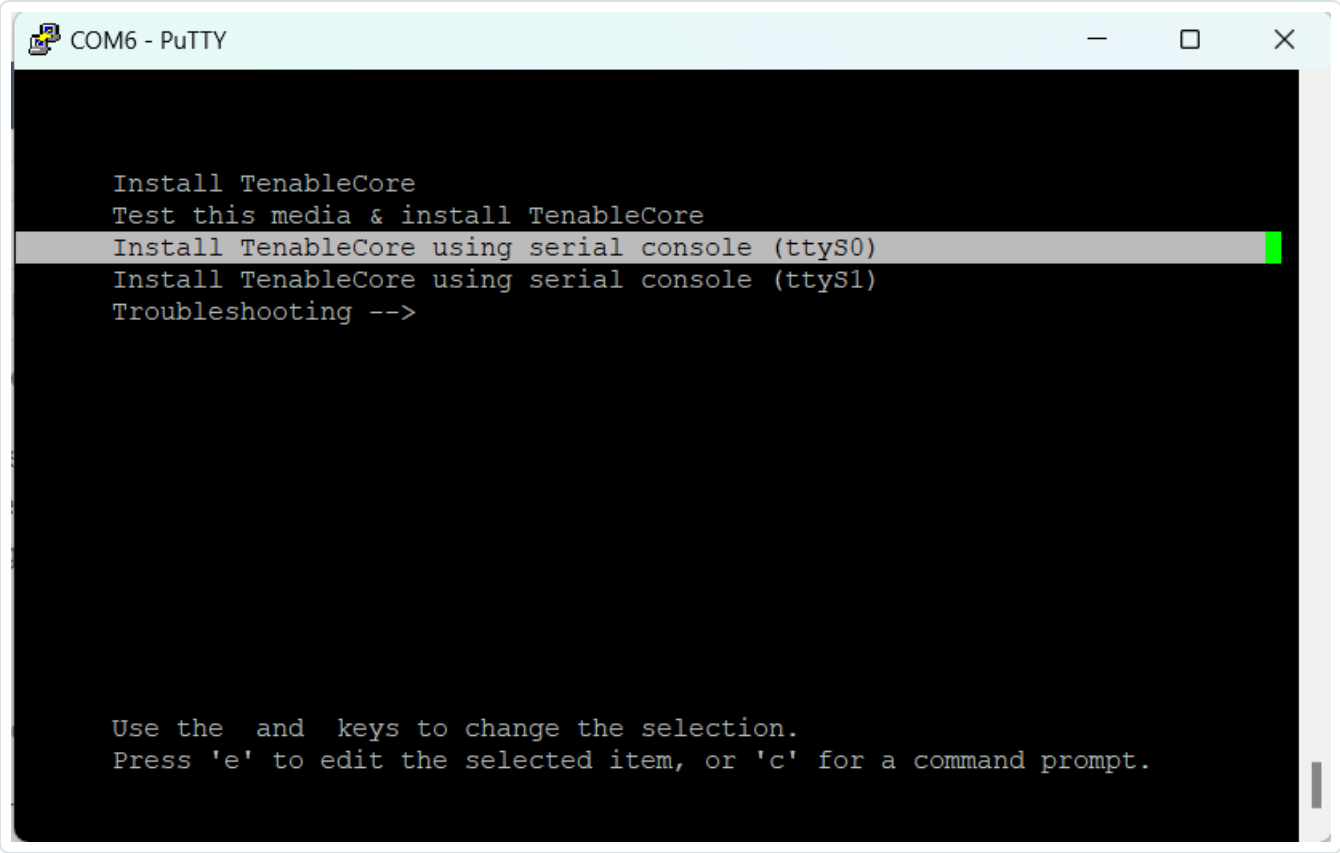


Hinweis: Sie können „One-Shot-Boot“ auf Appliances verwenden, die die Funktion unterstützen.

8. Wählen Sie im Abschnitt **Save & Exit** (Speichern und beenden) die Option **Save Changes and Reset** (Änderungen speichern und zurücksetzen) aus.

9. Wählen Sie nach dem Neustart der Appliance an der Eingabeaufforderung die Option **Install TenableCore using serial console (ttyS0)** (TenableCore über serielle Konsole (ttyS0) installieren) aus. Dadurch wird sichergestellt, dass die Installationsausgabe in den seriellen Konsolenanschluss der Appliance verschoben wird.

Hinweis: Wenn Ihre Hardware eine Monitorausgabe (VGA, HDMI usw.) unterstützt, können Sie die Option **Install TenableCore** (TenableCore installieren) auswählen. In diesem Fall wird die Ausgabe der Installation auf Ihrem angeschlossenen Monitor angezeigt.



Warten Sie, bis die Appliance die Installation abgeschlossen hat. Das System wird möglicherweise mehrmals neu gestartet. Die Installation ist abgeschlossen, wenn eine Login-Eingabeaufforderung angezeigt wird. Auf einigen Appliances wird das System nach Abschluss der Installation möglicherweise standardmäßig heruntergefahren.

> **Hinweis**: Das System führt möglicherweise einige Installationsvorgänge durch, auch nachdem die Login-Eingabeaufforderung angezeigt wird. Tenable empfiehlt, einige Minuten zu warten, bevor Sie den Setup-Assistenten von Tenable Core starten.

10. Trennen Sie den USB-Speicherstick erst, wenn die Installation abgeschlossen ist.

Nächste Schritte

OT Security mit dem Netzwerk verbinden

Virtuelle OT Security ICP-Appliance installieren

Um Tenable Core + OT Security als virtuelle VMware-Maschine bereitzustellen, müssen Sie die OVA-Datei für Tenable Core + OT Security herunterladen und auf einem Hypervisor bereitstellen.

Hinweis: Wenn Sie die `ISO`-Datei anstelle der vorkonfigurierten `OVA`-Datei bereitstellen:

- Befolgen Sie die Systemanforderungen für Tenable Core + OT Security.
- Wenn Sie aufgefordert werden, eine Setup-Methode auszuwählen, wählen Sie **Tenable Core installieren** aus. Siehe Neuinstallation von Tenable Core + Tenable OT Security.
- Verfolgen und überwachen Sie den Installationsprozess über die Installationsbenutzeroberfläche auf der Konsole der virtuellen Maschine. Der Installationsprozess läuft vollständig automatisiert ab. Interagieren Sie daher nicht mit dem System, bis die Installation vollständig abgeschlossen ist.

Bevor Sie beginnen:

- Bestätigen Sie, dass Ihre Umgebung die beabsichtigte Verwendung der Instanz unterstützt, wie unter Systemanforderungen beschrieben.
- Vergewissern Sie sich, dass Ihr Internet- und Port-Zugang die von Ihnen beabsichtigte Nutzung der Instanz unterstützt, wie unter Zugriffsanforderungen beschrieben

So stellen Sie Tenable Core + OT Security als virtuelle Maschine bereit:

1. Laden Sie die `OVA`-Datei für Tenable Core + OT Security von der Tenable Downloads-Seite herunter.
2. Öffnen Sie Ihre virtuelle VMware-Maschine im Hypervisor.
3. Importieren Sie die `OVA`-Datei für Tenable Core + OT Security VMware von Ihrem Computer auf Ihre virtuelle Maschine.
   Informationen zum Konfigurieren Ihrer virtuellen Maschinen finden Sie in der VMware-Dokumentation.
4. Konfigurieren Sie an der Setup-Eingabeaufforderung die virtuelle Maschine so, dass sie den Speicherbedarf Ihres Unternehmens sowie die unter OT SecuritySystemanforderungen beschriebenen Anforderungen erfüllt.
5. Starten Sie Ihre Tenable Core + OT Security-Instanz.

   Der Startvorgang der virtuellen Maschine wird in einem Terminal-Fenster angezeigt. Der Startvorgang kann mehrere Minuten dauern.

Hinweis: Das System führt möglicherweise einige letzte Installationsvorgänge durch, auch nachdem die Login-Eingabeaufforderung angezeigt wird. Tenable empfiehlt, einige Minuten zu warten, bevor Sie den Setup-Assistenten von Tenable Core starten.

Tipp: Wenn Sie Ihren Festplattenspeicher vergrößern möchten, um den Datenspeicherbedarf Ihres Unternehmens zu decken, finden Sie weitere Informationen unter Disk Management.

Nächste Schritte

OT Security mit dem Netzwerk verbinden

OT Security mit dem Netzwerk verbinden

Sie können OT Security sowohl für die Netzwerküberwachung als auch für aktive Abfragen verwenden. Weitere Informationen finden Sie unter Überlegungen zum Netzwerk.

- **Netzwerküberwachung** – Schließen Sie das Gerät an einen Spiegelport am Netzwerk-Switch an, der mit den entsprechenden Controllern/SPS verbunden ist.
- **Aktive Abfragen** – Schließen Sie das Gerät an einen regulären Port mit einer IP-Adresse am Netzwerk-Switch an, der mit den entsprechenden Controllern/SPS verbunden ist.

In der Standardkonfiguration verwenden die aktive Abfrage und die Verwaltungskonsole denselben Port am Gerät (Port 1). Nach der Ersteinrichtung können Sie jedoch den Verwaltungsport vom Port für aktive Abfragen trennen, indem Sie die Verwaltung an Port 3 konfigurieren. Nach dieser Konfiguration können Sie Port 3 am Gerät mit einem regulären Port am Switch verbinden, um die Verwaltung wie unter Separaten Verwaltungsport verbinden (Port-Trennung) beschrieben durchzuführen.

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

So verbinden Sie die OT Security Appliance mit dem Netzwerk:

Auf einer Hardware-Appliance:

1. Schließen Sie an der OT Security Appliance das Ethernet-Kabel (mitgeliefert) an Port 1an.
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.

Auf einer virtuellen Appliance:

Wenn Sie die Appliance mithilfe der `.ova`-Datei bereitgestellt haben, wird die Appliance mit vier Netzwerkschnittstellen vorkonfiguriert geliefert.

Wenn Sie eine benutzerdefinierte virtuelle Appliance mit der `.iso`- oder `.zip`-Datei (Hyper-V) bereitgestellt haben, muss die virtuelle Maschine gemäß den unter Systemanforderungen beschriebenen Anforderungen konfiguriert werden. Weitere Informationen zum Konfigurieren des Netzwerks auf virtuellen Maschinen finden Sie in der VMware-Dokumentation oder der Hyper-V-Dokumentation.

OT Security ICP konfigurieren

Ziel: Vorbereitung der Software auf die Aktivierung.

Nachdem Sie OT Security ICP installiert haben, können Sie OT Security konfigurieren. Die Konfiguration umfasst die folgenden Schritte:

1. Tenable Core einrichten – Führen Sie die Ersteinrichtung für Tenable Core über die CLI oder die Benutzeroberfläche durch.
2. OT Security unter Tenable Core installieren – Installieren Sie OT Security unter Tenable Core.
3. Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren – Konfigurieren Sie die grundlegenden Einstellungen Ihrer OT Security ICP mit dem Setup-Assistenten.

Tenable Core einrichten

Sie können die Erstkonfiguration von Tenable Core sowohl über die CLI als auch über die Tenable Core-Benutzeroberfläche durchführen.

Die Verwendung der Tenable Core-Benutzeroberfläche ist obligatorisch, um die Konfiguration für die Bereitstellung virtueller Appliances abzuschließen.

Hinweis: Wenn Sie den Setup-Assistenten nicht innerhalb von etwa 30 Minuten abschließen, starten Sie die Appliance neu.

Erstkonfiguration über die CLI (optional)

So konfigurieren Sie Tenable Core über die CLI:

1. Stellen Sie über die serielle Konsole eine Verbindung zur OT Security Appliance her, wie unter Neuinstallation von Tenable Core + OT Security beschrieben.
2. Loggen Sie sich mit dem Benutzernamen `wizard` und dem Passwort `admin` ein.

   Die Terminaloberfläche **Network Manager** (Netzwerk-Manager) wird angezeigt.

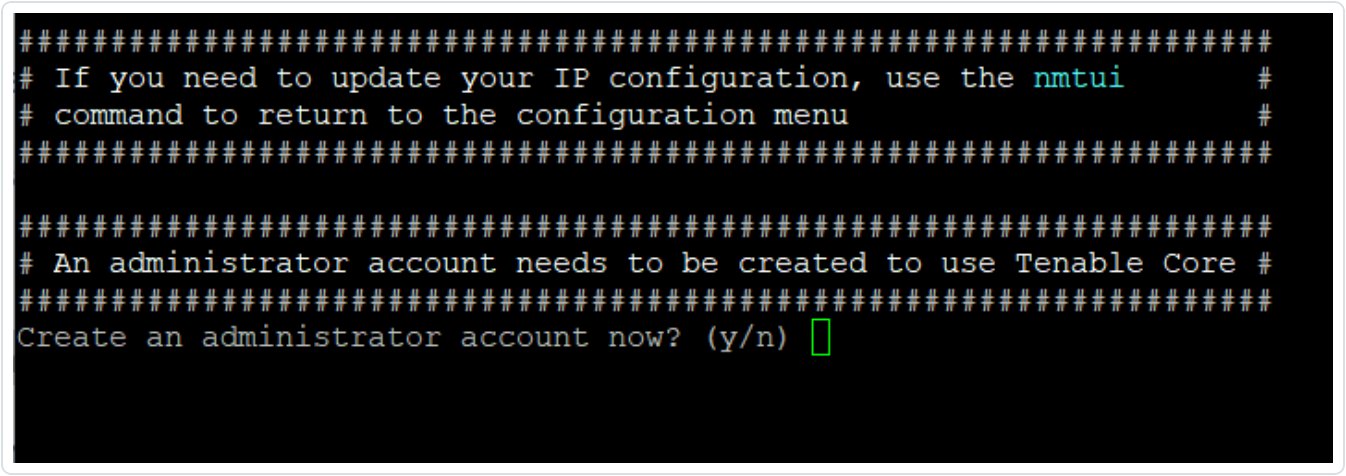
3. (Optional) Geben Sie **y** ein, um die Verwaltungs-IP-Adresse zu konfigurieren.
4. Drücken Sie die **Eingabetaste**.

   Das Fenster **Edit Connection** (Verbindung bearbeiten) wird angezeigt.
5. Navigieren Sie mit den Pfeiltasten und konfigurieren Sie die erforderliche IP-Adresse, das Standard-Gateway, die DNS-Server usw. Sie können diese Konfiguration später ändern.
6. Navigieren Sie mit dem Abwärtspfeil zum unteren Bildschirmrand und wählen Sie **<OK>** aus.

   Das Fenster **Network Manager** (Netzwerk-Manager) wird angezeigt.
7. Wählen Sie **<Quit>** (Beenden).

Hinweis: Standardmäßig ist `nic0` oder Systemport 1mit der IP-Adresse 192.168.1.5/24 vorkonfiguriert. Sie können diese IP-Adresse verwenden, um die Konfiguration des Systems über die Tenable Core-Schnittstelle (Port 8000) von jedem über ein IP-Netzwerk erreichbaren PC abzuschließen.

8. Geben Sie **y** ein und befolgen Sie die Anweisungen, um ein Administratorkonto zu erstellen. Verwenden Sie dieses Konto nur, um sich bei Tenable Core einzuloggen (Terminalkonsole, SSH und Tenable Core-Benutzeroberfläche). Verwenden Sie separate Konten für die OT Security-Anwendung.



9. Nachdem Sie das Konto erstellt haben, verwenden Sie es, um sich über die Konsole oder über eine Netzwerkverbindung beim Terminal einzuloggen: über SSH oder die Tenable Core-Schnittstelle (https://<mgmt-IP>:8000).

Erstkonfiguration über die Tenable Core-Benutzeroberfläche

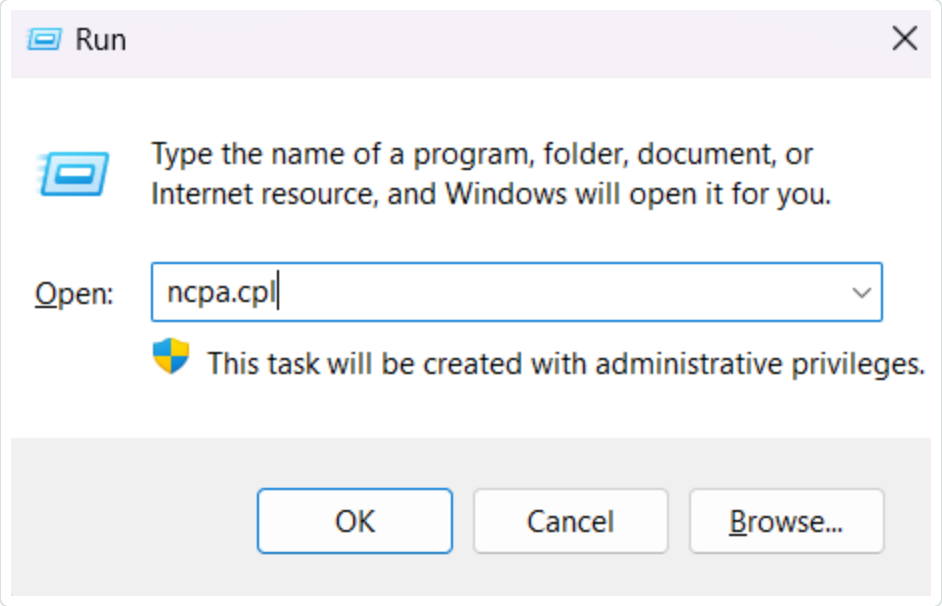
Um die Erstkonfiguration über die Tenable Core-Benutzeroberfläche (verfügbar unter https://<mgmt-IP>:8000) durchzuführen, benötigen Sie eine funktionierende Netzwerkverbindung zur Appliance.

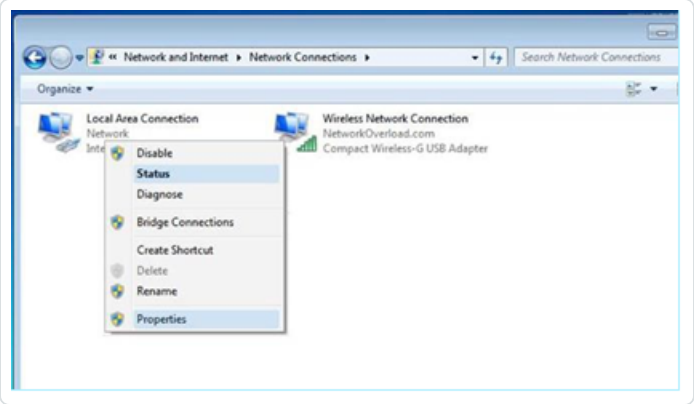
Wenn Sie die Verwaltungs-IP-Adresse nicht konfiguriert haben, können Sie entweder einen direkt verbundenen PC oder ein entsprechend konfiguriertes Netzwerk verwenden, um die Tenable Core-Benutzeroberfläche über eine der folgenden Schnittstellen zu erreichen:

- **port 1** – Standard-Verwaltungsschnittstelle, vorkonfiguriert mit IP-Adresse 192.168.1.5/24
- **port 4** – Engineering-Schnittstelle, vorkonfiguriert mit IP-Adresse 192.168.3.3/24 Sofern keine Änderung erfolgt, kann diese Verbindung für Wiederherstellungsverfahren verwendet werden.

So stellen Sie direkt über Ihren PC oder Laptop eine Verbindung zu Tenable Core her:

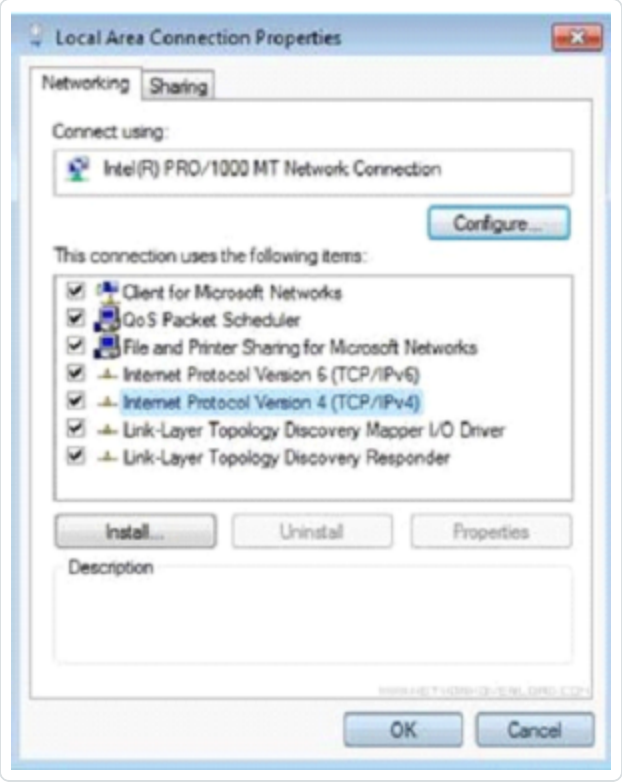
1. Schließen Sie ein Ethernet-Kabel zwischen Ihrem PC und einem der vorkonfigurierten Ports der OT Security Appliance an.
2. Verwenden Sie unter Windows **win+R**, um **Ausführen** zu öffnen, und geben Sie `ncpa.cpl` ein, um **Netzwerkverbindungen** zu öffnen.





3. Klicken Sie mit der rechten Maustaste auf Ihre Netzwerkverbindung (namens **LAN-Verbindung**) und wählen Sie **Eigenschaften** aus.

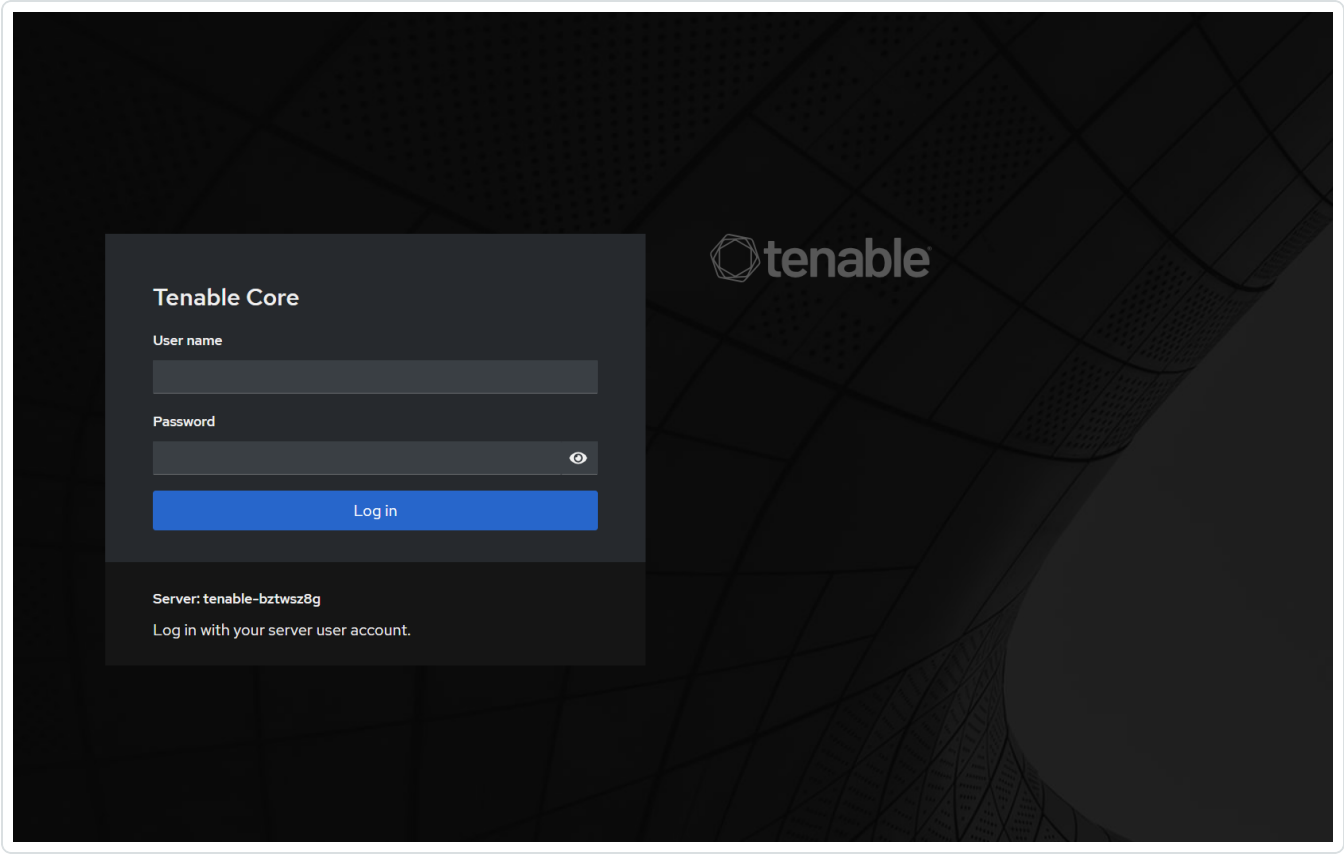
Das Fenster **Eigenschaften für LAN-Verbindung** wird angezeigt.



4. 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.

5. Wählen Sie **Folgende IP-Adresse verwenden** aus.
6. Geben Sie im Feld **IP-Adresse** eine entsprechende IP-Adresse für die Schnittstelle ein, zu der Sie eine Verbindung herstellen. Zum Beispiel 192.168.1.10 als Standardadresse von Port 1/nic0 oder 192.1683.10 als Standardadresse von .
7. Geben Sie in das Feld **Subnetzmaske** 255.255.255.0 ein.
8. Klicken Sie auf **OK**.
9. Navigieren Sie im Chrome-Browser zu https://<mgmt-ip>:8000.



10. Wenn Sie das Administratorbenutzerkonto noch nicht konfiguriert haben, werden Sie vom System aufgefordert, dies jetzt zu tun und sich dann mit Ihrem neu erstellten Benutzer erneut einzuloggen. Weitere Informationen finden Sie unter Create an Initial Administrator User Account.

    Nach Erstellung des Administratorkontos empfiehlt Tenable, die Verwaltungs-IP-Adresse zu konfigurieren. Wenn Sie die **Split-Port**-Konfiguration verwenden möchten, stellen Sie sicher, dass die Schnittstellen die entsprechenden Netzwerke erreichen können. Weitere Informationen finden Sie unter Überlegungen zum Netzwerk.

    > **Hinweis**: Um die Verwaltungs-IP-Adresse zu konfigurieren oder zu ändern, loggen Sie sich wieder bei Tenable Core ein, aktivieren Sie den Administratorzugriff und bearbeiten Sie die Netzwerkkonfiguration.

Nächste Schritte

OT Security unter Tenable Core installieren

OT Security unter Tenable Core installieren

Auf nicht von Tenable bereitgestellter Hardware oder virtuellen Maschinen müssen Sie die Installation der OT Security-Anwendung manuell abschließen.

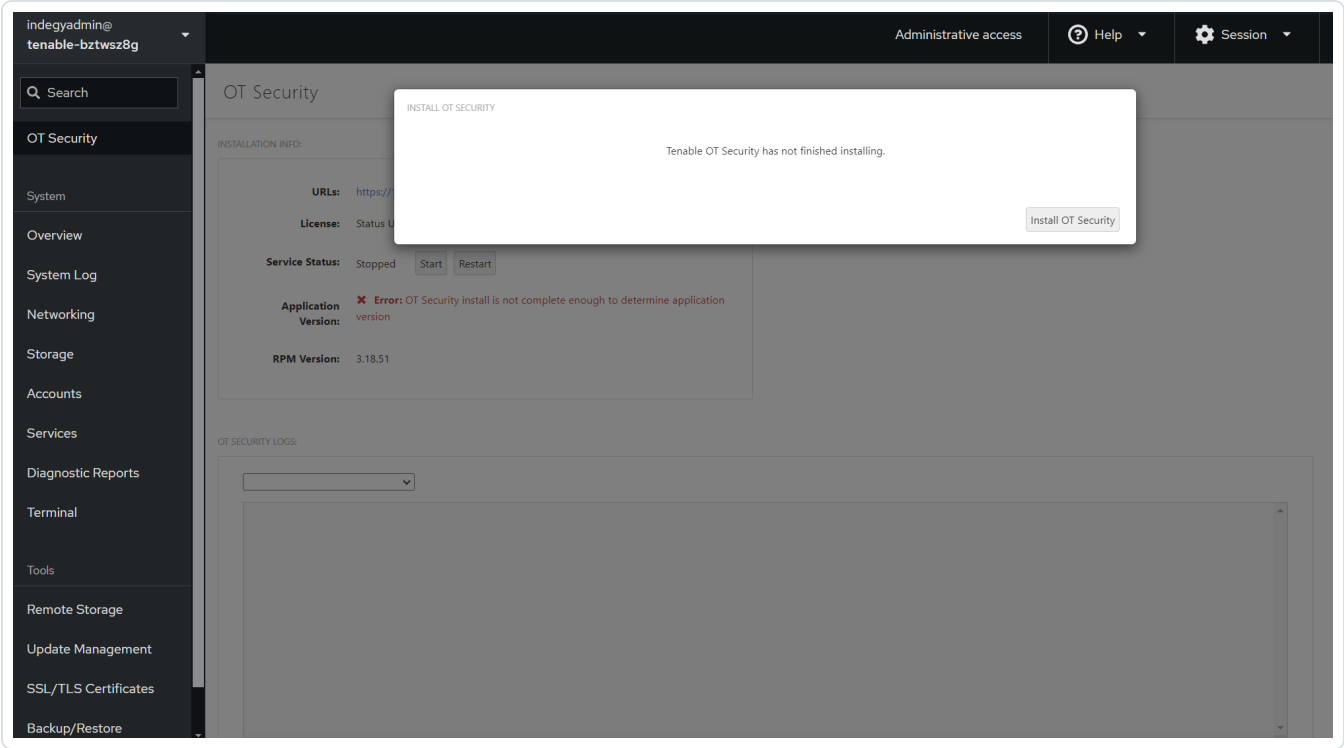
So installieren Sie OT Security unter Tenable Core:

1. Um sich von Ihrem Chrome-Browser aus bei Tenable Core einzuloggen, navigieren Sie zu `https://<mgmt-ip>:8000`.

   Hinweis: Vergewissern Sie sich, dass Sie über Administratorzugriff verfügen.

2. Navigieren Sie zu OT Security.

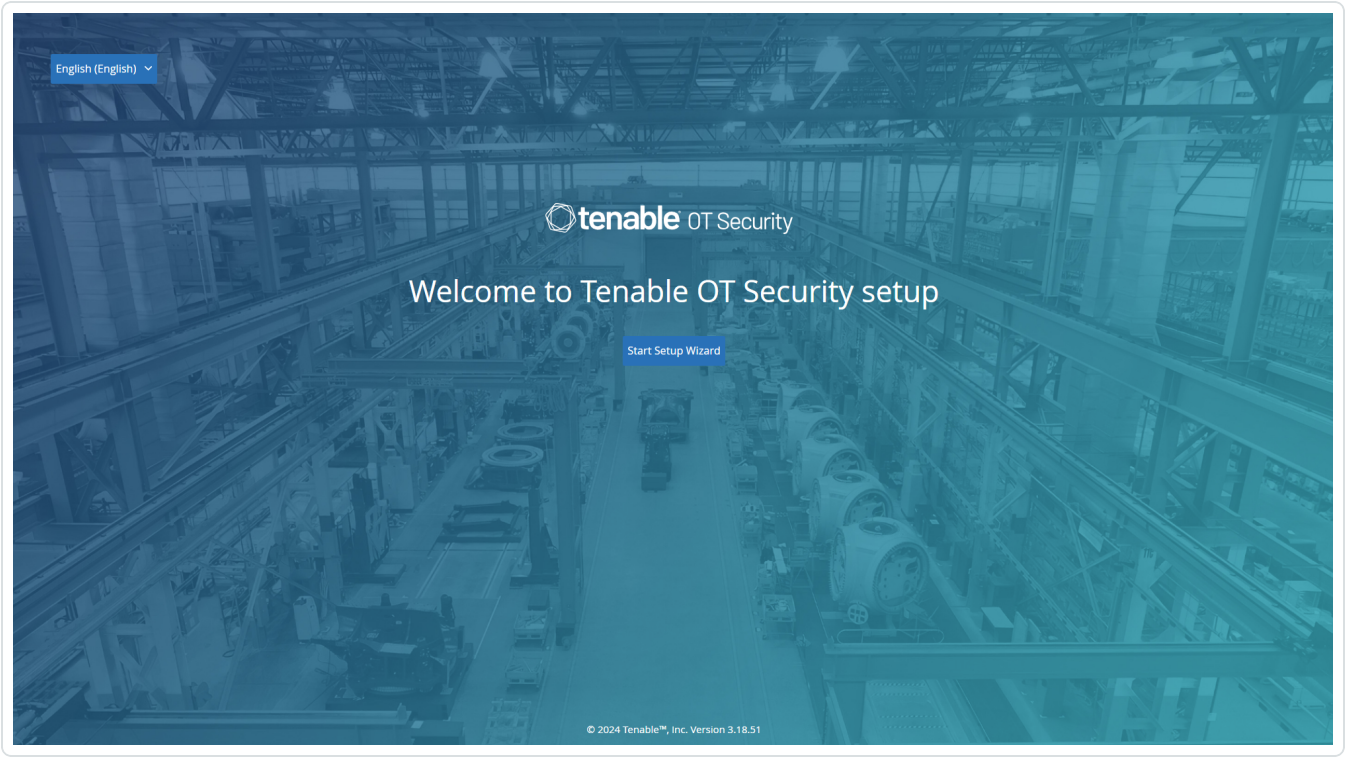
3. Klicken Sie an der Installationsaufforderung auf **Tenable OT Security installieren**.



Hinweis: Der Installationsprozess kann einige Zeit dauern. Unterbrechen Sie den Installationsprozess nicht.

Wenn die Installation abgeschlossen ist, können Sie sich unter `https://<mgmt-ip>` bei der Benutzeroberfläche von OT Security einloggen.

`mgmt-ip` ist Ihre IP-Adresse, die im Feld **URLs** oben im Tenable Core-Fenster angezeigt wird.



Nächste Schritte

Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren

Einstellungen von OT Security mit dem Setup-Assistenten konfigurieren

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

> **Hinweis**: Sie können die Konfiguration bei Bedarf im Bildschirm **Einstellungen** in der Verwaltungskonsole (Benutzeroberfläche) ändern.

Um auf den Setup-Assistenten zuzugreifen, müssen Sie sich zuerst bei der OT Security Verwaltungskonsole einloggen. Informationen zum Einloggen bei der Verwaltungskonsole finden Sie unter Bei der OT Security Verwaltungskonsole einloggen.

Konfigurieren Sie mit dem Setup-Assistenten Folgendes:

1. Benutzerinformationen
2. Gerät

3. Systemzeit
4. Separaten Verwaltungsport verbinden (Port-Trennung)

Hinweis: Nachdem Sie den Setup-Assistenten abgeschlossen haben, werden Sie von OT Security aufgefordert, das System neu zu starten.

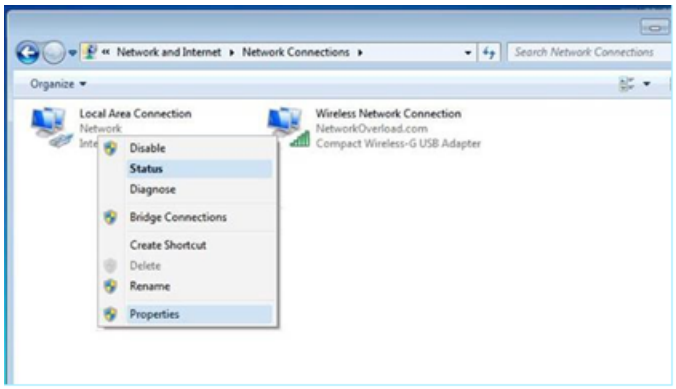
Bei der OT Security Verwaltungskonsole einloggen

So loggen Sie sich bei der OT Security 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 1der OT Security Appliance.
   - Verbinden Sie die Workstation der Verwaltungskonsole mit dem Netzwerk-Switch.

   Hinweis: Stellen Sie sicher, dass die Workstation der Verwaltungskonsole entweder Teil desselben Subnetzes ist wie die OT Security Appliance (192.168. 1.0/24) oder an das Gerät umgeleitet werden kann.
2. Richten Sie wie folgt eine statische IP ein, um eine Verbindung zur OT Security Appliance herzustellen:
   a. Gehen Sie zu **Netzwerk und Internet** > **Netzwerk- und Freigabecenter** > **Adaptereinstellungen ändern**.

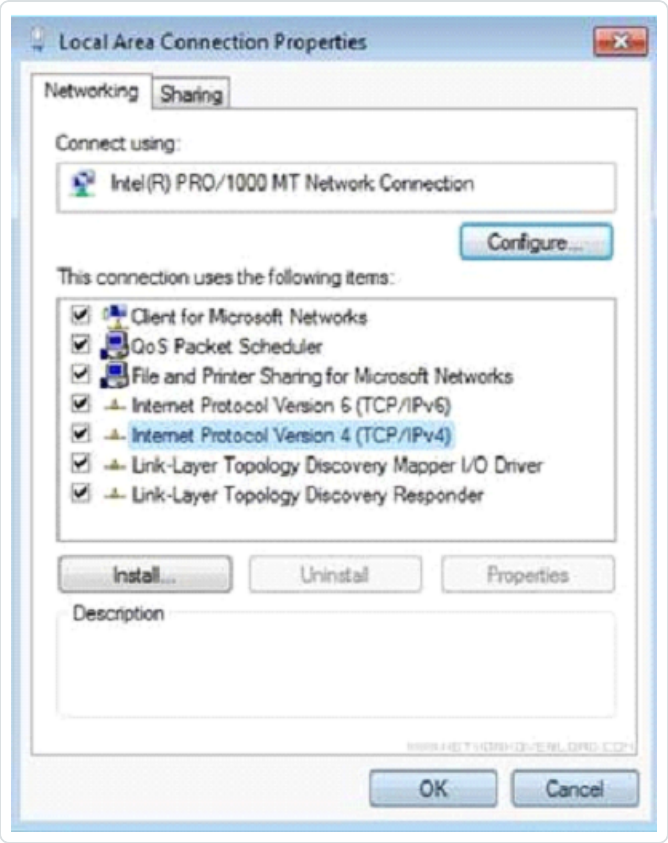
   Der Bildschirm **Netzwerkverbindungen** wird angezeigt.



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

b. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung** und wählen Sie **Eigenschaften** aus.

   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 in das Feld **IP-Adresse** 192.168.1.10 ein.

f. Geben Sie in das Feld **Subnetzmaske** 255.255.255.0 ein.

g. Klicken Sie auf **OK**.

   OT Security wendet die neuen Einstellungen an.

h. Navigieren Sie im Chrome-Browser zu https://192.168.1.5.

   Der **Begrüßungsbildschirm** des Setup-Assistenten wird geöffnet.

Hinweis: Für den Zugriff auf die Benutzeroberfläche ist die neueste Version von Chrome erforderlich.

i. Klicken Sie auf **Setup starten**.

Der Setup-Assistent wird geöffnet und zeigt die Seite **Benutzerinformationen** an.

Nächste Schritte

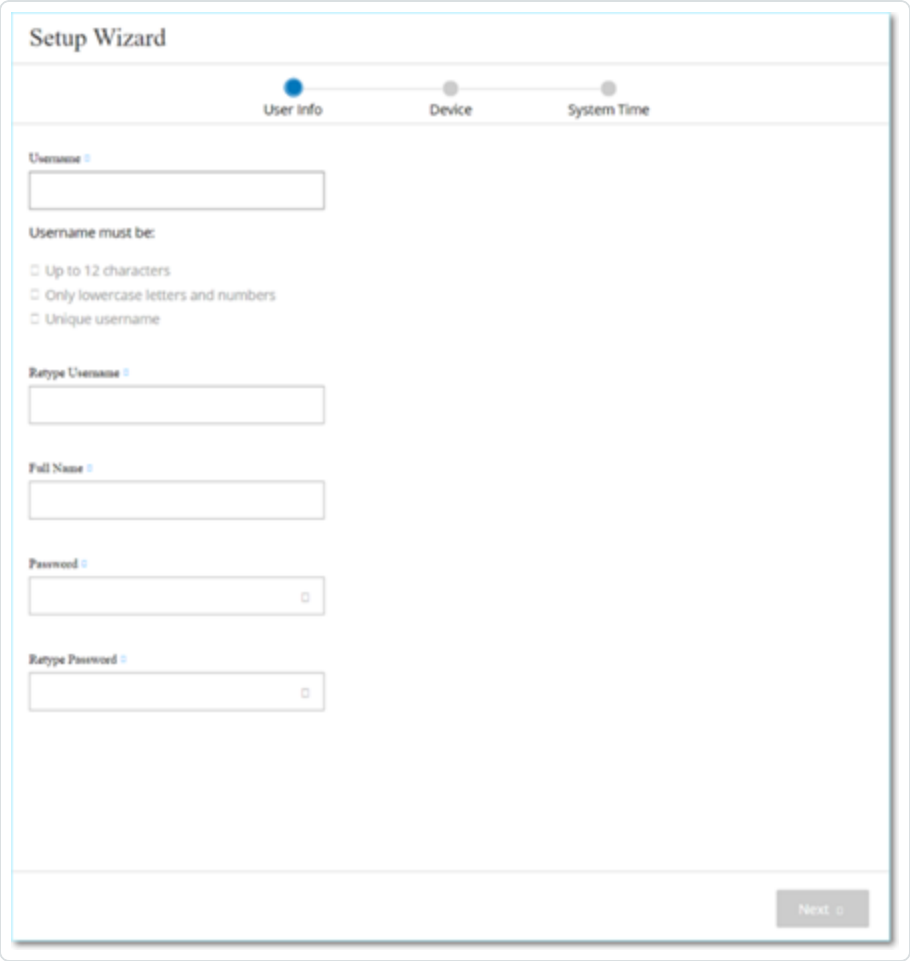
Benutzerinformationen

Benutzerinformationen

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

Hinweis: Sie können die Konfiguration bei Bedarf im Bildschirm **Einstellungen** in der Verwaltungskonsole (Benutzeroberfläche) ändern.

Benutzerinformationen



Geben Sie auf der Seite **Benutzerinformationen** die Informationen zu Ihrem Benutzerkonto ein.

Hinweis: Im Setup-Assistenten können Sie die Zugangsdaten für ein Administratorkonto konfigurieren. 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 zum Einloggen beim System ein.

   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 Benutzernamen erneut ein.
3. Geben Sie im Abschnitt **Vollständiger Name** Ihren vollständigen **Vor- und Nachnamen** ein.

   Hinweis: Dies ist der Name, der in der Kopfleiste und in Ihren Aktivitätsprotokollen im System angezeigt wird.

4. Geben Sie im Feld **Passwort** ein Passwort zum Einloggen beim System ein.
   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.

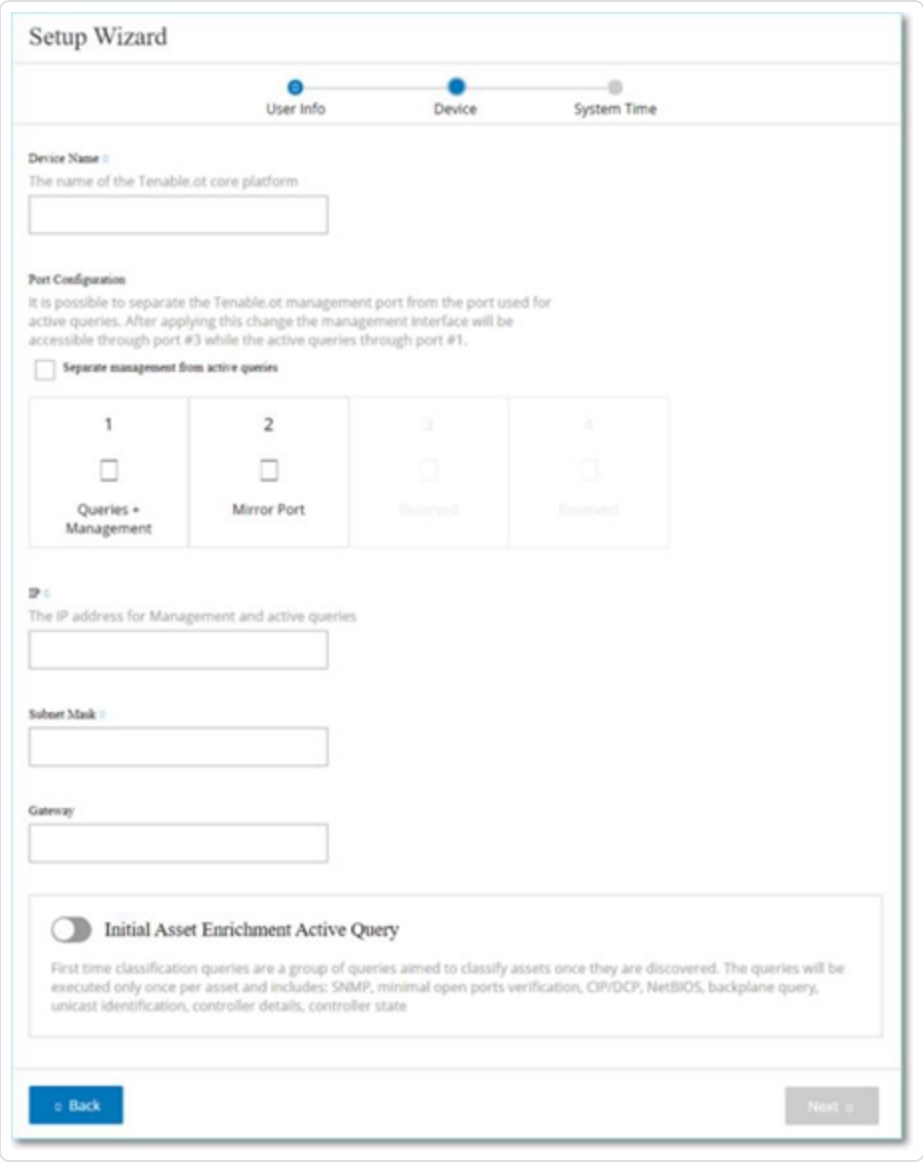
Nächste Schritte

Das Gerät konfigurieren

Gerät

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

> **Hinweis**: Sie können die Konfiguration bei Bedarf im Bildschirm **Einstellungen** in der Verwaltungskonsole (Benutzeroberfläche) ändern.



Geben Sie auf der Seite **Gerät** Informationen zur OT Security-Plattform an:

1. Geben Sie im Feld **Gerätename** eine eindeutige Kennung für die OT Security-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**. Bei Auswahl dieser Option wird Port 1als Port nur für Abfragen und Port 3 als Port nur für die Verwaltung konfiguriert.

> **Hinweis**: 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 das Kontrollkästchen **Verwaltung von aktiven Abfragen trennen** nicht. In diesem Fall können Sie Schritt 3 dieses Verfahrens überspringen und mit Schritt 4 fortfahren.

3. Wenn Sie die Option für die **Port-Trennung** auswählen:

   a. Geben Sie im Feld **IP für aktive Abfragen** die IP-Adresse des Abfrageports des Geräts ein.

      Dieser Port ist mit einem regulären Port im Netzwerk-Switch verbunden, der mit den Controllern kommunizieren bzw. zu diesen umgeleitet werden kann. Da OT Security aktiv eine Verbindung zu den Controllern herstellt, benötigt es eine IP-Adresse innerhalb des Subnetzes des Netzwerks.

   b. Geben Sie im Feld **Die Subnetzmaske für aktive Abfragen** die Subnetzmaske des Abfrageports ein.

   c. Geben Sie im Feld **Das Gateway für aktive Abfragen** (optional) die IP-Adresse des Gateways im Betriebsnetzwerk ein.

4. Geben Sie im Feld **Management-IP** eine IP-Adresse (innerhalb des Netzwerk-Subnetzes) ein, die auf die OT Security-Plattform angewendet werden soll.

   Diese wird zur IP-Adresse für die Verwaltung von OT Security. Diese IP-Adresse ist auch Adresse für Abfragen, wenn keine Trennung zwischen den Ports festlegt wurde.

5. Geben Sie im Feld **Management-Subnetzmaske** die Subnetzmaske des Netzwerks ein.

6. (Optional) Wenn Sie ein Gateway einrichten möchten, geben Sie im Feld **Management-Gateway** die Gateway-IP für das Netzwerk ein.

   > **Hinweis**: Wenn Sie die Management-Gateway-IP nicht angeben, kann OT Security nicht mit externen Komponenten außerhalb des Subnetzes, wie E-Mail-Servern, Syslog-Servern usw., kommunizieren.

7. **Erste aktive Abfrage für Asset-Anreicherung** umfasst eine Reihe von Abfragen, die für jedes Asset ausgeführt werden, das im System erkannt wird.

   Dies ermöglicht OT Security die Klassifizierung der Assets. Um diese Abfragen für jedes neue Asset auszuführen, das OT Security erkennt, stellen Sie den Umschalter **Erste Abfrage für Asset-Anreicherung** auf „Ein“.

8. Klicken Sie auf **Weiter**.

   Die Seite **Systemzeit** des Setup-Assistenten wird geöffnet.

Nächste Schritte

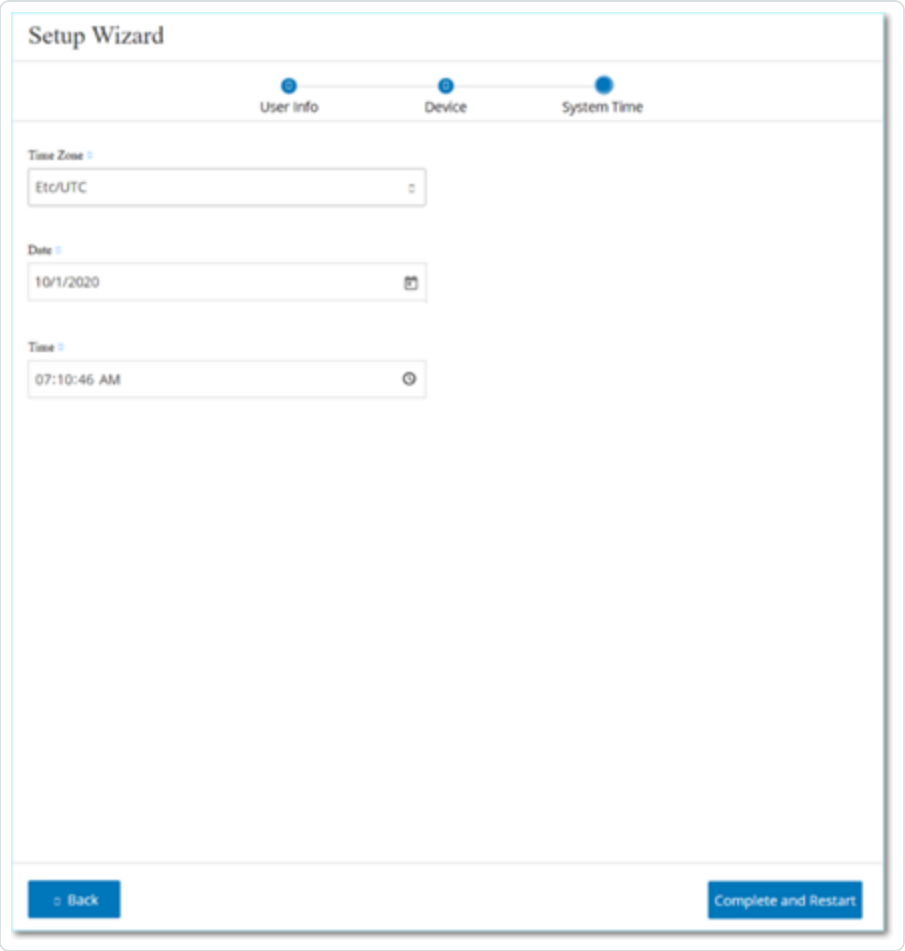
Systemzeit-Einstellungen konfigurieren

Systemzeit

Der Setup-Assistent von OT Security führt Sie durch die Konfiguration der grundlegenden Systemeinstellungen.

> **Hinweis**: Sie können die Konfiguration bei Bedarf im Bildschirm **Einstellungen** in der Verwaltungskonsole (Benutzeroberfläche) ändern.

Systemzeit

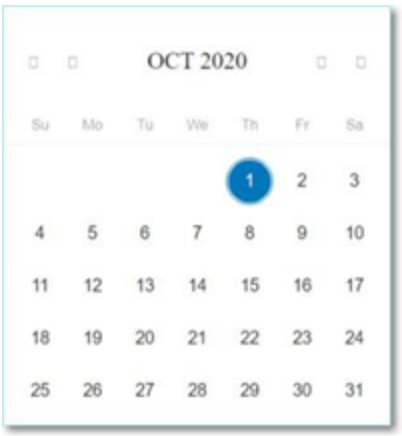


Hinweis: Die Einstellung des richtigen Datums und der richtigen Uhrzeit ist für die genaue Aufzeichnung von Protokollen und Warnungen unerlässlich.

Auf der Seite **Systemzeit** werden die korrekte Uhrzeit und das Datum automatisch angezeigt. Wenn dies nicht der Fall ist, gehen Sie wie folgt vor:

1. Wählen Sie im Dropdown-Feld **Zeitzone** 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** Stunden, Minuten und Sekunden AM/PM aus und geben Sie die richtige Zahl entweder über die Tastatur oder die Aufwärts- und Abwärtspfeile ein.

   > **Hinweis**: 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 das Setup abzuschließen, klicken Sie auf **Abschließen und neu starten**.

   Sobald der Neustart abgeschlossen ist, leitet OT Security Sie zum Bildschirm **Lizenzierung** weiter.

   > **Hinweis**: Wenn Sie die Option für die Port-Trennung ausgewählt haben, ändern Sie Ihre Netzwerkverbindungen wie unter Separaten Verwaltungsport verbinden (Port-Trennung) beschrieben.

Nächste Schritte

Führen Sie Folgendes durch:

- Separaten Verwaltungsport verbinden (Port-Trennung)
- Lizenzaktivierung für OT Security

Separaten Verwaltungsport verbinden (Port-Trennung)

Wenn Sie die Option zur **Port-Trennung** ausgewählt haben (um Abfragen von der Verwaltung zu trennen), müssen Sie Port 3 auf der OT Security Appliance (jetzt der Verwaltungsport) mit einem

Port an 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 an der OT Security Appliance ein Ethernet-Kabel (mitgeliefert) an Port 3 an.
2. Schließen Sie das Kabel an einen Port an einem Netzwerk-Switch an.

Nächste Schritte

Lizenzaktivierung für OT Security

Lizenzaktivierung für OT Security

Ziel: Freischaltung von Systemfunktionen durch Lizenzaktivierung.

Tenable berechnet Lizenzen basierend auf der Anzahl eindeutiger IP-Adressen im System. Jede IP-Adresse erfordert eine separate Lizenz. Beispiel: Tenable basiert die Lizenzierung auch dann auf der Anzahl eindeutiger IP-Adressen, wenn mehrere Geräte dieselbe IP-Adresse nutzen (mehrere Geräte, die mit derselben Backplane verbunden sind und dieselben drei IP-Adressen verwenden). Deshalb benötigen Sie drei Lizenzen, unabhängig von der Anzahl der Geräte.

Nachdem Sie die OT Security Appliance installiert haben, können Sie Ihre Lizenz aktivieren.

Hinweis: Um Ihre OT Security-Lizenz zu aktualisieren oder neu zu initialisieren, wenden Sie sich an Ihren Tenable Account Manager. Sobald Ihr Tenable Account Manager Ihre Lizenz aktualisiert hat, können Sie Ihre Lizenz aktualisieren oder neu initialisieren.

Informationen zur Bereitstellung und Lizenzierung von Tenable OT Security für Tenable One finden Sie im Tenable One Deployment Guide.

Bevor Sie beginnen

- Installieren Sie die OT Security Appliance.
- Vergewissern Sie sich, dass Ihnen der Lizenzcode (20 Buchstaben/Ziffern) vorliegt, den Sie bei der Bestellung des Geräts von Tenable erhalten haben.

- Vergewissern Sie sich, dass Sie Zugang zum Internet haben. Wenn Ihr OT Security-Gerät nicht mit dem Internet verbunden ist, können Sie die Lizenz von jedem PC aus registrieren.
- Vergewissern Sie sich, dass Sie Zugriff auf das Tenable Account Management-Portal haben. Wenden Sie sich an Ihren Tenable Customer Success Manager, um Zugriff zu erhalten.

OT Security-Lizenz aktivieren

Sie können Ihre OT Security-Lizenz aktivieren und das Tenable Account Management-Portal zum Erstellen neuer Sites für die Verwaltung Ihrer Assets nutzen.

Weitere Informationen zum Account Management-Portal finden Sie in der Dokumentation zum Account Management-Portal.

So aktivieren Sie Ihre OT Security-Lizenz:

1. Melden Sie sich mit Ihrem Community-Konto beim Tenable Account Management-Portal an.

   Die Seite **Account** (Konto) wird mit den Optionen angezeigt, für die Sie Anzeigeberechtigungen haben.

2. Wählen Sie in der linken Navigationsleiste die Option **Products** (Produkte) aus.

   Auf der Seite **My Products** (Meine Produkte) werden alle Ihre Tenable-Produkte aufgelistet.

3. Klicken Sie auf die Tenable OT Security-Lizenz.

   Die Seite **Details** für **Tenable OT Security** wird angezeigt. Die OT Security-Lizenzen werden mit Details wie Kaufdatum, Ablaufdatum und Anzahl der lizenzierten IP-Adressen und Sites angezeigt.

4. Kopieren Sie den 20-stelligen OT Security-Lizenzcode aus der Spalte für den **Aktivierungscode**.

5. Generieren Sie das Aktivierungszertifikat in OT Security:

   a. Gehen Sie in OT Security zur Seite **Lizenzaktivierung**.

   b. Klicken Sie in Schritt 1 auf **Neuen Lizenzcode eingeben**.

      Der Bereich **Neuen Lizenzcode eingeben** wird auf der rechten Seite angezeigt.

c. Fügen Sie im Feld **Lizenzcode** den Code (**Aktivierungscode**) ein, den Sie im Account Management-Portal kopiert haben.

d. Klicken Sie auf **Verifizieren**.

In OT Security wird der Abschnitt **Aktivierungszertifikat generieren** aktiviert.

e. Klicken Sie auf **Zertifikat generieren**.

Der Bereich **Zertifikat generieren** wird auf der rechten Seite angezeigt.

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

OT Security generiert das Zertifikat, das Sie im Tenable Account Management-Portal angeben müssen, um Ihre Sites hinzuzufügen.

6. Navigieren Sie im Tenable Provisioning-Portal zur Seite **Tenable OT Security Provisioning** (Tenable OT Security Bereitstellung) und klicken Sie auf ⊕ **Add Site** (Site hinzufügen).

Das Fenster **Add New Tenable OT Security Site** (Neue Tenable OT Security Site hinzufügen) wird angezeigt.

a. (Optional) Geben Sie im Feld **Label** (Bezeichnung) einen Namen für die Site ein.

b. Geben Sie in das Feld **IPs** die Anzahl der IP-Adressen ein, die Sie dieser Site zuweisen möchten. Verwenden Sie die Schaltflächen **+** und **–**, um den Wert zu erhöhen oder zu verringern.

> **Tipp**: Um die Anzahl der IP-Adressen anzupassen, die der Lizenz zugewiesen sind, können Sie auch den Schieberegler unter dem Feld **IPs** verwenden.

c. Fügen Sie im Feld **Activation Certificate** (Aktivierungszertifikat) das Zertifikat ein, das Sie aus OT Security kopiert haben. Siehe Schritt f.

d. Klicken Sie auf **Erstellen**.

Daraufhin wird ein Dialogfeld mit einem Aktivierungscode angezeigt. Dies ist ein generierter Einmal-Code, den Sie in die OT Security-Instanz kopieren müssen.

e. Klicken Sie auf die Schaltfläche und dann auf **Confirm** (Bestätigen).

Die neue Site wird auf der Registerkarte **Sites** (Sites) angezeigt.

7. Klicken Sie auf der Tenable OT Security-Produktseite im Account Management-Portal auf die Registerkarte **Sites** (Sites).

   Die Registerkarte **Sites** (Sites) wird angezeigt.

8. Um eine Site zu erstellen, klicken Sie auf **Manage Sites** (Sites verwalten) > **Create Site** (Site erstellen).

   Das Fenster **Create New Site** (Neue Site erstellen) wird angezeigt.

   a. (Optional) Geben Sie im Feld **Label** (Bezeichnung) einen Namen für die Site ein.

   b. Geben Sie in das Feld **Size** (Größe) die Anzahl der IP-Adressen ein, die Sie dieser Site zuweisen möchten.

   > **Tipp**: Um die Anzahl der IP-Adressen anzupassen, die der Lizenz zugewiesen sind, können Sie den Schieberegler unter dem Feld **Size** (Größe) verwenden.

   c. Fügen Sie im Feld **Activation Certificate** (Aktivierungszertifikat) das Zertifikat ein, das Sie aus OT Security kopiert haben. Siehe Schritt f.

   d. Klicken Sie auf **Erstellen**.

      Daraufhin wird ein Dialogfeld mit einem Aktivierungscode angezeigt. Dies ist ein generierter Einmal-Code, den Sie in die OT Security-Instanz kopieren müssen.

   e. Klicken Sie auf die Schaltfläche .

   f. Klicken Sie auf **Confirm** (Bestätigen).

9. Navigieren Sie zurück zur OT Security-Instanz und klicken Sie in Schritt 3 im Abschnitt **Aktivierungscode eingeben** auf **Aktivierungscode eingeben**.

   Der Bereich **Aktivierungscode eingeben** wird auf der rechten Seite angezeigt.

10. Fügen Sie im Feld **Aktivierungscode** den generierten Einmal-Code ein, den Sie auf der Seite **Tenable OT Security Account Management** kopiert haben. Siehe Schritt 8e.

11. Klicken Sie auf **Aktivieren**.

    In OT Security wird die Bestätigungsmeldung angezeigt, dass das System erfolgreich aktiviert wurde, und die Benutzeroberfläche von OT Security wird angezeigt.

12. Klicken Sie auf **Aktivieren**.

    OT Security ist jetzt aktiviert und kann verwendet werden.

13. Navigieren Sie zurück zum Tenable Account Management-Portal und aktivieren Sie im Dialogfeld mit dem generierten Einmal-Aktivierungscode das Kontrollkästchen **I confirm I have saved the activation license** (Ich bestätige, dass ich die Aktivierungslizenz gespeichert habe).

14. Klicken Sie auf **Confirm** (Bestätigen).

    Die neu hinzugefügte Site wird auf der Registerkarte **Sites** (Sites) für OT Security angezeigt.

Lizenz aktualisieren

Wenn Sie Ihr Asset-Limit erhöhen, Ihren Lizenzzeitraum verlängern oder Ihren Lizenztyp ändern, können Sie Ihre Lizenz aktualisieren.

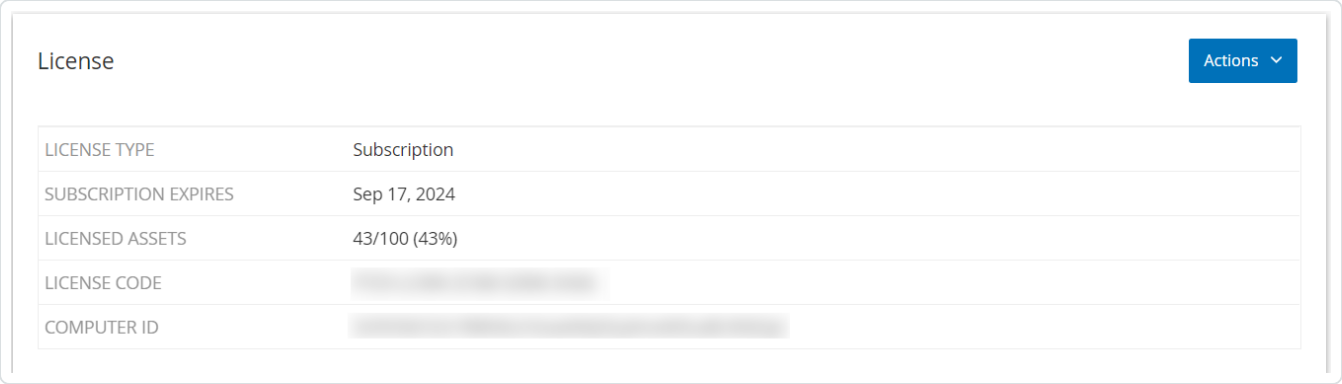
Bevor Sie beginnen

- Ihr Tenable Account Manager muss Ihre Lizenzinformationen bereits in seinem System aktualisiert haben, bevor Sie Ihre Lizenz aktualisieren können.
- Sie benötigen Zugang zum Internet. Wenn Ihr OT Security-Gerät das Internet nicht erreichen kann, können Sie die Lizenz von jedem PC aus registrieren.

So aktualisieren Sie Ihre Lizenz:

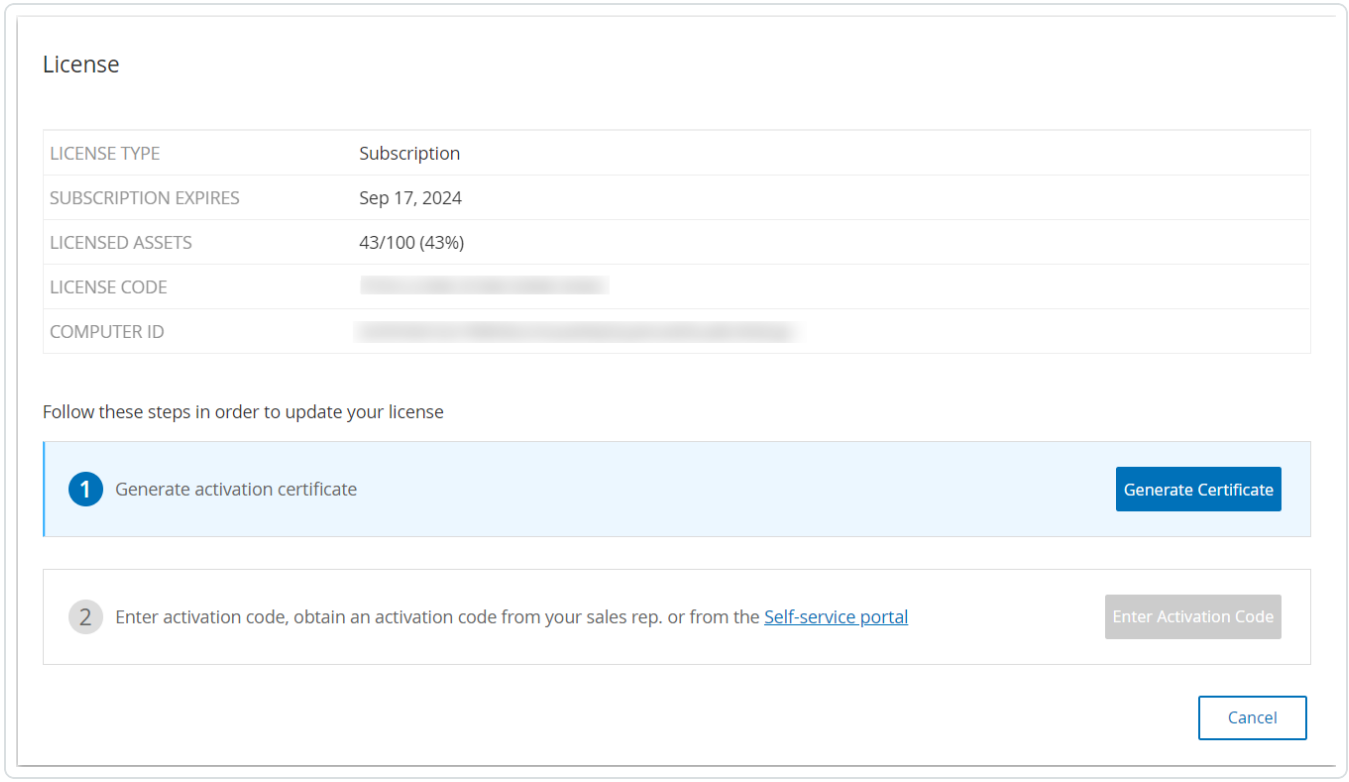
1. Gehen Sie zu **Einstellungen** > **Systemkonfiguration** > **Lizenz**.

   Das Fenster **Lizenz** wird angezeigt.



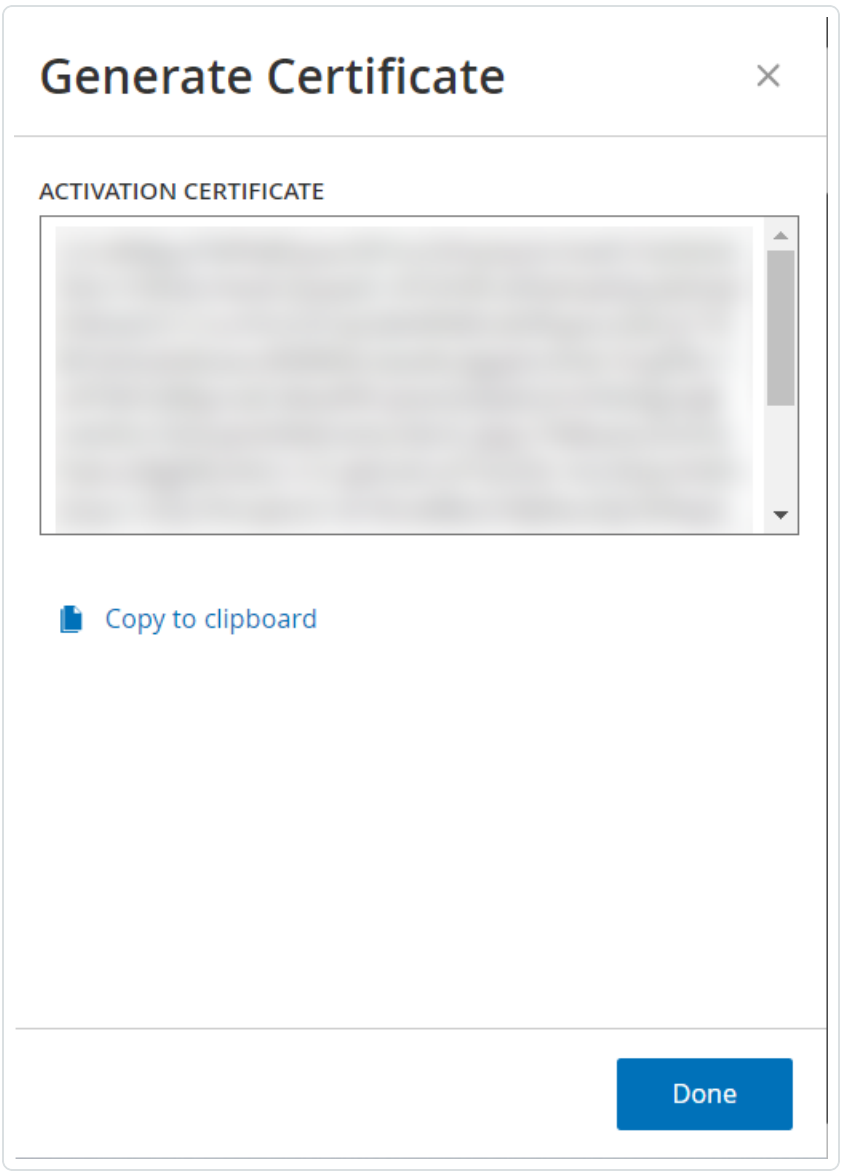
2. Wählen Sie im Menü **Aktionen** die Option **Lizenz aktualisieren** aus.

   Die Schritte **Zertifikat generieren** und **Aktivierungscode eingeben** werden angezeigt.



3. Klicken Sie im Feld **(1) Aktivierungszertifikat generieren** auf **Zertifikat generieren**.

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



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

   Der Seitenbereich wird geschlossen.

5. Bearbeiten Sie die Site-Details im Tenable Account Management-Portal:

   a. Navigieren Sie im Tenable Account Management-Portal zur Seite mit **Tenable OT Security**-Details und klicken Sie in der Zeile der zu aktualisierenden Site auf die Schaltfläche ⋯.

      Ein Menü wird angezeigt.

b. Klicken Sie auf **Edit Site** (Site bearbeiten).

   Das Bearbeitungsfenster für die Site wird angezeigt.

c. Passen Sie die Details nach Bedarf an.

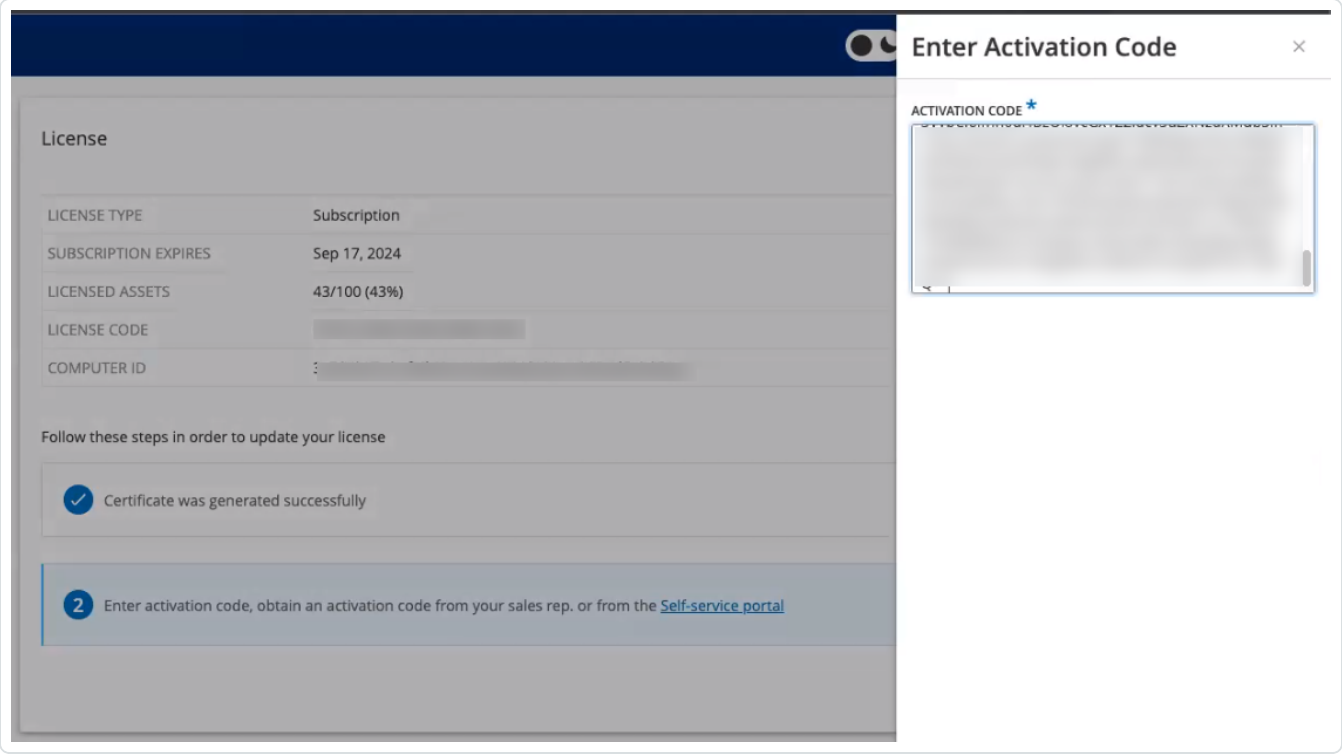
d. Fügen Sie im Feld **Activation Certificate** (Aktivierungszertifikat) das Zertifikat ein, das Sie im Fenster **Zertifikat generieren** in OT Security kopiert haben.

e. Klicken Sie auf **Aktualisieren**.

   Im Portal wird ein Dialogfeld mit einem Aktivierungscode angezeigt. Dies ist ein generierter Einmal-Code, den Sie in die OT Security-Instanz kopieren müssen.

f. Klicken Sie auf die Schaltfläche und dann auf **Confirm** (Bestätigen).

6. Navigieren Sie zurück zur OT Security-Instanz.
7. Klicken Sie im Feld **(2) Aktivierungscode eingeben** auf **Aktivierungscode eingeben**.
8. Fügen Sie im Feld **Aktivierungscode** den generierten Einmal-Code ein, den Sie auf der Seite **Tenable OT Security Account Management** kopiert haben.

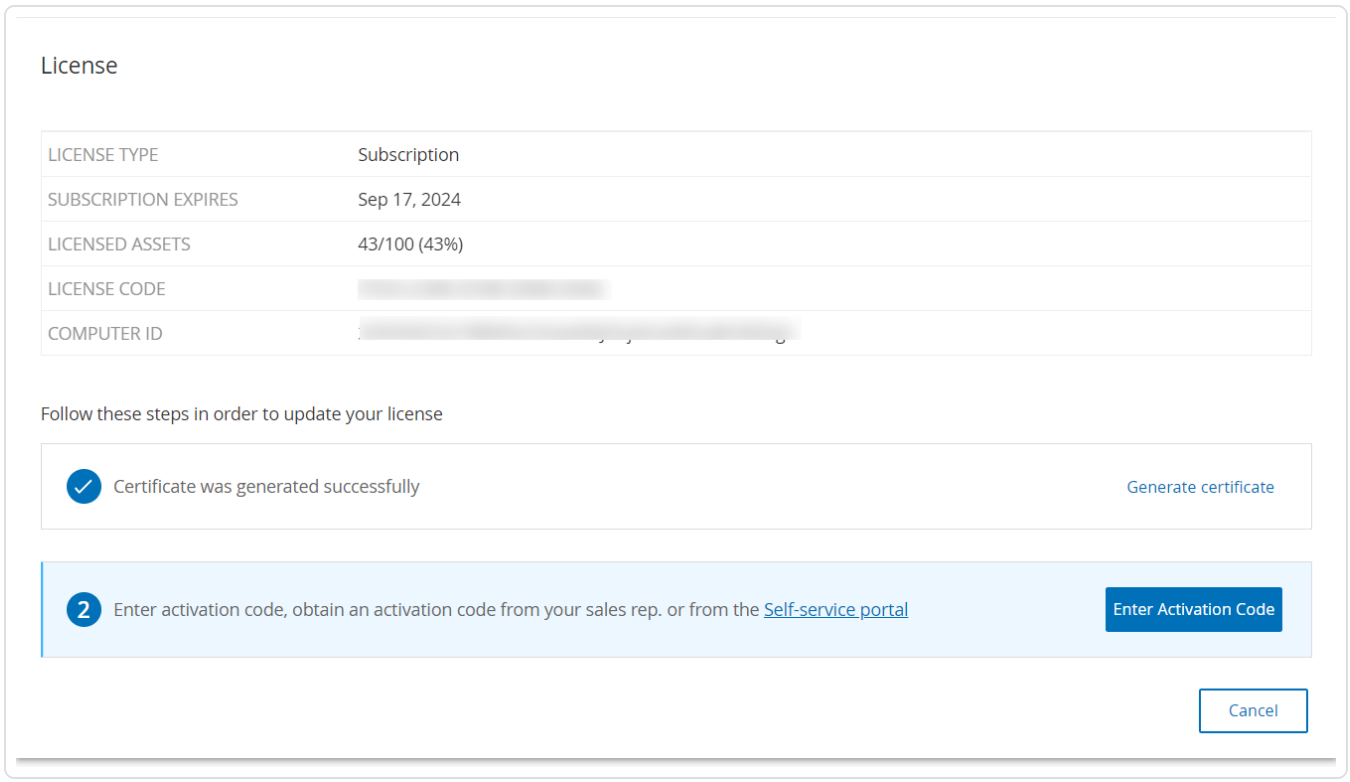


9. Klicken Sie auf **Aktivieren**.

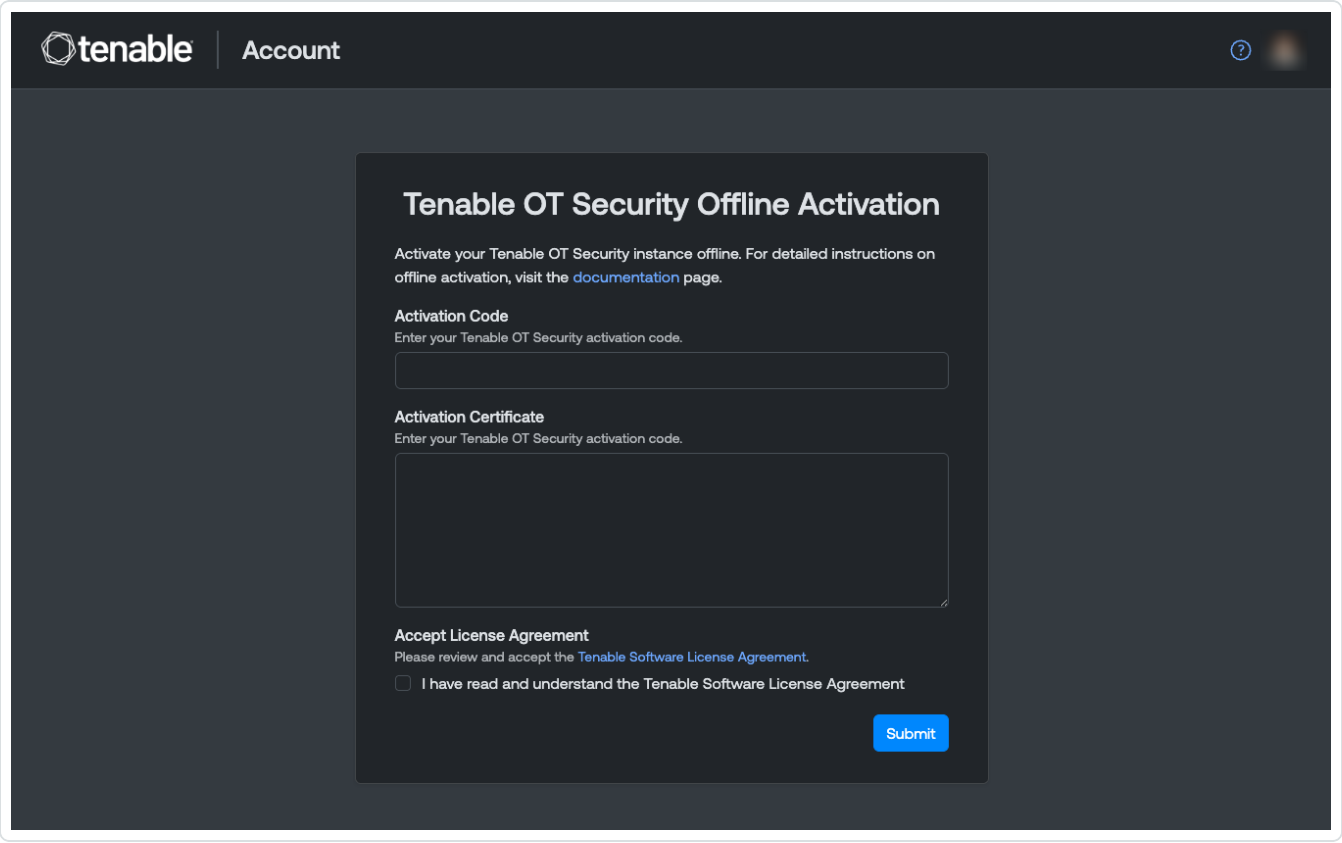
In OT Security wird die Bestätigungsmeldung angezeigt, dass das System erfolgreich aktiviert wurde, und auf der Seite **Lizenz** werden die aktualisierten Lizenzdetails angezeigt.

Lizenz im Offline-Modus aktualisieren

1. Führen Sie die Schritte 1bis 4 wie im Abschnitt Lizenz aktualisieren beschrieben aus.
2. Klicken Sie im Feld **(2) Aktivierungscode eingeben** auf den Link zum Self-Service-Portal.



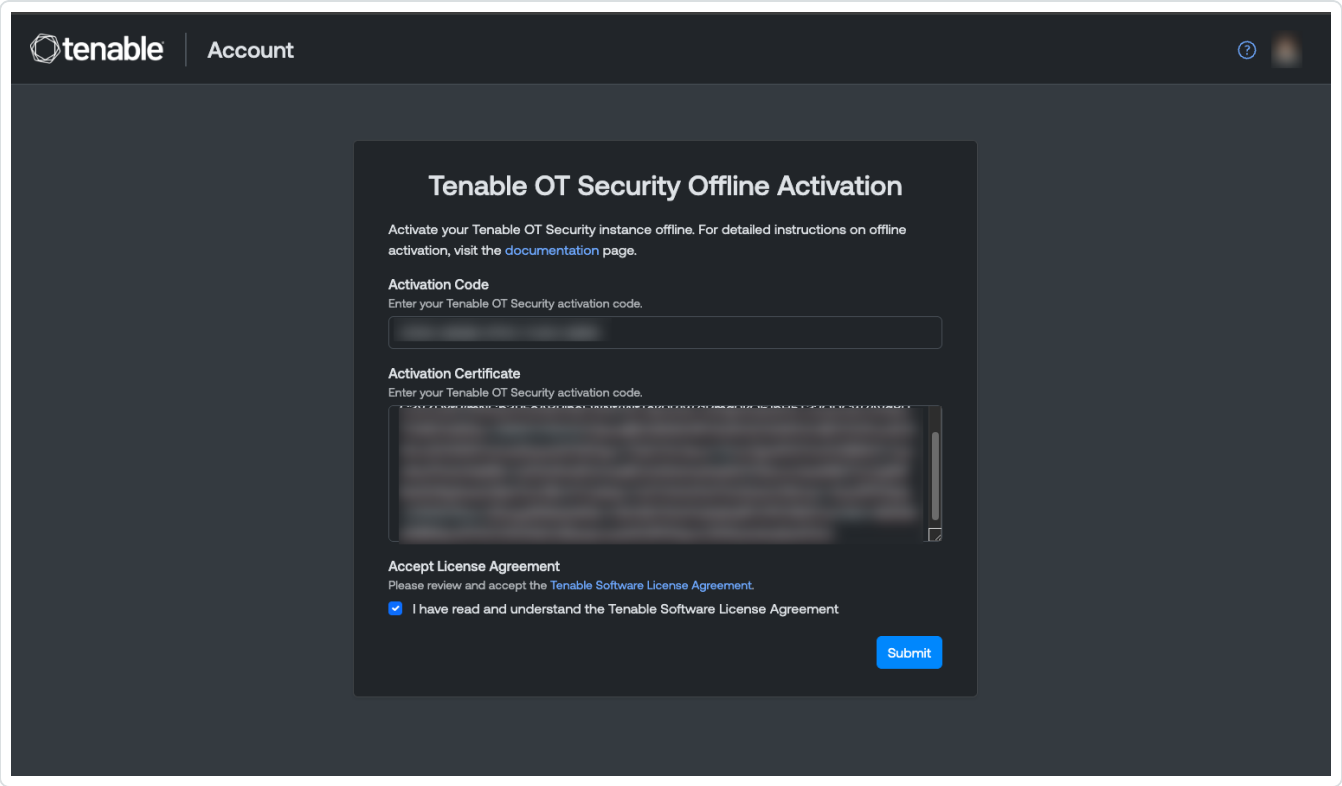
Das Fenster **OT Security offline aktivieren** wird auf einer neuen Registerkarte geöffnet.



Hinweis: Sie können den Bildschirm „OT Security offline aktivieren“ von einem mit dem Internet verbundenen Gerät über die folgende URL aufrufen: https://account.tenable.com/offline-activation/ot-security.

Hinweis: Wenn Sie nicht bei tenable.com eingeloggt sind, können Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort einloggen. Verwenden Sie das E-Mail-Konto, über das Sie Ihren **Lizenzcode** erhalten haben. Wenn Sie keine Login-Zugangsdaten haben, können Sie entweder auf **Passwort vergessen** klicken (und den Anweisungen folgen) oder sich an Ihren Tenable Account Manager wenden.

3. Geben Sie im Feld **Aktivierungscode** Ihren 20-stelligen **Lizenzcode** ein (diesen können Sie im Fenster **Lizenz** kopieren und hier einfügen).
4. Fügen Sie im Feld **Aktivierungszertifikat** das **Aktivierungszertifikat** ein.
5. Aktivieren Sie das Kontrollkästchen **Ich habe die Tenable-Softwarelizenzvereinbarung gelesen und verstanden**.



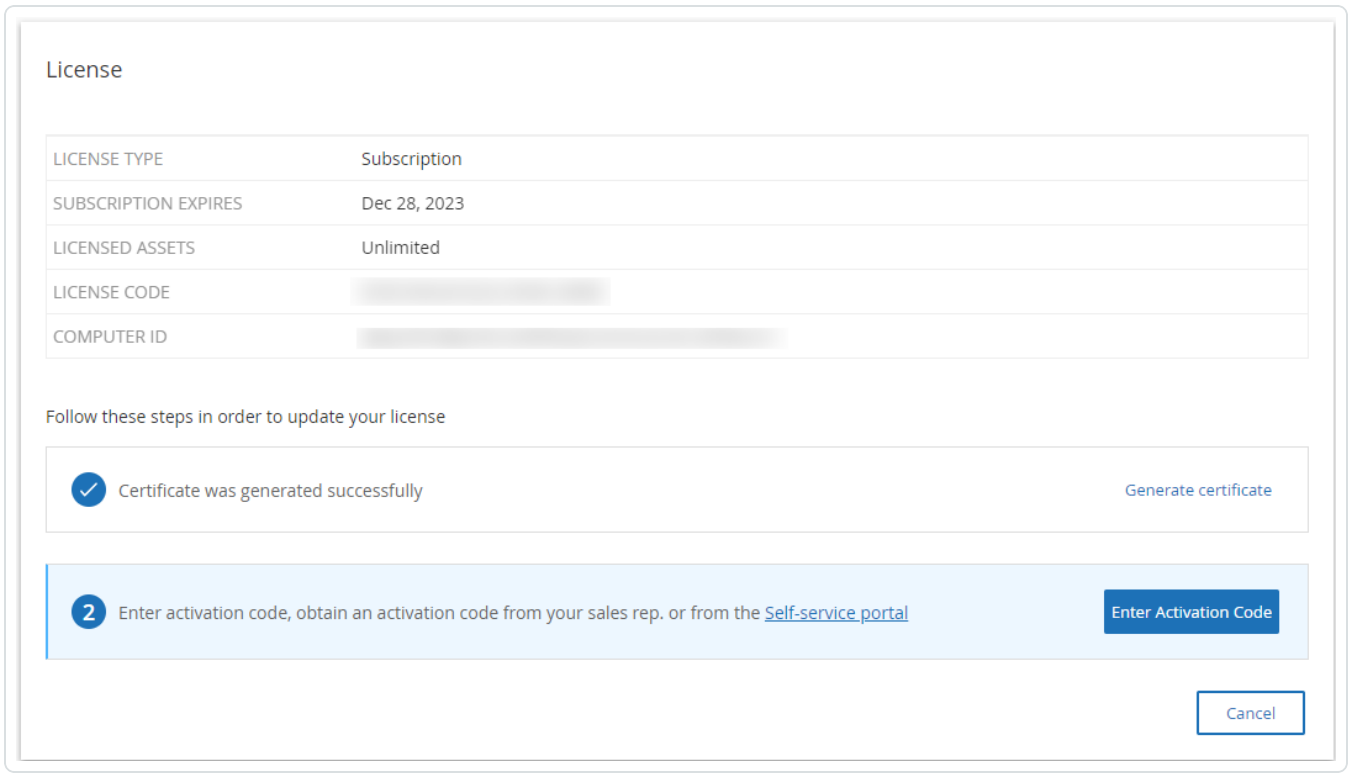
Hinweis: Um die Lizenzvereinbarung anzuzeigen, klicken Sie auf den Link **Tenable-Softwarelizenzvereinbarung**.

6. Klicken Sie auf **Senden**.

   OT Security generiert den Aktivierungscode.

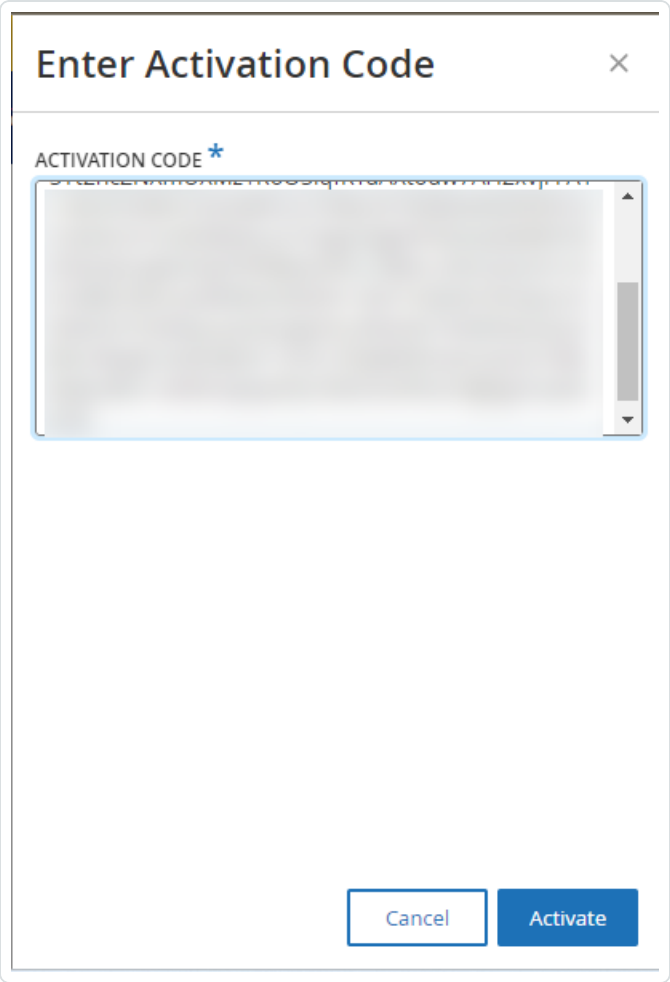
7. Um den Aktivierungscode zu kopieren, klicken Sie auf die Schaltfläche .

8. Navigieren Sie zurück zur Registerkarte **Lizenz** in OT Security und klicken Sie auf **Aktivierungscode eingeben**.



Der Seitenbereich **Aktivierungscode eingeben** wird angezeigt.

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



Der Seitenbereich wird geschlossen und die Lizenz wird von OT Security aktualisiert.

Lizenz neu initialisieren

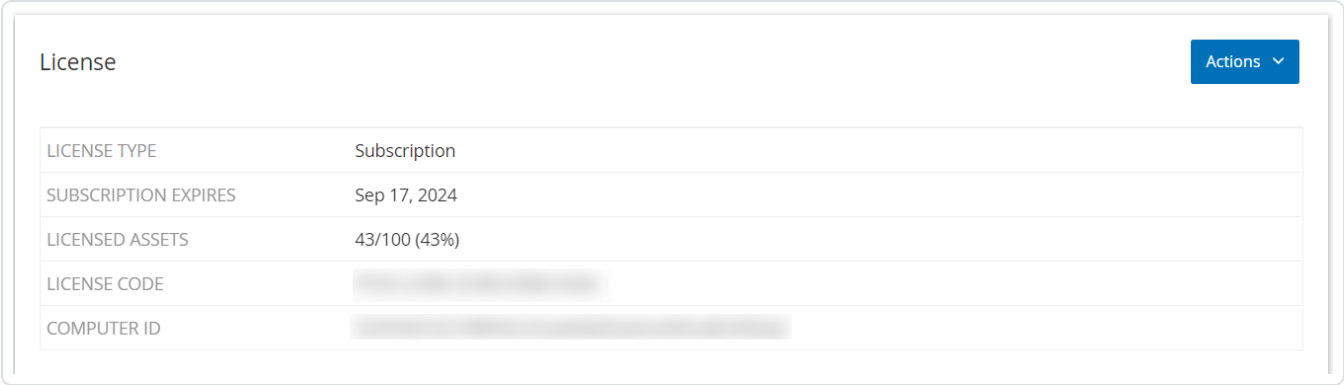
Durch die Neuinitialisierung Ihrer Lizenz wird Ihre aktuelle Lizenz aus dem System entfernt und eine neue Lizenz aktiviert, ähnlich wie bei der Lizenzaktivierung während des Systemstarts. Wenn Sie Ihre Lizenz neu initialisieren müssen (d. h., wenn Sie eine neue Lizenz erhalten), verwenden Sie das folgende Verfahren.

Bevor Sie beginnen

- 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 OT Security-Gerät nicht mit dem Internet verbunden werden kann, können Sie die Lizenz von jedem PC aus registrieren.

So initialisieren Sie Ihre Lizenz neu:

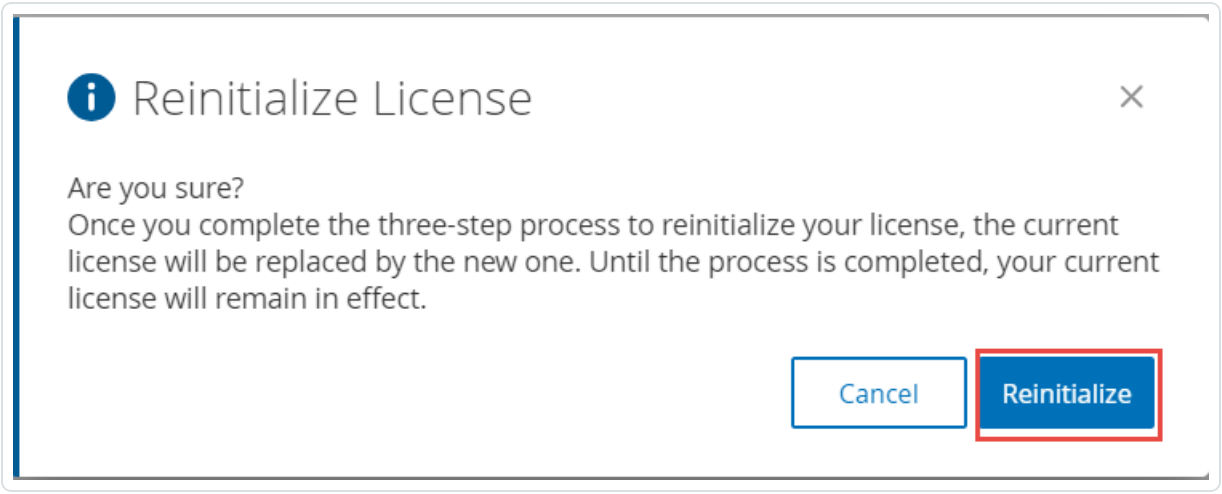
1. Gehen Sie zu **Einstellungen** > **Systemkonfiguration** > **Lizenz**.



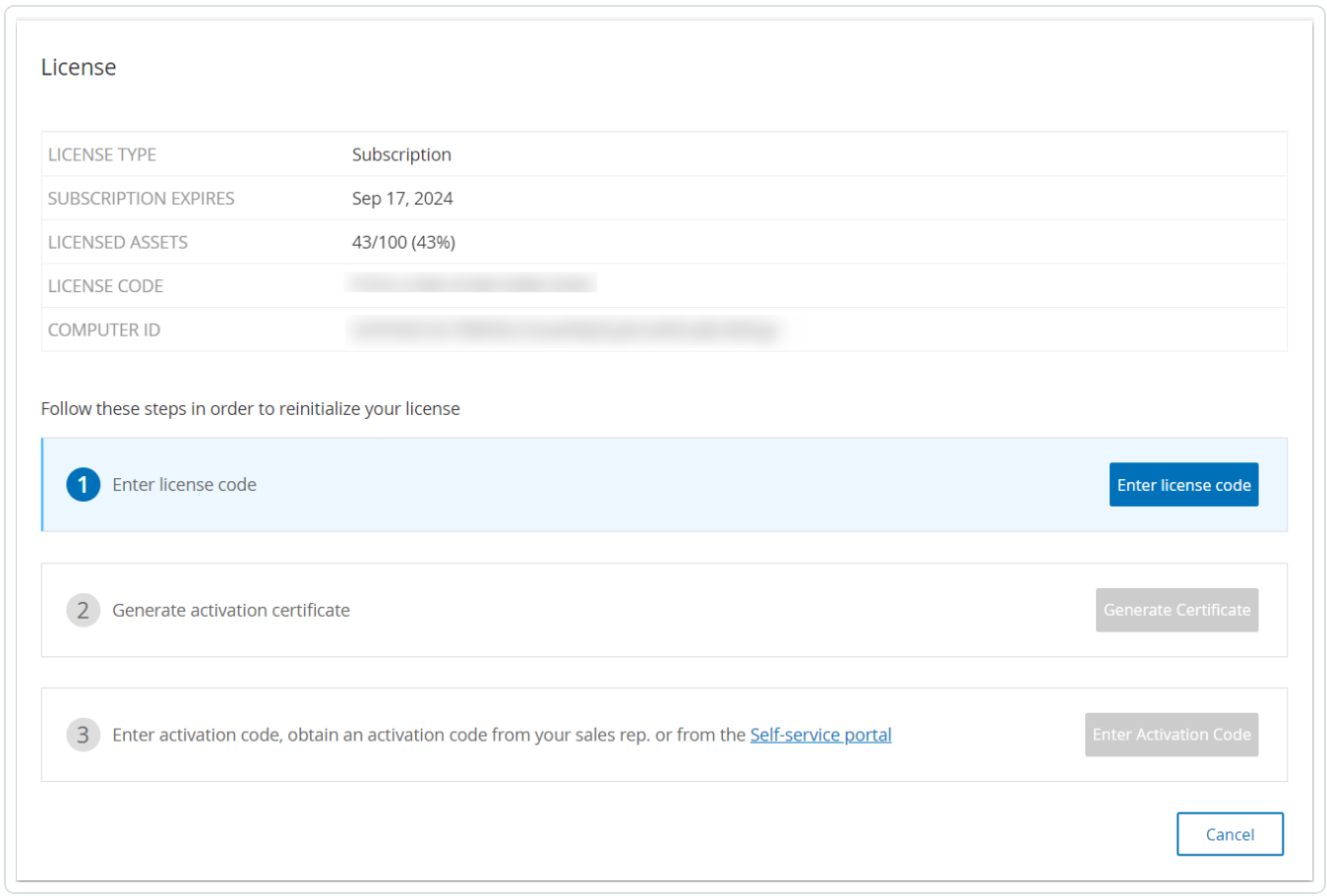
2. Wählen Sie im Menü **Aktionen** die Option **Lizenz erneut initialisieren** aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

3. Klicken Sie auf **Neu initialisieren**.



   Das Fenster **Lizenz** mit den drei Schritten zur Neuinitialisierung wird angezeigt.



4. Befolgen Sie die Schritte zum Systemstart, um Ihre Lizenz zu aktivieren. Siehe Lizenz aktivieren.

   Nachdem Sie Ihren **Aktivierungscode** angegeben haben, wird Ihre aktuelle Lizenz durch Ihre neue Lizenz ersetzt.

Nächste Schritte

Das OT Security-System aktivieren

OT Security starten

Ziel: Start des Systems und seine Nutzung für Ihre OT-Sicherheitsbedürfnisse.

Nachdem Sie Tenable Core + OT Security konfiguriert haben, aktivieren Sie das System, um OT Security zu verwenden.

1. Das OT Security-System aktivieren – Aktivieren Sie das OT Security-System, nachdem Sie Ihre Lizenz aktiviert haben.
2. OT Security verwenden – Konfigurieren Sie Ihre überwachten Netzwerke, die Port-Trennung, Benutzer, Gruppen, Authentifizierungsserver usw. so, dass sie OT Security verwenden.

Das OT Security-System aktivieren

Nach Abschluss der Lizenzaktivierung zeigt OT Security die Schaltfläche **Aktivieren** an.

Aktivieren Sie OT Security, um die Kernfunktionen des Systems zu aktivieren, wie zum Beispiel:

- Identifizieren von Assets im Netzwerk
- Erfassen und Überwachen des gesamten Netzwerk-Traffic
- Protokollieren von „Konversationen“ im Netzwerk

Sie können alle zusammengestellten Daten und Analysen aus diesen Funktionalitäten in der Benutzeroberfläche einsehen.

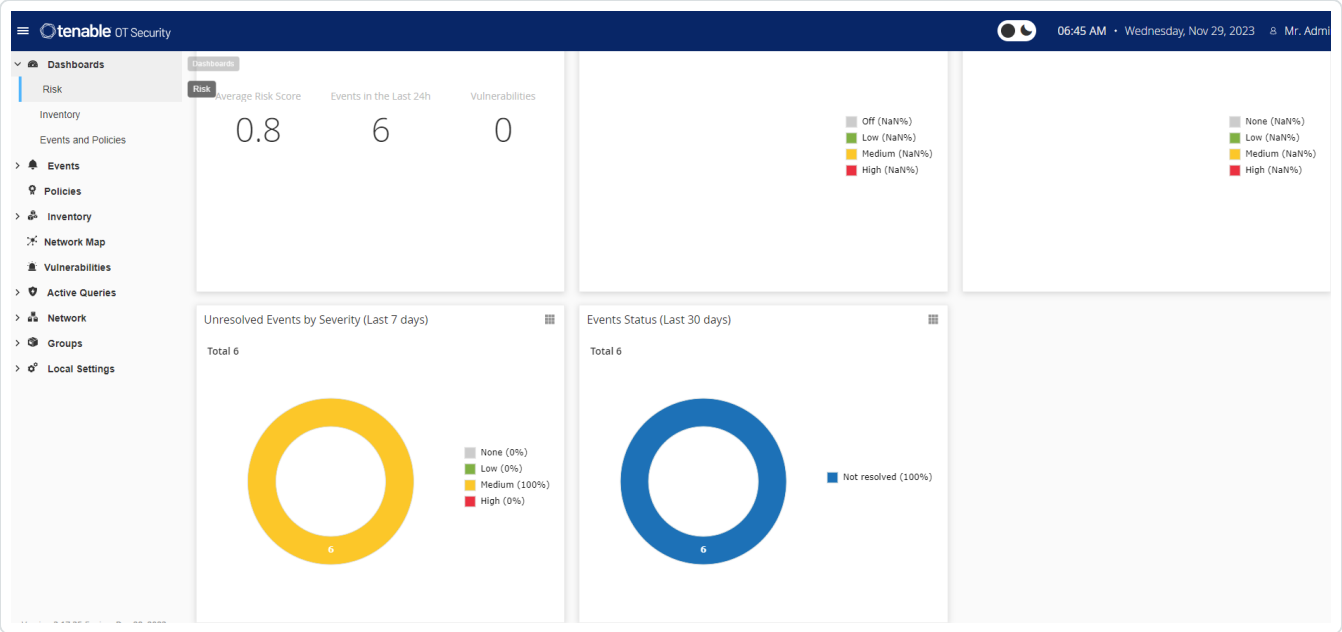
> **Hinweis**: Dies sind laufende Prozesse, die sich über einen längeren Zeitraum erstrecken. Daher kann es einige Zeit dauern, bis in der Benutzeroberfläche vollständig aktualisierte Ergebnisse angezeigt werden.

Sie können zusätzliche Funktionen wie aktive Abfragen im Fenster **Lokale Einstellungen** in der Verwaltungskonsole (Benutzeroberfläche) konfigurieren und aktivieren. Weitere Informationen finden Sie unter Aktive Abfragen.

So aktivieren Sie OT Security:

1. Klicken Sie auf **Aktivieren**.

   OT Security aktiviert das System und zeigt das Fenster **Dashboard** > **Risiko** an.



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

OT Security verwenden

Nach der Installation können Sie OT Security konfigurieren und verwenden.

Überwachte Netzwerke konfigurieren

Konfigurieren Sie die Netzwerksegmente, die OT Security überwachen soll, und stellen Sie sicher, dass alle für Ihr Netzwerk relevanten Bereiche enthalten sind. Siehe Überwachte Netzwerke.

> **Hinweis**: Entfernen Sie nicht benötigte überwachte Netzwerke. Sie können alle Assets ausblenden, die Sie aus diesen Netzwerken hinzugefügt haben. Weitere Informationen finden Sie unter Assets ausblenden.

Ports überprüfen und konfigurieren

Sofern Sie dies noch nicht getan haben, können Sie die Ports für Verwaltung und aktive Abfragen trennen.

Benutzer, Gruppen und Authentifizierungsserver konfigurieren

Legen Sie Ihre lokalen Benutzer und Benutzergruppen fest. Sie können externe Authentifizierungsserver konfigurieren oder SAML für ein einfacheres SSO-Login verwenden.

Netzwerkdienste hinzufügen

Fügen Sie Ihre DNS- und NTP-Server hinzu. Sie können auch Syslog und E-Mail-Server so konfigurieren, dass alle kritischen Ereignisse abgerufen werden.

Aktive Abfragen aktivieren

Aktive Abfragen stellen einen der Hauptvorteile von OT Security dar. Sie können darüber direkt auf Ihre Assets zugreifen, um möglichst genaue und zeitnahe Details und Einblick zu erhalten. Weitere Informationen finden Sie unter Aktive Abfragen.

Aktive Asset-Erfassung – Untersuchen und erfassen Sie proaktiv „stille“ Assets oder Assets, die durch passives Monitoring von Traffic nicht abgedeckt werden.

Nessus-Scans erstellen

Konfigurieren Sie Nessus-Scans für IT-Geräte in Ihrem OT Security-Netzwerk. Tenable Nessus-Scans sind sicher und betreffen nur erfasste IT-Assets. Weitere Informationen finden Sie unter Nessus-Plugin-Scans erstellen.

Sicherungen einrichten

Konfigurieren Sie regelmäßige Systemsicherungen und entscheiden Sie, ob Sie diese lokal speichern oder in einen Remote-Speicher exportieren möchten. Weitere Informationen finden Sie unter Application Data Backup and Restore.

Updates abrufen

Achten Sie unbedingt darauf, Feed- und System-Updates zu überprüfen. Wenn Ihr System offline ist, sollten Sie regelmäßig ein manuelles Update durchführen. Weitere Informationen finden Sie unter Updates.

Optimieren

Wenn OT Security eingerichtet ist und ausgeführt wird, sehen Sie sich die generierten Ereignisse an und optimieren Sie Ihre Richtlinien entsprechend den Anfoderungen Ihrer Umgebung.

Integrieren

Integrieren Sie OT Security mit anderen Tenable-Produkten oder Drittanbieterdiensten. Weitere Informationen finden Sie unter Integrationen.

OT Security Sensor installieren

Hinweis: Dieser Abschnitt beschreibt das Verfahren zur Konfiguration eines Sensors ab Version 3.14.

Die Installation des OT Security-Sensors umfasst die Kopplung der Sensoren mit der Industrial Core Platform (ICP). Um Sensoren mit der OT Security-ICP zu koppeln, verwenden Sie sowohl die ICP-Verwaltungskonsole als auch die Tenable Core-Benutzeroberfläche des Sensors.

Sie können entweder die automatische Genehmigung eingehender Kopplungsanfragen aktivieren oder die automatische Genehmigung deaktivieren und nur die manuelle Genehmigung für jede neue Kopplungsanfrage des Sensors zulassen.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Die Sensor-Hardware ist ordnungsgemäß installiert (siehe Sensor einrichten).
- Der Sensor ist mit Ihrem Netzwerk-Switch verbunden (siehe Sensor mit dem Netzwerk verbinden).
- Der Sensor hat seine eigene statische IPv4-Adresse (siehe Sensor-Setup-Assistenten aufrufen).
- Der Sensor ist mit der Tenable Core-Plattform verbunden und Sie verfügen über einen Benutzernamen und ein Passwort zum Einloggen bei der Core-Benutzeroberfläche. Weitere Informationen zur Verwendung der Benutzeroberfläche von Tenable Core finden Sie im Tenable Core + Tenable OT Security-Benutzerhandbuch.
- In der ICP-Konsole ist ein gültiges Zertifikat vorhanden (siehe Zertifikat).

Hinweis: Tenable empfiehlt, einen dedizierten ICP-Benutzer mit Administratorrolle für das Koppeln von Sensoren zuzuweisen, um Verbindungsunterbrechungen zu vermeiden (siehe Hinzufügen lokaler Benutzer). Sie können einen neuen Administratorbenutzer hinzufügen, um mehrere Sensoren zu koppeln.

Hinweis: Informationen zum Anwenden von Offline-Updates auf Ihren Tenable Core-Computer finden Sie unter Update Tenable Core Offline.

Sensor koppeln

So koppeln Sie einen Sensor der Version 3.14 oder höher mit der ICP:

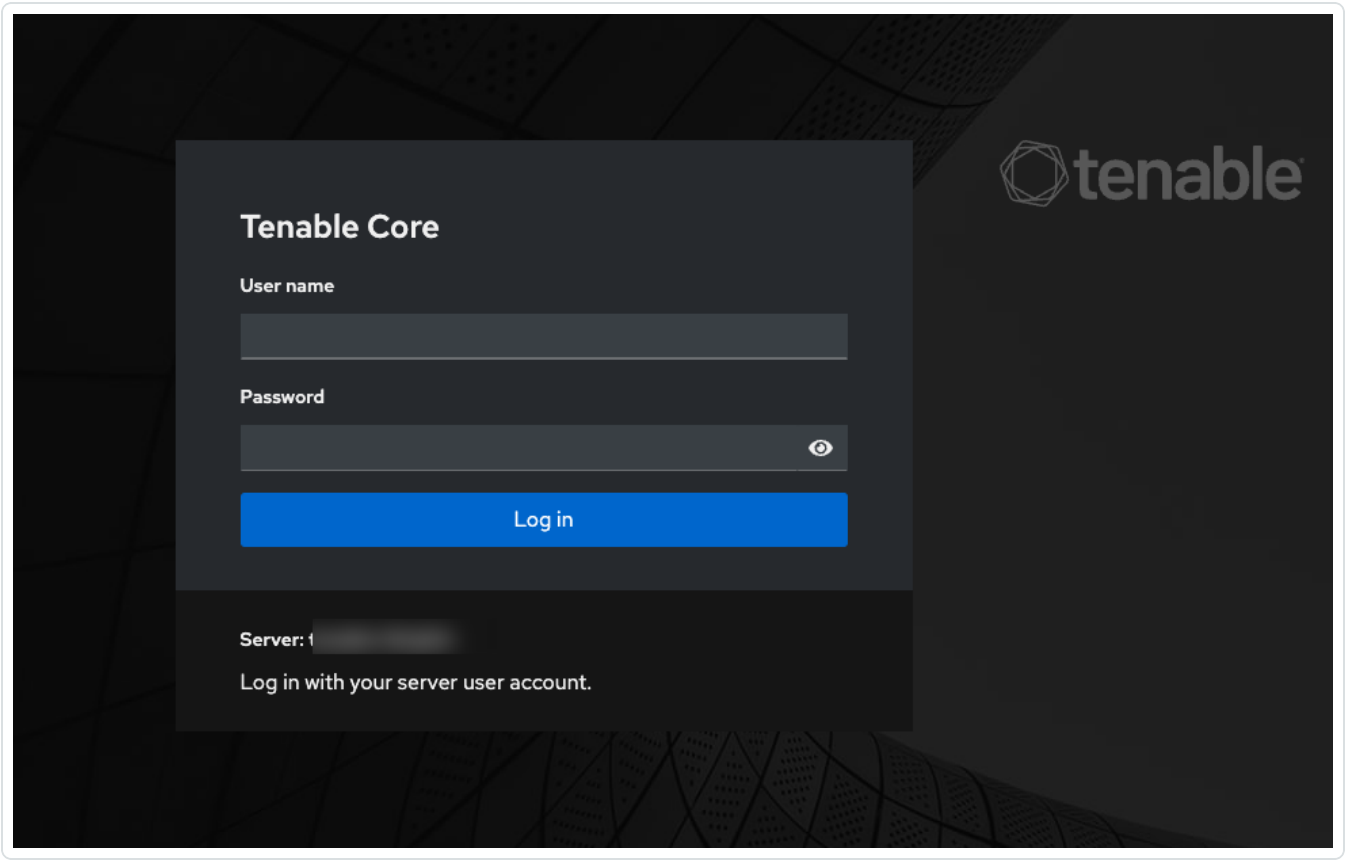
1. Navigieren Sie in der ICP-Verwaltungskonsole (Benutzeroberfläche) zum Bildschirm **Lokale Einstellungen** > **Sensoren**.

2. Um die automatische Genehmigung der Sensorkopplung zu aktivieren, stellen Sie sicher, dass der Umschalter **Sensorkopplungsanforderungen automatisch genehmigen** oben auf der Seite auf **EIN** gestellt ist. Wenn dies nicht der Fall ist, müssen alle Kopplungsanfragen manuell genehmigt werden.

3. Lassen Sie die ICP-Registerkarte geöffnet und öffnen Sie eine neue Registerkarte. Geben Sie **<Sensor-IP>:8000** ein, um auf die Tenable Core Core-Benutzeroberfläche des Sensors zuzugreifen.

   > **Hinweis**: Der Zugriff auf die Tenable Core-Benutzeroberfläche ist nur mit der neuesten Version von Chrome möglich.

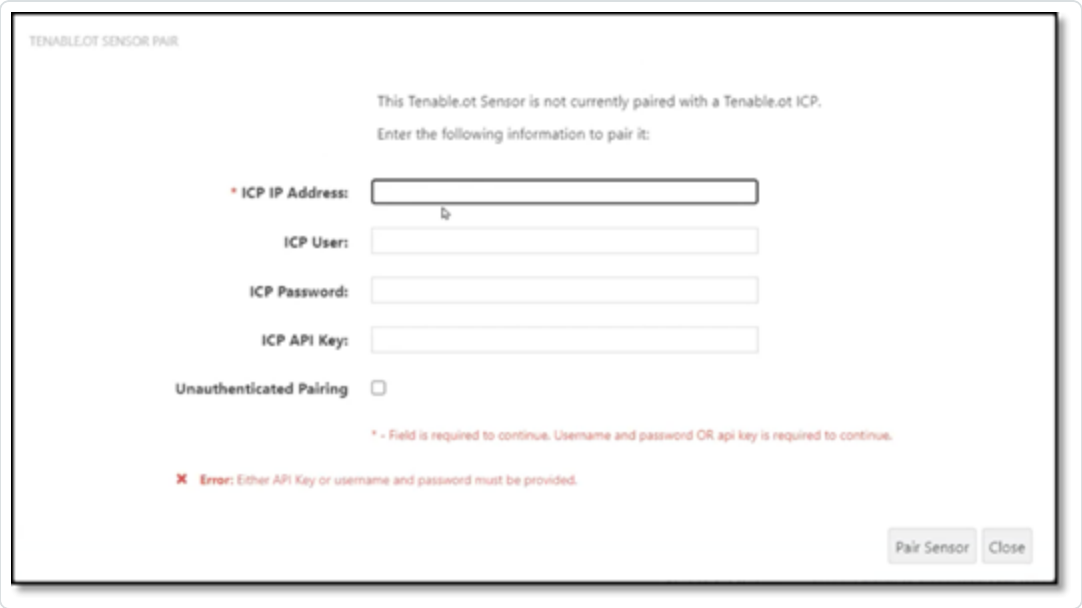
4. Geben Sie im Login-Fenster der Tenable Core-Konsole Ihren **Benutzernamen** und Ihr **Passwort** ein, aktivieren Sie das Kontrollkästchen **Reuse my password for privileged tasks** (Mein Passwort für privilegierte Aufgaben wiederverwenden) und klicken Sie auf **Log In** (Einloggen).



Wichtig: Wenn Sie die Option **Reuse my password for privileged tasks** (Mein Passwort für privilegierte Aufgaben wiederverwenden) beim Login nicht aktivieren, können Sie den Sensor-Dienst nicht neu starten.

5. Klicken Sie in der Navigationsmenüleiste auf **OT Security Sensor**.

   Das Fenster **OT Security Sensor Pair** (Sensor Pair) wird angezeigt.



Hinweis: Das Fenster **Tenable OT Security Sensor Pair** wird nur beim ersten Laden der Seite angezeigt. Wenn Sie das Fenster zu einem späteren Zeitpunkt öffnen möchten, klicken Sie auf die Schaltfläche im Abschnitt **Pairing Info** (Kopplungsinfo) der **Tenable Core**-Konsole.

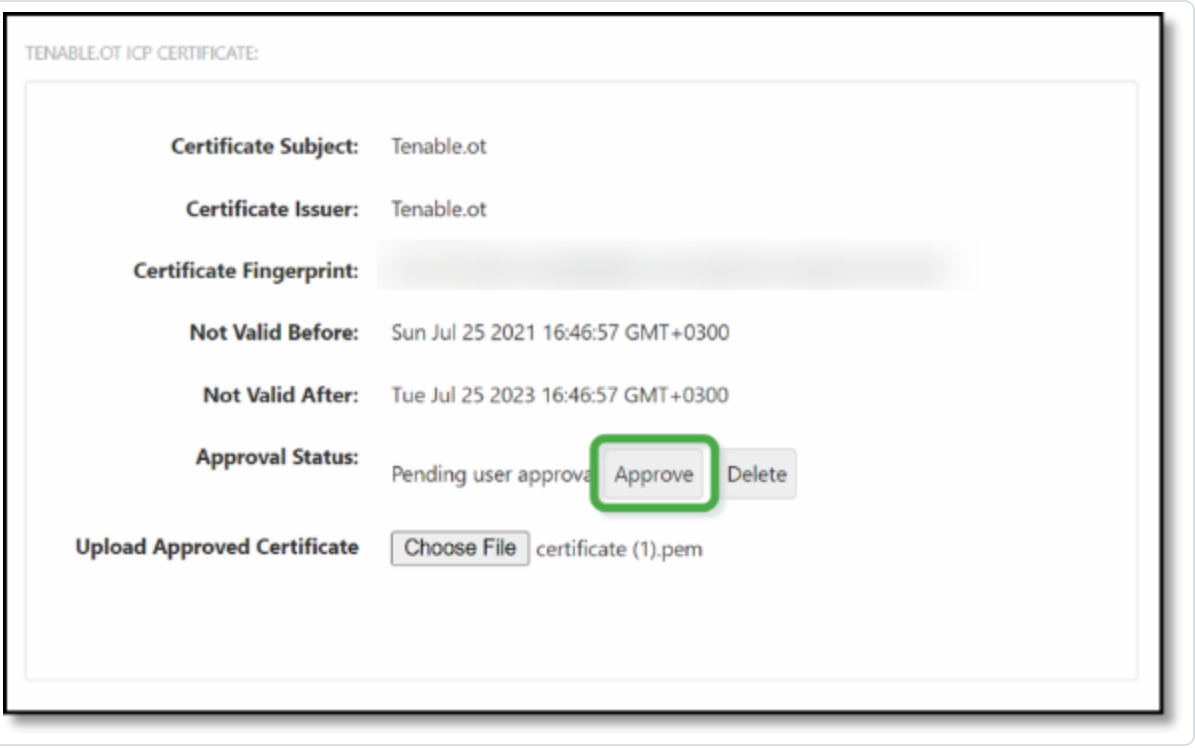
6. Geben Sie im Feld **ICP IP Address** (ICP-IP-Adresse) die IPv4-Adresse der ICP ein, die mit diesem Sensor gekoppelt werden soll.
7. Um eine nicht authentifizierte (unverschlüsselte) Kopplung zu verwenden, wählen Sie die Option **Unauthenticated Pairing** (Nicht authentifizierte Kopplung) aus und fahren Sie mit Schritt 8 fort.

   Hinweis: Sensoren, die die **nicht authentifizierte Kopplung** verwenden, können ihre Netzwerksegmente nur passiv scannen und können nicht von der 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 User** (ICP-Benutzer) und das ICP-Passwort in das Feld **ICP Password** (ICP-Passwort) ein.
   - Geben Sie im Feld **ICP-API-Schlüssel** (ICP API Key) einen API-Schlüssel für die ICP ein.

Hinweis: Tenable empfiehlt, einen dedizierten ICP-Benutzer für das Koppeln von Sensoren zu erstellen, um Konnektivität während des Kopplungsvorgangs sicherzustellen (siehe Hinzufügen lokaler Benutzer).

Hinweis: Die Authentifizierungsmethode mit Benutzername und Passwort bietet den Vorteil, dass die Zugangsdaten nicht ablaufen, im Gegensatz zu einem API-Schlüssel, der irgendwann abläuft.

9. Klicken Sie auf **Pair Sensor** (Sensor koppeln).
10. So nutzen Sie ein von der ICP angebotenes Zertifikat:
    a. Warten Sie in **Tenable Core** im Abschnitt **Tenable ICP Certificate** (Tenable ICP-Zertifikat) unter **Approval Status** (Genehmigungsstatus), bis die Zertifikatinformationen geladen wurden.



    b. Klicken Sie auf **Approve** (Genehmigen), um das Zertifikat zu genehmigen.
    c. Klicken Sie im Fenster **Confirm Accept Tenable OT Security Server Certificate** (Akzeptieren des Tenable.ot-Serverzertifikats bestätigen) auf **Accept This Certificate** (Dieses Zertifikat akzeptieren).

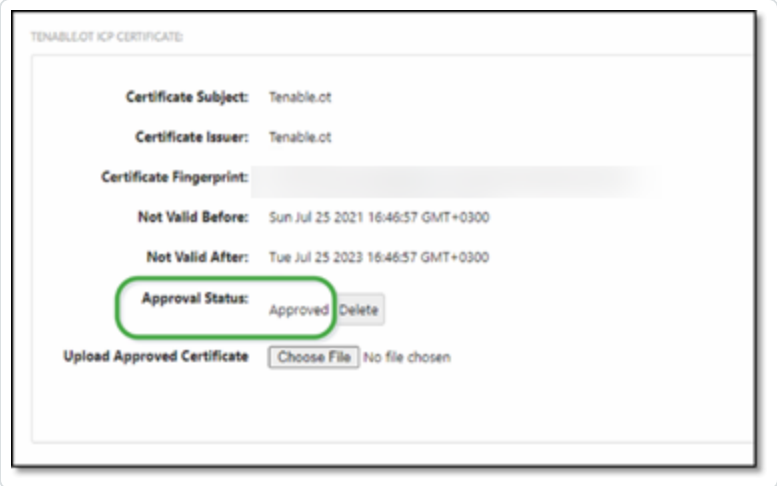
Wenn Sie es vorziehen, ein Zertifikat manuell hochzuladen:

a. Befolgen Sie in der **Tenable ICP-Konsole** das unter **Generieren eines HTTPS-Zertifikats** beschriebene Verfahren.

b. Klicken Sie in **Tenable Core** im Abschnitt **Tenable ICP Certificate** (Tenable ICP-Zertifikat) unter **Upload Approved Certificate** (Genehmigtes Zertifikat hochladen) auf **Choose File** (Datei auswählen).

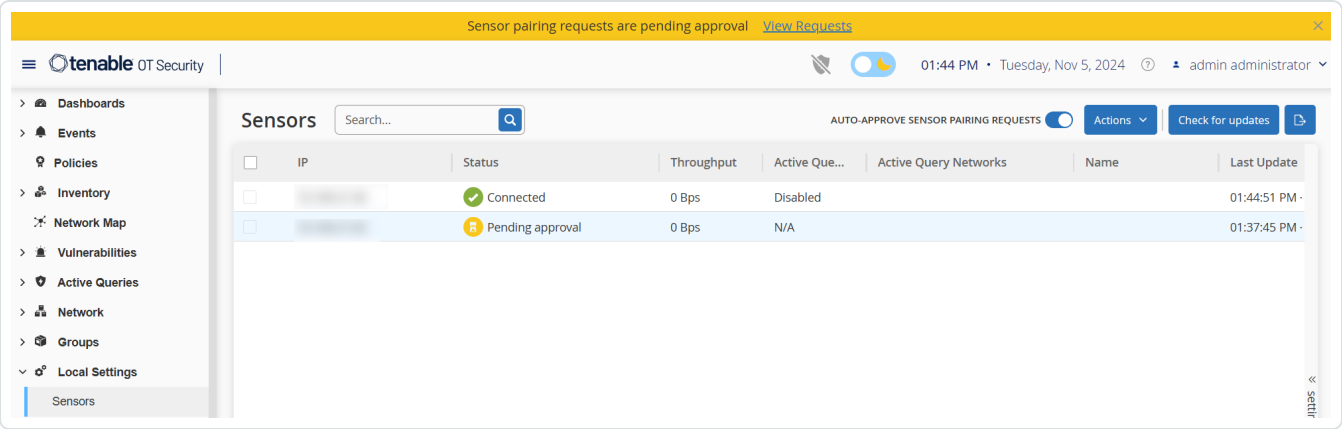
c. Navigieren Sie zur hochzuladenden `.pem`-Zertifikatdatei.

   Sobald ein gültiges Zertifikat ordnungsgemäß geladen wurde, wird sein **Approval State** (Genehmigungsstatus) in der Tabelle **OT Security-ICP Certificate** (ICP-Zertifikat) als **Approved** (Genehmigt) angezeigt.

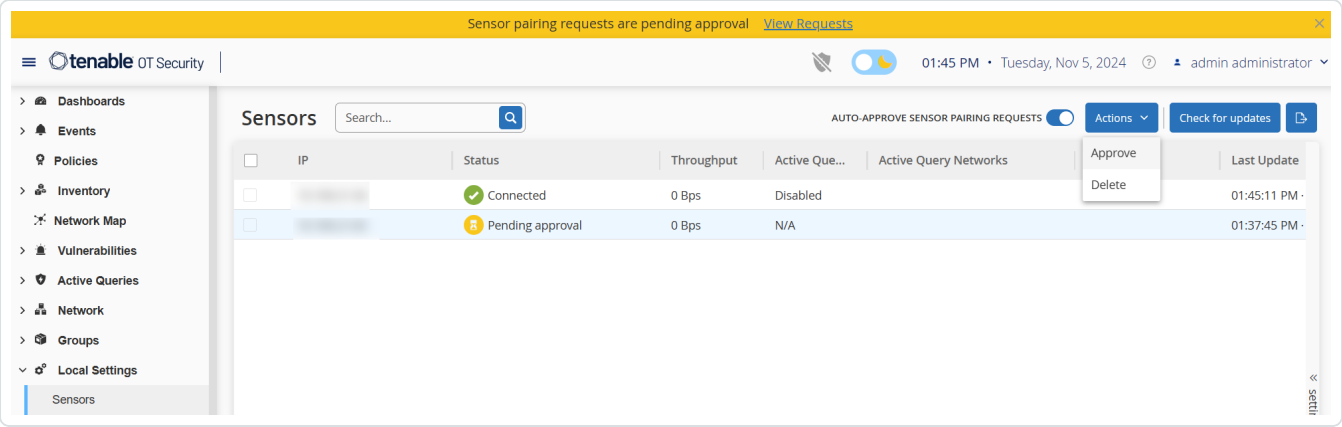


11. Navigieren Sie in der ICP-Benutzeroberfläche zu **Lokale Einstellungen** > **Sensoren**.

    OT Security zeigt den neuen Sensor in der Tabelle angezeigt und der **Status** lautet **Genehmigung ausstehend**.



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



Der **Status** ändert sich in **Verbunden**, wodurch angezeigt wird, 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. Beispiele: Tunnelfehler und API-Problem.
- **Verbunden (Tunnelfehler)** – Die Kopplung war erfolgreich, aber die Kommunikation über den Tunnel funktioniert nicht. Überprüfen Sie die Konnektivität von Port 28304 vom Sensor zum ICP. Weitere Informationen finden Sie unter Überlegungen zur Firewall.

Sobald OT Security die Kopplung für einen authentifizierten Sensor abgeschlossen hat, können Sie aktive Abfragen zur Ausführung auf diesem Sensor konfigurieren. Siehe Aktive Abfragen.

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

Sensor einrichten

Der Sensor ist in zwei Ausführungen erhältlich, als Rack-Montage-Sensor und als konfigurierbarer Sensor, wie unter OT Security 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).

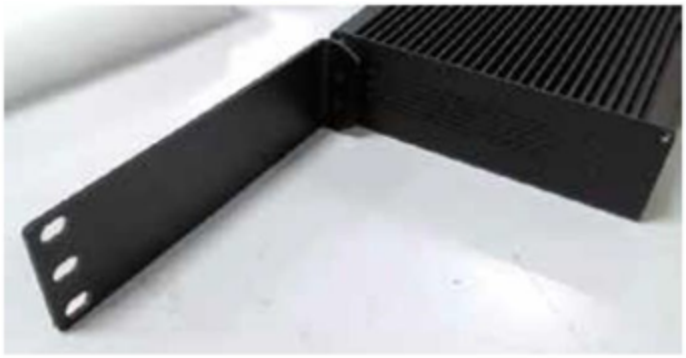
Rack-Montage-Sensor einrichten

Sie können den Sensor entweder in einem standardmäßigen 19-Zoll-Rack montieren oder auf eine ebene Oberfläche stellen (z. B. einen Schreibtisch).

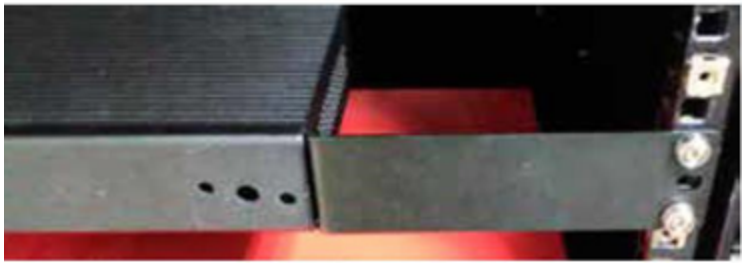
Rack-Montage (für Rack-Montage-Modell)

So montieren Sie den OT Security Sensor in einem 19-Zoll-Standard-Rack:

1. Befestigen Sie die L-förmigen Halterungen an den Schraubenlöchern auf jeder Seite des Sensors, wie in der folgenden Abbildung 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 mitgelieferten Rack-Montage-Halterungen am Rack-Rahmen befestigen. Verwenden Sie dabei geeignete Schrauben für die Rack-Montage (nicht mitgeliefert).



Wichtig:

- 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 OT Security Sensor auf einer ebenen Oberfläche:

1. Legen Sie den Sensor auf eine trockene, ebene Oberfläche (z. B. einen Schreibtisch).

Wichtig:

- Stellen Sie sicher, dass die Tischplatte eben und trocken ist.
- Stellen Sie sicher, 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).

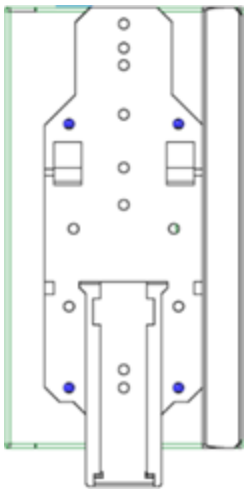
Konfigurierbaren Sensor einrichten

Sie können den konfigurierbaren Sensor entweder auf einer DIN-Schiene oder in einem standardmäßigen 19-Zoll-Rack montieren (unter Verwendung des Montagelaschen-Adapterkits).

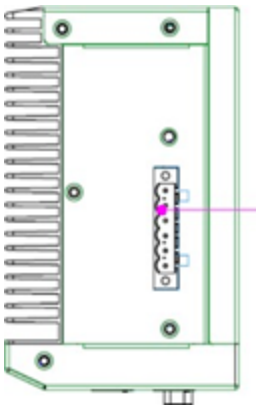
Montage auf DIN-Schiene

So montieren Sie den konfigurierbaren OT Security 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.

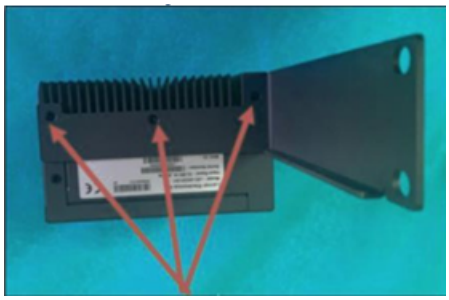
  Stecken Sie dann das eine Ende des Wechselstromkabels (mitgeliefert) in das Netzteil und das andere Ende in eine Netzsteckdose.

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):

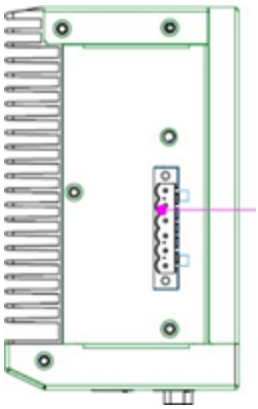
1. Bereiten Sie das Gerät für die Rack-Montage vor:
    a. Entfernen Sie drei Schrauben auf jeder Seite des Geräts.
    b. Befestigen Sie die Montagelaschen mit neuen Schrauben (mitgeliefert) auf beiden Seiten des Geräts.



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

> **Hinweis**:
>
> - 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.

Sensor mit dem Netzwerk verbinden

Der OT Security Sensor wird verwendet, um Netzwerk-Traffic zu erfassen und an die OT Security Appliance weiterzuleiten. Um eine Netzwerküberwachung durchzuführen, schließen Sie das Gerät an einen Spiegelport am Netzwerk-Switch an, der mit den relevanten Controllern/SPS verbunden ist.

Um den Sensor zu verwalten, verbinden Sie das Gerät mit einem Netzwerk. Dies kann ein anderes Netzwerk sein als das für die Netzwerküberwachung verwendete.

So verbinden Sie den OT Security Rack-Montage-Sensor mit dem Netzwerk:

1. Schließen Sie am OT Security 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 OT Security Sensor mit dem Netzwerk:

1. Schließen Sie am OT Security 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.

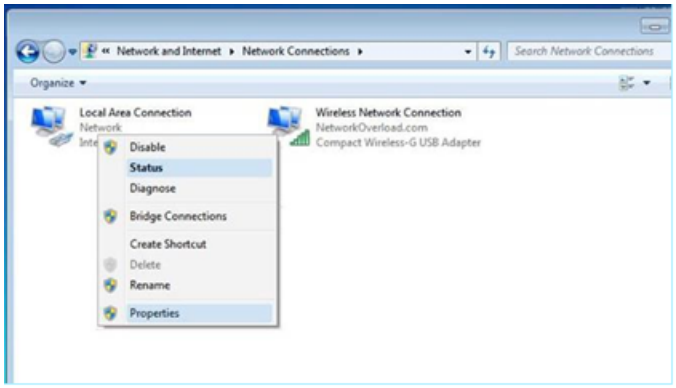
Sensor-Setup-Assistenten aufrufen

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 OT Security Sensors.
    - 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 OT Security 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 OT Security Sensor herzustellen):
    a. Gehen Sie zu **Netzwerk und Internet** > **Netzwerk- und Freigabecenter** > **Adaptereinstellungen ändern**.

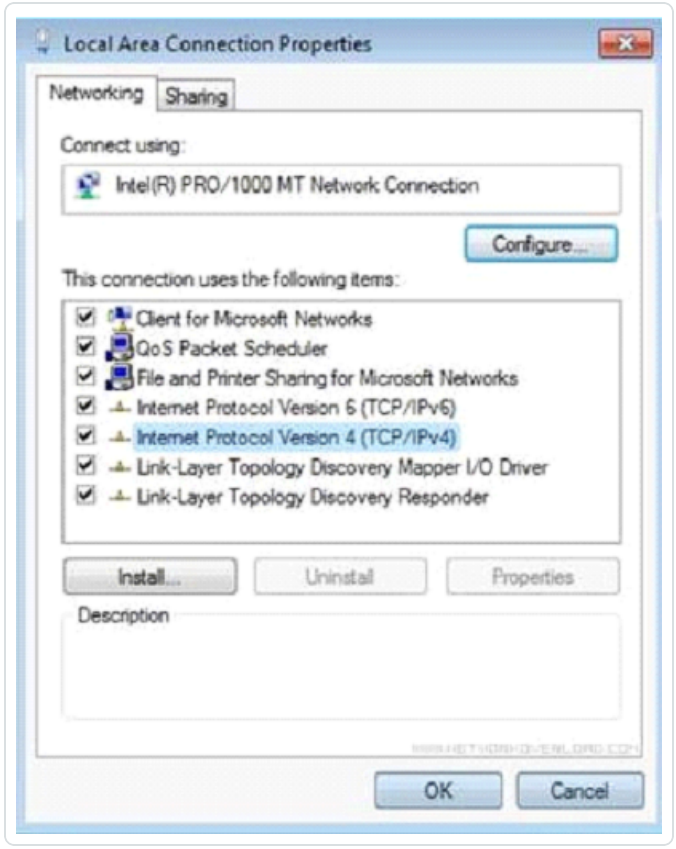
Hinweis: Die Navigation kann bei den verschiedenen Windows-Versionen leicht variieren.

Das Fenster **Netzwerkverbindungen** wird angezeigt.



b. Klicken Sie mit der rechten Maustaste auf **LAN-Verbindung** und wählen Sie **Eigenschaften** aus.

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 in das Feld **IP-Adresse** 192.168.1.10 ein.

f. Geben Sie in das Feld **Subnetzmaske** 255.255.255.0 ein.

g. Klicken Sie auf **OK**.

OT Security wendet die neuen Einstellungen an.

4. Navigieren Sie im Chrome-Browser zu https://192.168.1.5:8000.

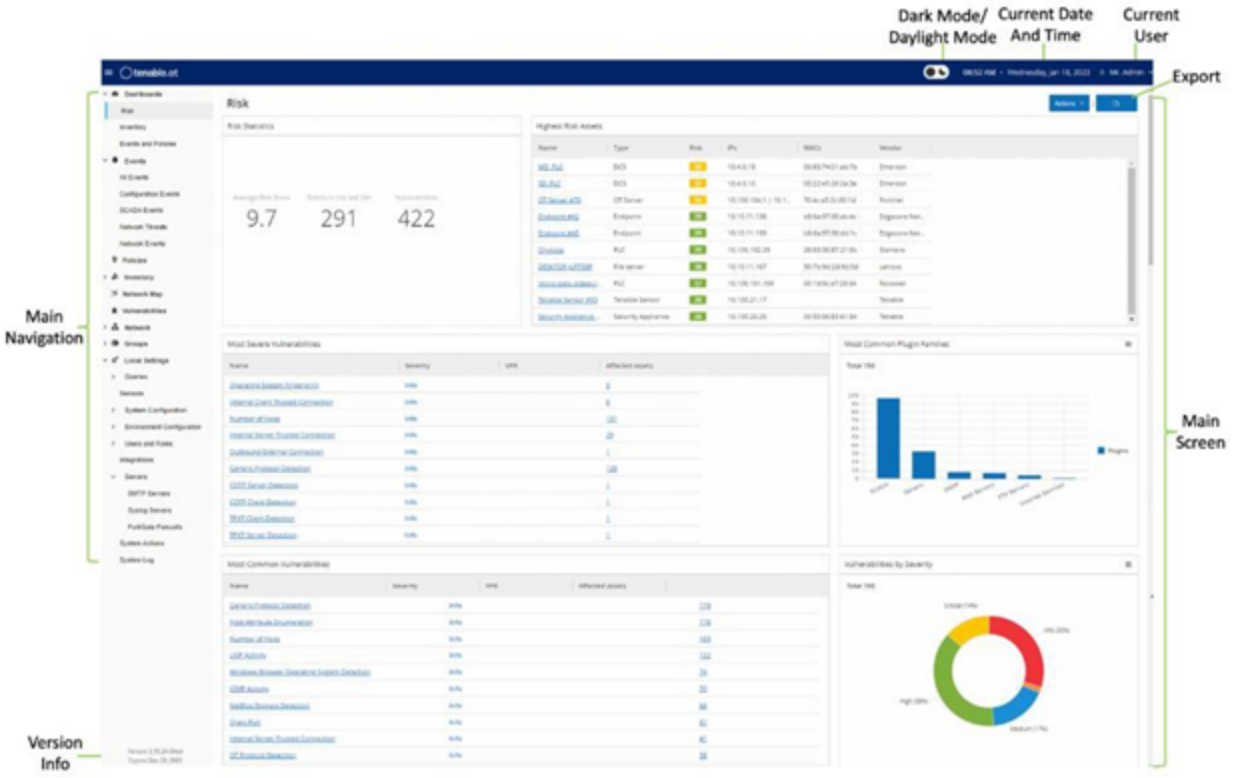
> **Hinweis**: Auf die Benutzeroberfläche kann nur über einen Chrome-Browser zugegriffen werden. Verwenden Sie die neueste Version von Chrome.

5. Koppeln Sie den Sensor.

Elemente in der Benutzeroberfläche der Verwaltungskonsole

Die Benutzeroberfläche der Verwaltungskonsole bietet einfachen Zugriff auf wichtige Daten in Bezug auf Asset-Management, Netzwerkaktivität und Sicherheitsereignisse, die von OT Security erfasst werden. Sie können die Benutzeroberfläche verwenden, um die Funktionen der OT Security-Plattform Ihren Anforderungen entsprechend zu konfigurieren.

Hauptelemente der Benutzeroberfläche



In der folgenden Tabelle werden die Hauptelemente der Benutzeroberfläche beschrieben.

Element der Benutzeroberfläche	Beschreibung
Hauptnavigation	Hauptnavigationsmenü. Klicken Sie auf das Symbol ☰, um das Hauptnavigationsmenü anzuzeigen oder auszublenden.
Aktive Abfragen	Gibt an, ob die Funktion **Aktive Abfragen** aktiviert oder deaktiviert ist.

Dunkler Modus/ Tageslichtmodus	Ändert das Farbschema der Anzeige in den dunklen Modus oder den Tageslichtmodus.
Aktuelle(s) Datum und Uhrzeit	Zeigt das aktuelle Datum und die Uhrzeit an, wie sie im System registriert sind.
Ressourcen-Center	Ressourcen-Center von OT Security
Aktueller Benutzername	Zeigt den Namen des Benutzers an, der derzeit beim System eingeloggt ist. Klicken Sie auf den Abwärtspfeil, um die Menüoptionen anzuzeigen: **Info** (zeigt Informationen zur Software an) und **Ausloggen**. Nachdem Sie OT Security aktiviert haben, können Sie Ihre Tenable-Kunden-ID in der Ansicht **Info** einsehen. Diese Kunden-ID ist erforderlich, wenn Sie sich an den technischen Support oder das Customer Success-Team wenden.
Lizenzinformationen	Zeigt die Softwareversion von OT Security und das Ablaufdatum der Lizenz an.
Hauptbildschirm	Zeigt den Bildschirm an, der Sie in der Hauptnavigation ausgewählt haben.
Exportieren	Lädt eine PDF-Datei des Dashboards herunter.

Dunklen Modus aktivieren oder deaktivieren

Sie können das Farbschema **Dunkler Modus** in allen Bildschirmen verwenden, indem Sie den Umschalter für den dunklen Modus auf „Ein“ stellen.

So aktivieren oder deaktivieren Sie den dunklen Modus:

1. Klicken Sie oben im Fenster auf den Umschalter (Dunkler Modus).

   OT Security wendet die ausgewählte Einstellung auf alle Bildschirme an.

2. Um die Einstellung für den Tageslichtmodus wiederherzustellen, klicken Sie auf den Umschalter (Tageslichtmodus).

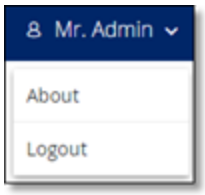
Aktuelle Softwareversion überprüfen

Sie können die Version Ihrer Software über das Benutzerprofilsymbol in der oberen rechten Ecke der Kopfleiste überprüfen.

So zeigen Sie die aktuelle Softwareversion an:

1. Klicken Sie in der Hauptkopfleiste auf das Symbol in der oberen rechten Ecke.

   OT Security zeigt das Benutzermenü an.



2. Klicken Sie auf **Info**.

   OT Security zeigt die aktuelle Softwareversion an.

In OT Security navigieren

Sie können über die linke Navigationsleiste auf die folgenden Hauptseiten zugreifen:

- **Dashboards** – Zeigt Widgets mit Diagrammen und Tabellen, die einen allgemeinen Überblick über das Inventar und die Sicherheitslage Ihres Netzwerks geben. Es gibt separate Dashboards für Risiko, Inventar, Ereignisse und Richtlinien. Siehe Dashboards.
- **Ereignisse** – Zeigt alle Ereignisse an, die als Folge von Richtlinienverletzungen aufgetreten sind. Die Seite **Alle Ereignisse** enthält separate Bildschirme für jeden spezifischen

Ereignistyp. Beispiel: Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse. Siehe Ereignisse.

- **Richtlinien** – Hier können Sie Richtlinien im System anzeigen, bearbeiten und aktivieren. Siehe Richtlinien.
- **Inventar** – Zeigt ein Inventar aller erfassten Assets an und ermöglicht so ein umfassendes Asset-Management, die Statusüberwachung der einzelnen Assets sowie die Anzeige der damit verbundenen Ereignisse. Die Seite **Alle Assets** enthält separate Ansichten für jeden spezifischen Asset-Typ (Controller und Module, Netzwerk-Assets und IoT). Siehe Inventar.
- **Netzwerkübersicht** – Zeigt eine visuelle Darstellung der Netzwerk-Assets und ihrer Verbindungen. Siehe Netzwerkübersicht.
- **Schwachstellen** – Zeigt alle von OT Security erkannten Netzwerkbedrohungen an, z. B. CVEs, anfällige Protokolle, anfällige offene Ports und mehr, und nennt empfohlene Behebungsmaßnahmen. Siehe Schwachstellen.
- **Netzwerk** – Bietet einen umfassenden Überblick über den Netzwerk-Traffic, indem Daten zu Konversationen angezeigt werden, die im Laufe der Zeit zwischen Assets im Netzwerk stattgefunden haben. Siehe Netzwerk.

  OT Security zeigt die Netzwerkinformationen in drei separaten Fenstern an:

  - **Netzwerk – Zusammenfassung** – Zeigt eine Übersicht über den Netzwerk-Traffic.
  - **Paketerfassungen** – Zeigt vollständige Paketerfassungen des Netzwerk-Traffic an.
  - **Konversationen** – Zeigt eine Liste aller im Netzwerk erkannten Konversationen mit Details zum Zeitpunkt des Auftretens und den beteiligten Assets an.
- **Gruppen** – Hier können Sie Gruppen anzeigen, erstellen und bearbeiten, die bei der Richtlinienkonfiguration verwendet werden. Siehe Gruppen.
- **Lokale Einstellungen** – Hier können Sie die Systemeinstellungen anzeigen und konfigurieren. Siehe Einstellungen.

Tabellen anpassen

Auf OT Security-Seiten werden Daten in einem Tabellenformat mit einer Liste für jedes Element angezeigt. Diese Tabellen verfügen über standardisierte Anpassungsfunktionen, die Ihnen einen einfachen Zugriff auf die relevanten Informationen ermöglichen.

Hinweis: Die hier gezeigten Beispiele beziehen sich auf die Seiten **Alle Ereignisse** und **Alle Assets**, aber ähnliche Funktionen sind für die meisten Seiten verfügbar. Sie können jederzeit zu den standardmäßigen Anzeigeeinstellungen zurückkehren, indem Sie auf **Einstellungen** > **Tabelle auf Standard zurücksetzen** klicken.

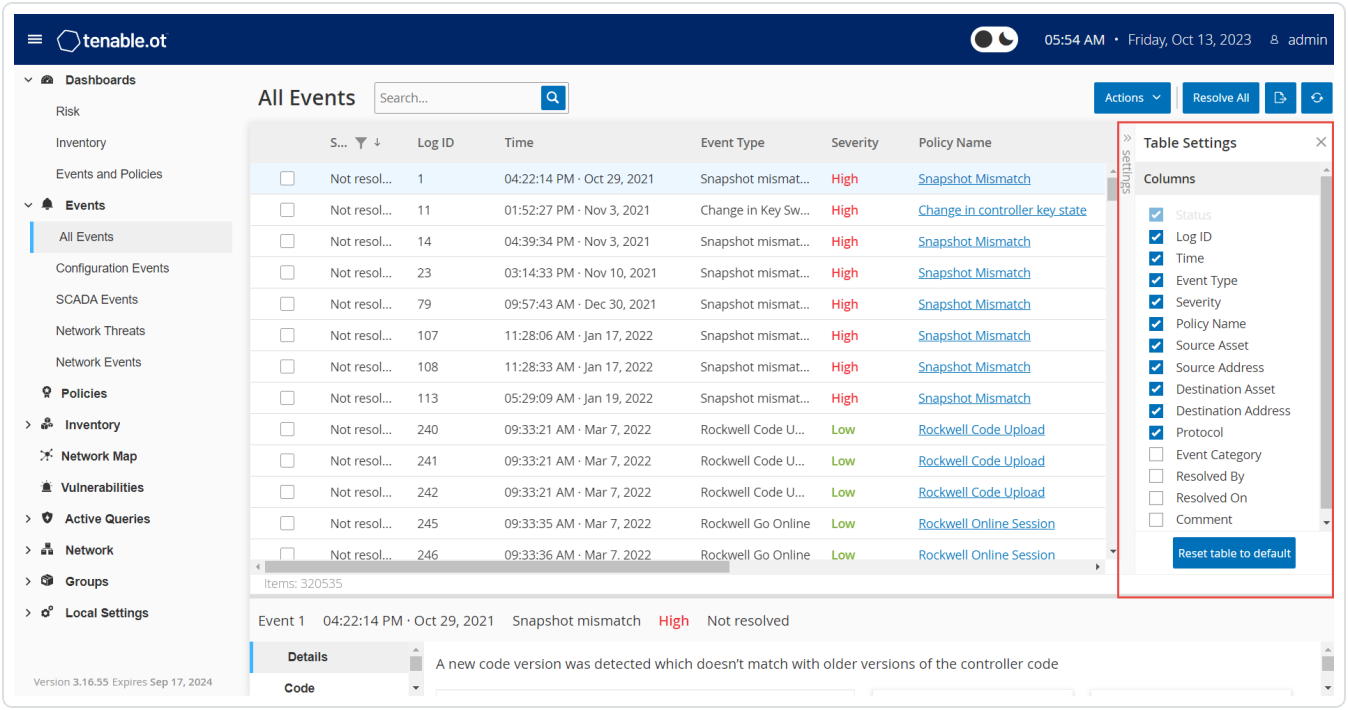
Spaltenanzeige anpassen

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

So geben Sie an, welche Spalten angezeigt werden:

1. Klicken Sie rechts neben der Tabelle auf **Einstellungen**.

   Der Bereich **Tabelleneinstellungen** wird mit dem Abschnitt **Spalten** angezeigt.



2. Aktivieren Sie im Abschnitt **Spalten** das Kontrollkästchen neben den Spalten, die angezeigt werden sollen.
3. Deaktivieren Sie das Kontrollkästchen neben den Spalten, die Sie ausblenden möchten.

   OT Security zeigt nur die ausgewählten Spalten an.
4. Klicken Sie auf das **x** (oder auf die Registerkarte **Einstellungen**), um das Fenster **Tabelleneinstellungen** zu schließen.

So passen Sie die Anzeigereihenfolge der Spalten an:

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

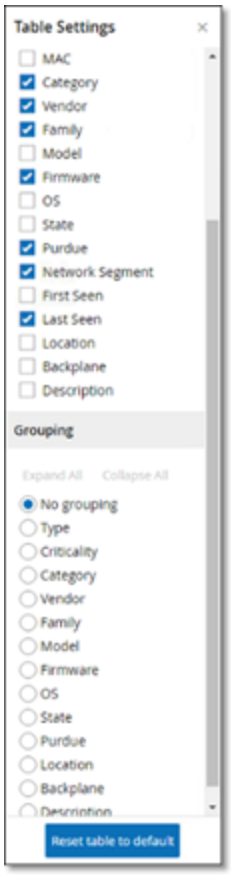
Listen nach Kategorien gruppieren

Für die **Inventar**-Seiten können Sie die Listen nach verschiedenen Parametern gruppieren, die für diesen bestimmten Bildschirm relevant sind.

So gruppieren Sie die Listen:

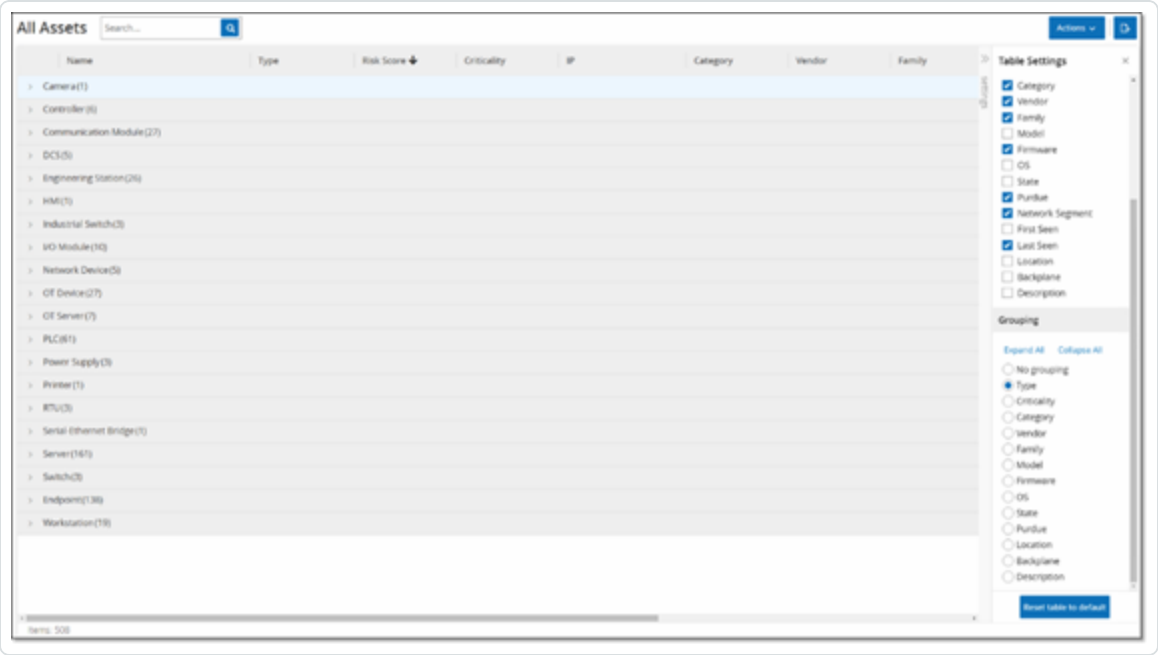
1. Klicken Sie am rechten Rand der Tabelle auf die Registerkarte **Einstellungen**.

   Der Bereich **Tabelleneinstellungen** wird auf der rechten Seite mit den Abschnitten **Spalten** und **Gruppierung** angezeigt.
2. Scrollen Sie nach unten zum Abschnitt **Gruppierung**.

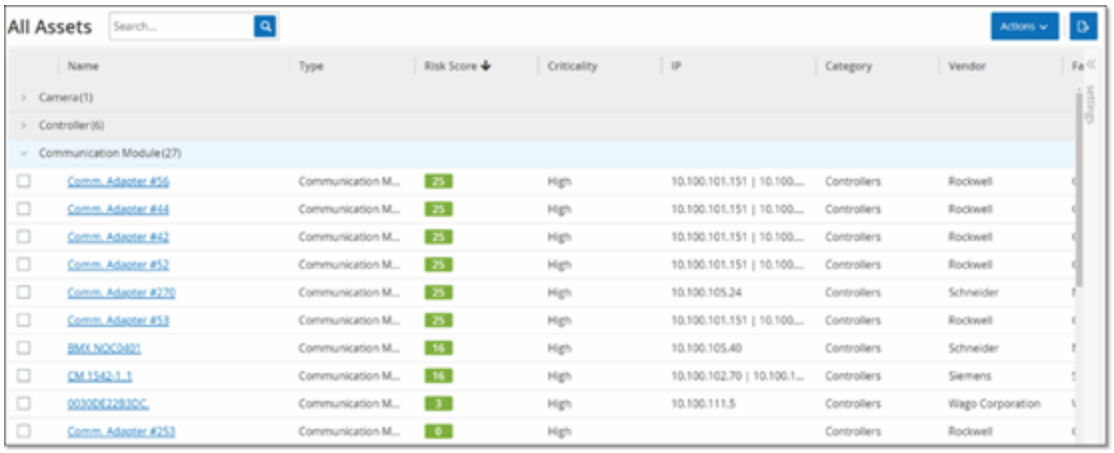


3. Wählen Sie den Parameter aus, nach dem die Listen gruppiert werden sollen. Beispiel: **Typ**.

   OT Security zeigt die gruppierten Kategorien an.



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.



Spalten sortieren

> **Hinweis**: Dieses Verfahren gilt für alle Versionen.

So sortieren Sie die Listen:

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

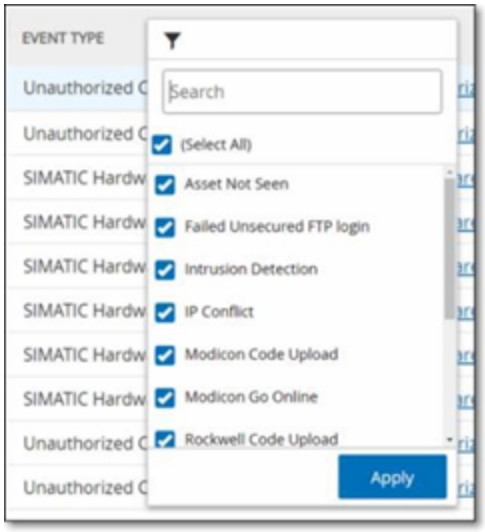
Spalten filtern

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 anzuzeigenden Elemente aus und deaktivieren Sie die Kontrollkästchen der Elemente, die ausgeblendet werden sollen.

> **Hinweis**: Sie können zunächst das Kontrollkästchen **Alle auswählen** deaktivieren und dann die Kontrollkästchen der Elemente aktivieren, die Sie anzeigen möchten.

4. Sie können die Liste nach Filtern durchsuchen und diese aktivieren oder deaktivieren.
5. Klicken Sie auf **Anwenden**.

   OT Security filtert die Listen wie angegeben.

> Die Filterschaltfläche neben der Spaltenüberschrift zeigt an, dass die Ergebnisse nach diesem Parameter gefiltert werden.

So entfernen Sie die Filter:

1. Klicken Sie auf die Filterschaltfläche .
2. Klicken Sie auf das Kontrollkästchen **Alle auswählen**, um Ihre Auswahl aufzuheben.
3. Klicken Sie erneut auf das Kontrollkästchen **Alle auswählen**, um alle Elemente auszuwählen.
4. Klicken Sie auf **Anwenden**.

Suche

Sie können auf jeder Seite nach bestimmten Datensätzen suchen.

So durchsuchen Sie die Listen:

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

Daten exportieren

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

> **Hinweis**: 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 der Seite, für die Sie Daten exportieren möchten.
2. Klicken Sie in der Kopfleiste auf **Exportieren**.

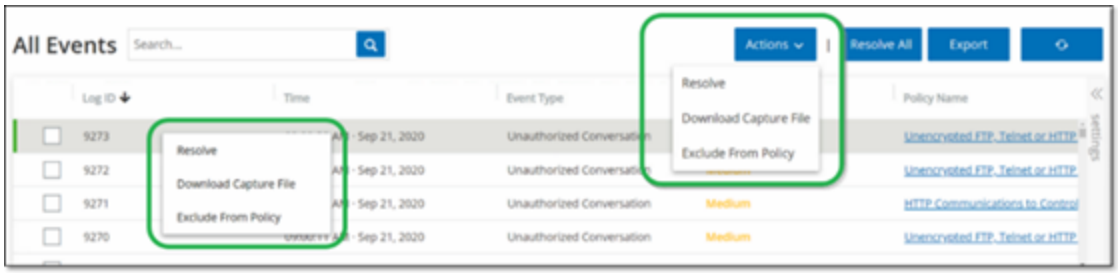
   OT Security lädt ein CSV-Format der Daten herunter.

Menü „Aktionen“

Jeder Bildschirm verfügt über eine Reihe von Aktionen, die Sie für die auf diesem Bildschirm aufgeführten Elemente ausführen können. Beispielsweise enthält der Bildschirm **Richtlinien** Optionen zum **Anzeigen**, **Bearbeiten**, **Duplizieren** oder **Löschen** einer Richtlinie. Im Bildschirm **Ereignisse** können Sie für ein Ereignis die Aktionen **Auflösen** und **Erfassungsdatei herunterladen** usw. ausführen.

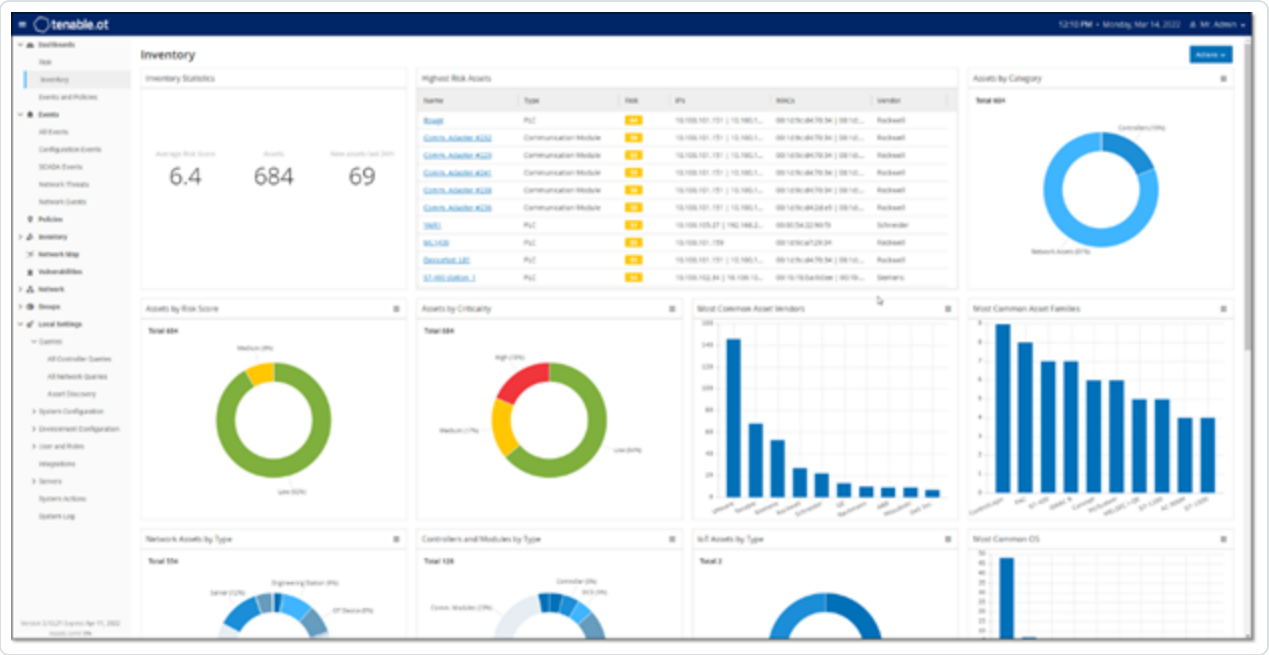
Führen Sie einen der folgenden Schritte aus, um auf das Menü **Aktionen** zuzugreifen:

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



Dashboards

OT Security bietet die drei Dashboards **Risiko**, **Inventar** sowie **Ereignisse und Richtlinien**, um einen Überblick über das Inventar und die Sicherheitslage Ihres Netzwerks zu geben.



So wählen Sie ein Dashboard aus:

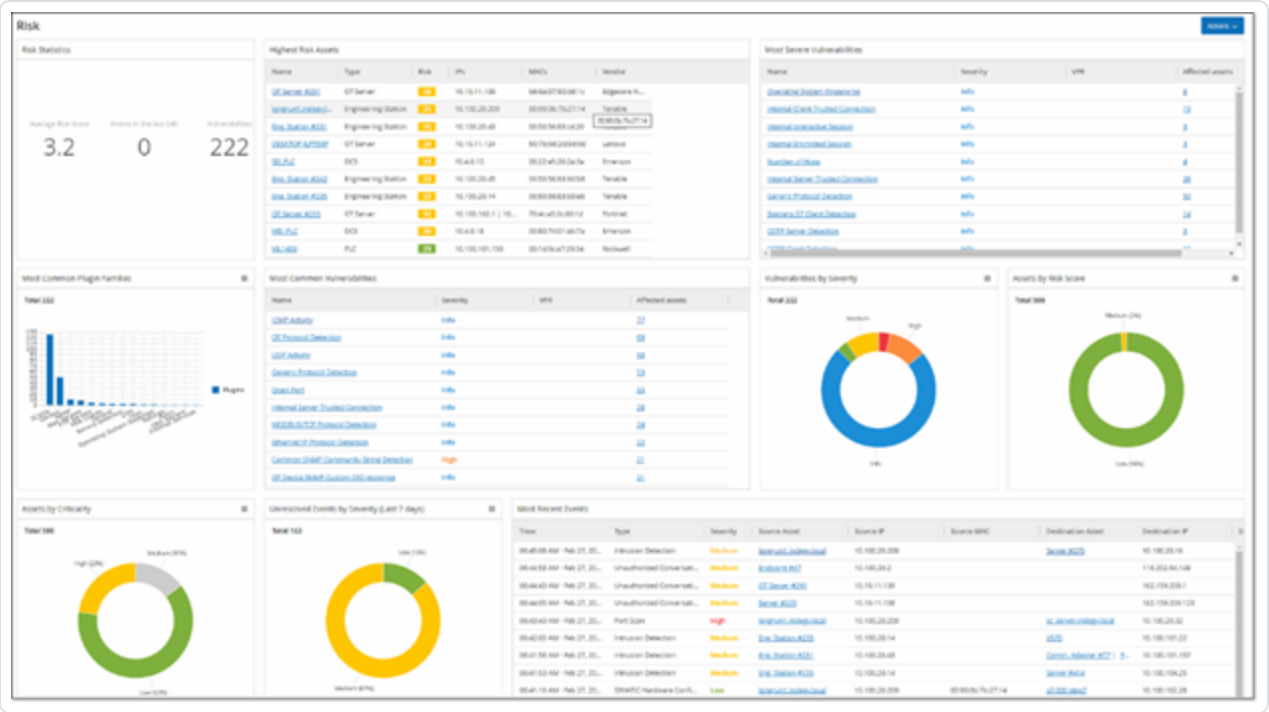
- Klicken Sie im Hauptnavigationsmenü auf **Dashboards**.

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.

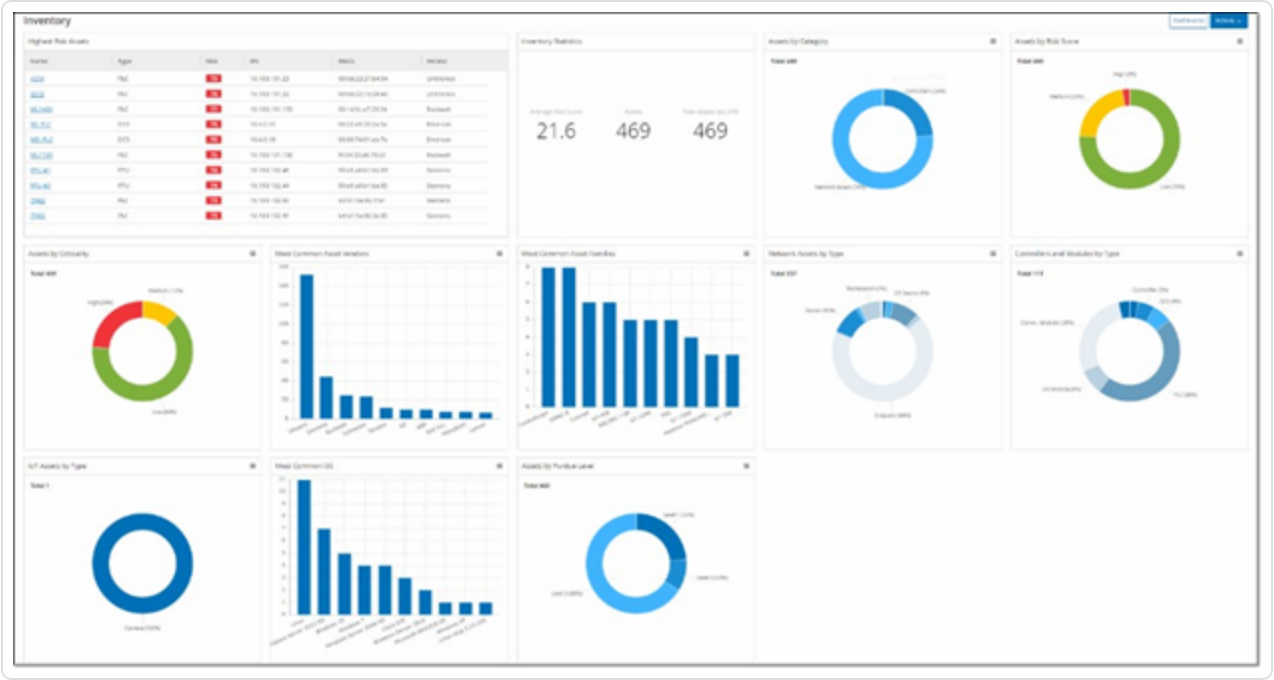


Das Dashboard **Risiko** zeigt Widgets wie„ Risikostatistik“, „Assets nach Risikowert“, „Assets nach Kritikalität“, „Ereignisse nach Schweregrad“, „Häufigste Schwachstellen“ usw.

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.

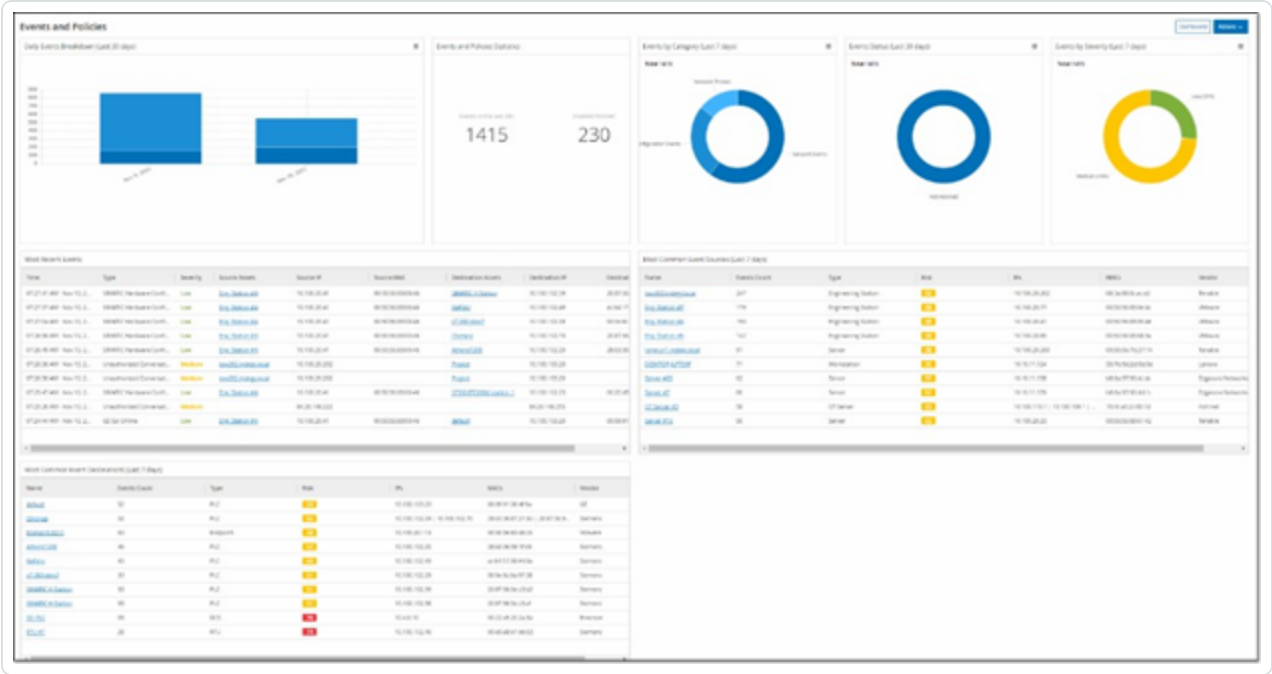


Das Dashboard **Inventar** zeigt Widgets wie „Assets mit höchstem Risiko“, „Inventar-Statistik“, „Assets nach Risikowert“, „Controller und Module nach Typ“, „Assets nach Purdue-Level“ usw.

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 Asset- oder Ereignis-Link gelangen Sie zum entsprechenden Element im Bildschirm **Inventar** bzw. **Ereignisse**.

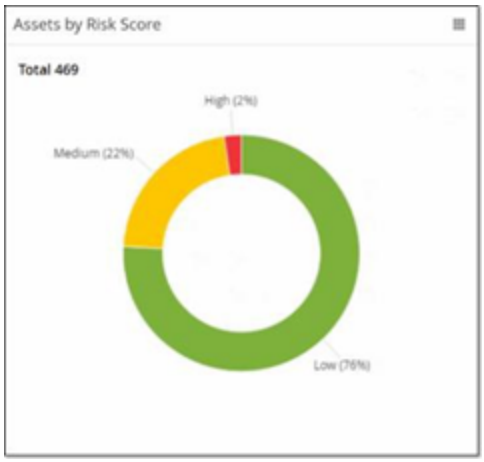
Interagieren mit Dashboards

Sie können die Dashboard-Anzeige anpassen, indem Sie mit Widgets interagieren. Es gibt zwei Modi zum Anzeigen von Daten in den Dashboards: Diagrammmodus und Tabellenmodus. Einige Widgets haben einen festen Anzeigemodus, während Sie bei anderen zwischen den Modi umschalten können. Widgets mit dem 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.

> **Hinweis**: Filter können nur im Tabellenmodus angewendet werden.

Diagrammmodus

Der Diagrammmodus zeigt eine grafische Visualisierung der Widget-Daten.

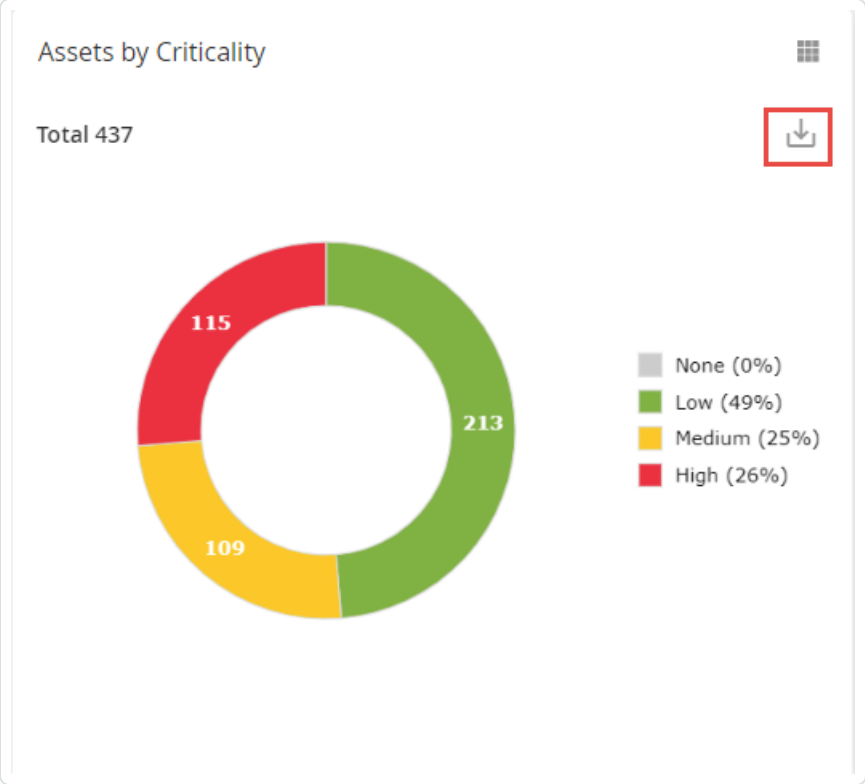


Sie können auf folgende Weise mit den Widgets interagieren:

- Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um ein Fenster mit Daten anzuzeigen, die für dieses Segment des Diagramms spezifisch sind.

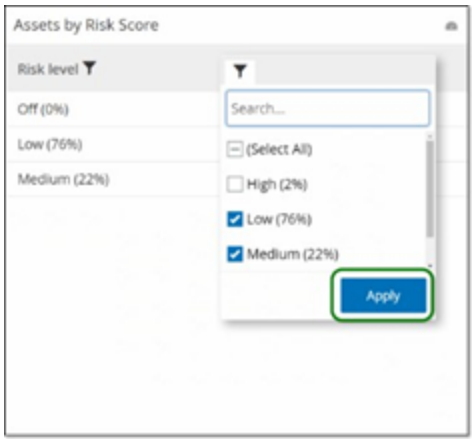
- Wenn Sie ein Widget im Diagrammmodus anzeigen, können Sie ein Bild des Diagramms herunterladen, indem Sie den Mauszeiger über das Widget bewegen und auf die Schaltfläche

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, die Sie im Tabellenmodus anwenden, werden nicht 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 verwenden möchten.

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

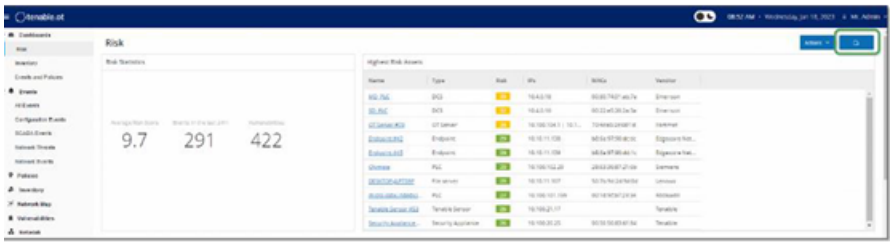
   OT Security aktualisiert das Standard-Dashboard und zeigt es bei Ihrem nächsten Zugriff auf die Verwaltungskonsole an

Dashboard exportieren

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 **Exportieren**.



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

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

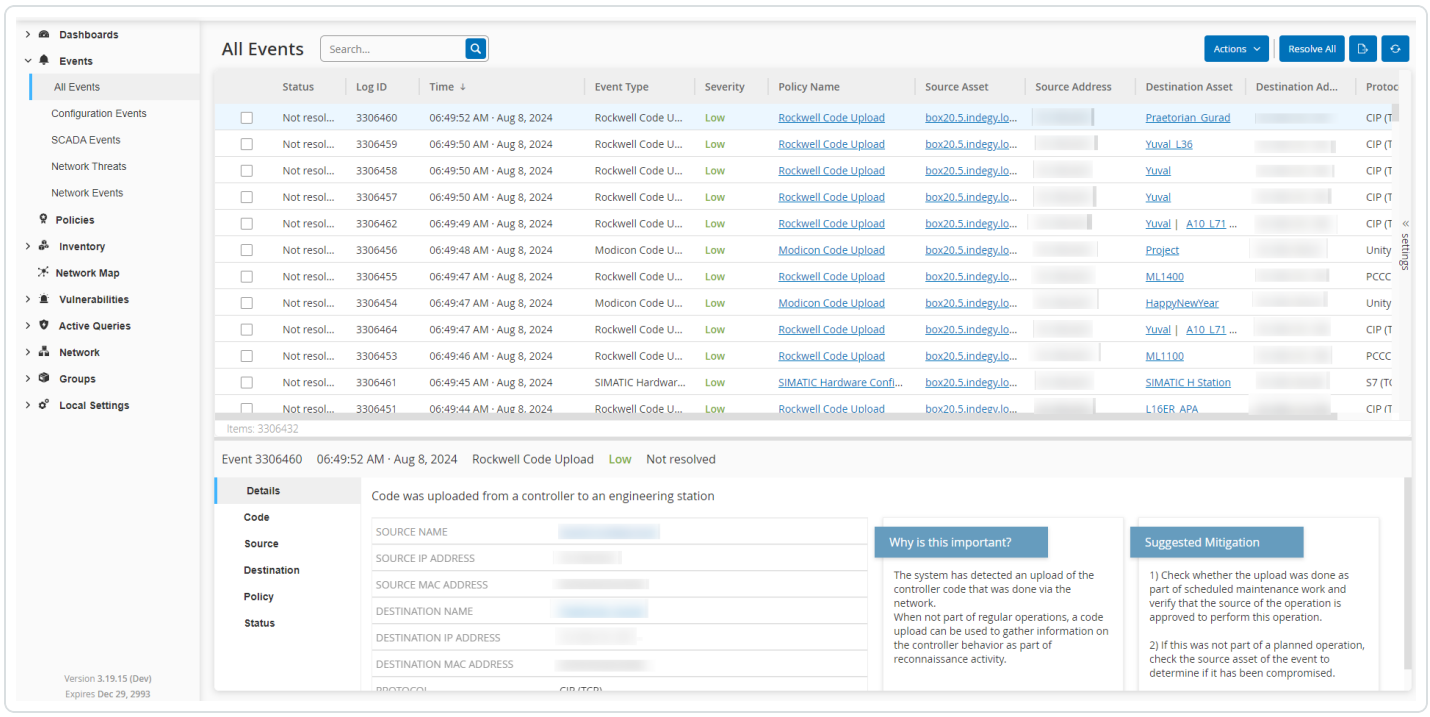
2. Navigieren Sie nach Abschluss des Downloads zu der heruntergeladenen Datei, um sie anzuzeigen oder freizugeben.

Ereignisse

Ereignisse sind vom System generierte Benachrichtigungen, um auf potenziell schädliche Aktivitäten im Netzwerk aufmerksam zu machen. Richtlinien, die Sie im OT Security-System einrichten, generieren Ereignisse in einer der folgenden Kategorien: Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse. OT Security weist jeder Richtlinie einen Schweregrad zu, der den Schweregrad des Ereignisses angibt.

Sobald Sie eine Richtlinie aktivieren, 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 auf der Seite **Alle Ereignisse** angezeigt. Spezifische Untergruppen der Ereignisse werden in separaten Fenstern für jede dieser Ereigniskategorien angezeigt: **Konfigurationsereignisse**, **SCADA-Ereignisse**, **Netzwerkbedrohungen** und **Netzwerkereignisse**.

Für jede Ereignisseite (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen und Netzwerkereignisse) können Sie die Anzeigeeinstellungen anpassen, indem Sie auswählen, welche Spalten angezeigt und wo sie jeweils positioniert werden sollen. Sie können die Ereignisse nach Ereignistyp, Schweregrad, Richtlinienname usw. gruppieren. Außerdem können Sie die Ereignislisten sortieren, filtern und durchsuchen. Weitere Informationen zu den Anpassungsfunktionen finden Sie unter Tabellen anpassen.

Verwenden Sie die Schaltfläche **Aktionen** in der Kopfleiste, um die folgenden Aktionen durchzuführen:

- Auflösen – Dieses Ereignis als „Aufgelöst“ markieren
- PCAP herunterladen – Die PCAP-Datei für dieses Ereignis herunterladen.
- Ausschließen – Einen Richtlinienausschluss für dieses Ereignis erstellen.

Im unteren Abschnitt der Seite werden auf verschiedenen Registerkarten 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.

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

Sie können die mit den einzelnen Ereignissen verknüpfte Paketerfassungsdatei herunterladen, siehe Netzwerk. 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 Inventar).
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 vom Benutzer in den Asset-Details von OT Security eingegeben. Siehe Inventar.
Zuletzt gesehen	Der Zeitpunkt, zu dem das Gerät zuletzt von OT Security 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.
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 Typen 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 und Unterkategorien): • 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 auf der Seite **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.).

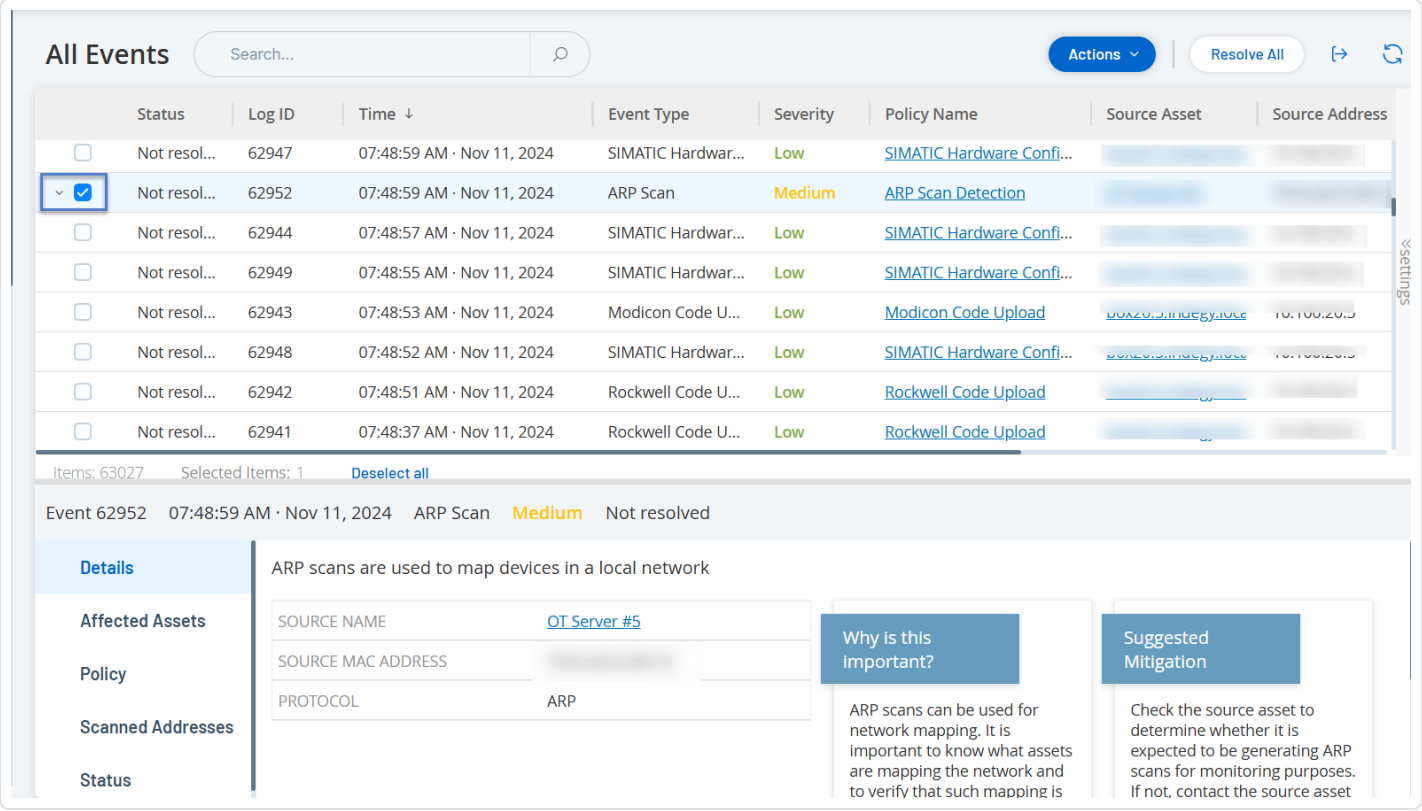
- **Kopfleiste** – Zeigt einen Überblick über wichtige Informationen über das Ereignis.
- **Details** – Gibt eine kurze Beschreibung des Ereignisses sowie eine Erklärung, warum diese Informationen wichtig sind, und schlägt Schritte vor, die unternommen werden sollten, um den durch das Ereignis verursachten 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.



Ereignisse auflösen

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 und sie in einem Batch-Prozess als **Aufgelöst** markieren. Sie können auch alle Ereignisse (oder alle Ereignisse einer bestimmten Kategorie) gleichzeitig als **Aufgelöst** markieren.

Einzelne Ereignisse auflösen

So markieren Sie bestimmte Ereignisse als aufgelöst:

1. Aktivieren Sie auf der entsprechenden Seite 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 **Aktionen**.

   Ein Dropdown-Menü wird geöffnet.

   > **Hinweis**: 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 **Auflösen** aus.

   Das Fenster **Ereignis auflösen** wird angezeigt.

4. (Optional) Im Feld **Kommentar** können Sie einen Kommentar hinzufügen, der die zur Behebung des Problems bzw. der Probleme ausgeführten Risikominderungsschritte beschreibt.
5. Klicken Sie auf **Auflösen**.

   Der Status der ausgewählten Ereignisse wird in **Aufgelöst** geändert.

Alle Ereignisse auflösen

Die Aktion **Alle auflösen** gilt für alle Ereignisse auf der aktuellen Seite, basierend auf den Filtern, die aktuell auf die Anzeige angewendet werden. Wenn beispielsweise die Seite **Konfigurationsereignisse** geöffnet ist, werden mit **Alle auflösen** Konfigurationsereignisse aufgelöst, jedoch keine SCADA-Ereignisse usw. Bei geclusterten Ereignissen werden alle Ereignisse im Cluster als aufgelöst markiert.

So markieren Sie alle Ereignisse als aufgelöst:

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

auflösen.

Das Fenster **Alle Ereignisse auflösen** wird mit der Anzahl der aufzulösenden Ereignisse angezeigt.

2. (Optional) Im Feld **Kommentar** können Sie einen Kommentar zu der Gruppe von Ereignissen hinzufügen, die aufgelöst werden sollen.
3. Klicken Sie auf **Auflösen**.

   OT Security zeigt eine Warnmeldung an.
4. Klicken Sie auf **Auflösen**.

   OT Security markiert alle Ereignisse in der aktuellen Anzeige werden als **Aufgelöst**.

Richtlinienausschlüsse erstellen

Wenn 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). 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.

Sie können Ausschlüsse auf der Seite **Ereignisse** erstellen, basierend auf Ereignissen, die von Ihren Richtlinien generiert wurden. Sie können angeben, welche Bedingungen eines bestimmten Ereignisses Sie aus der Richtlinie ausschließen möchten.

Um die Generierung von Ereignissen für die angegebenen Bedingungen zu einem späteren Zeitpunkt fortzusetzen, können Sie den Ausschluss löschen, wie unter Richtlinien beschrieben.

So erstellen Sie einen Richtlinienausschluss:

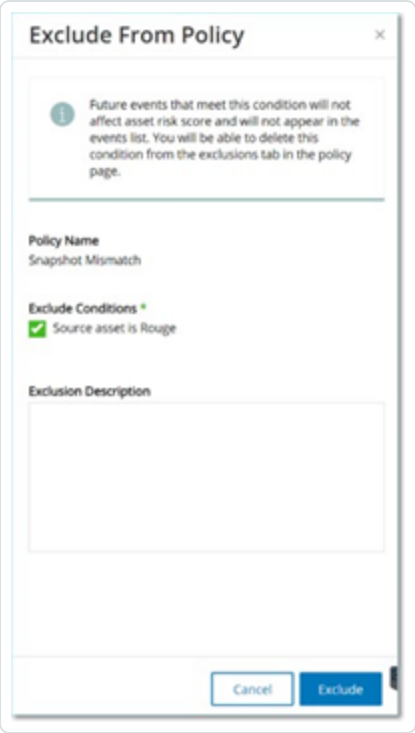
1. Wählen Sie auf der entsprechenden Seite für **Ereignisse** (Konfigurationsereignisse, SCADA-Ereignisse, Netzwerkbedrohungen oder Netzwerkereignisse) das Ereignis aus, für das Sie einen Ausschluss erstellen möchten.
2. Klicken Sie in der Kopfleiste auf **Aktionen** oder klicken Sie mit der rechten Maustaste auf das Ereignis.

   Das Menü **Aktionen** wird geöffnet.
3. Klicken Sie auf **Aus Richtlinie ausschließen**.

   Das Fenster **Aus Richtlinie ausschließen** wird geöffnet.
4. Im Abschnitt **Ausschlussbedingungen** sind standardmäßig alle Bedingungen ausgewählt.

   Dies führt dazu, dass Ereignisse mit einer der angegebenen Bedingungen aus der Richtlinie ausgeschlossen werden. Sie können das Kontrollkästchen neben jeder Bedingung, für die weiterhin Ereignisse generiert werden sollen, deaktivieren.

   > **Hinweis**: Wenn Sie beispielsweise im folgenden Fenster 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“.



Hinweis: Welche Bedingungen ausgeschlossen werden können, hängt vom Richtlinientyp ab, siehe folgende Tabelle.

5. (Optional) Im Feld **Ausschlussbeschreibung** können Sie einen Kommentar zum Ausschluss hinzufügen.
6. Klicken Sie auf **Ausschließen**.

   OT Security erstellt den Ausschluss.

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

Richtlinienkategorie	Ereignistyp	Ausschließbare Bedingungen
Controller-Aktivitäten	Konfigurationsereignisse (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 • 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

Einzelne Erfassungsdateien herunterladen

OT Security 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. Sie können auch PCAP-Dateien für das gesamte Netzwerk herunterladen, siehe Netzwerk.

Hinweis: 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.

PCAP-Datei herunterladen

So laden Sie eine PCAP-Datei herunter:

1. Aktivieren Sie auf der Seite **Ereignisse** das Kontrollkästchen neben dem Ereignis, für das Sie die PCAP-Datei herunterladen möchten.
2. Klicken Sie in der Kopfleiste auf **Aktionen**.

   Das Menü **Aktionen** wird geöffnet.
3. Wählen Sie **Erfassungsdatei herunterladen** aus.

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

FortiGate-Richtlinien erstellen

Die FortiGate-Integration ermöglicht es Ihnen, bestimmte OT Security-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 ist so eingestellt, dass sie automatisch für die Quell- und Ziel-Assets gilt, die am OT Security-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.

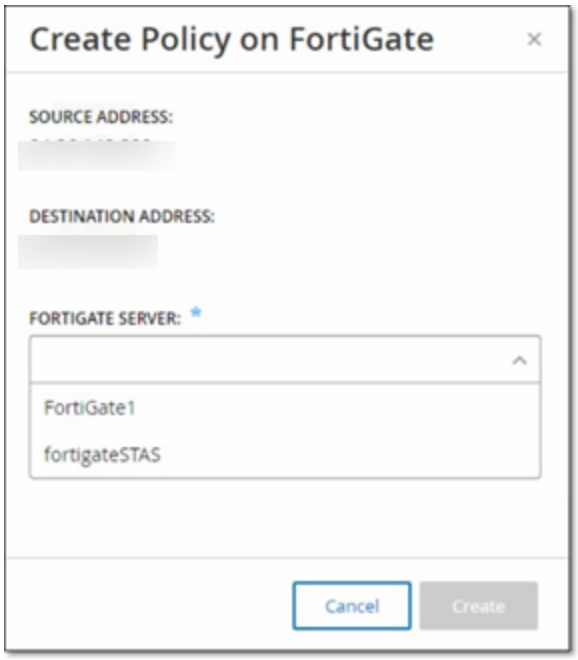
Bevor Sie FortiGate-Richtlinien vorschlagen, müssen Sie die Integration für den FortiGate-Firewall-Server mit OT Security einrichten. Siehe FortiGate-Firewalls.

So schlagen Sie eine FortiGate-Richtlinie vor:

1. Wählen Sie auf der entsprechenden Seite 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 **Aktionen** oder klicken Sie mit der rechten Maustaste auf das Ereignis.

   Ein Dropdown-Menü wird geöffnet.
3. Wählen Sie **FortiGate-Richtlinie erstellen** aus.

   Das Fenster **Richtlinie auf FortiGate erstellen** wird geöffnet. Die Felder **Quelladresse** und **Zieladresse** der am OT Security-Ereignis beteiligten Assets sind bereits ausgefüllt.
4. Wählen Sie im Dropdown-Menü **FortiGate-Server** den erforderlichen Server aus.



5. Klicken Sie auf **Erstellen**.

   Die Richtlinie wird in FortiGate erstellt und das Fenster wird geschlossen. Sie können die neue Richtlinie in der FortiGate-Anwendung anzeigen. Ein FortiGate-Administrator kann die Einstellungen wie erforderlich anpassen.

Richtlinien

OT Security enthält Richtlinien, die bestimmte Arten von Ereignissen 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, generiert das System ein Ereignis. Das System protokolliert das Ereignis und sendet Benachrichtigungen gemäß den für die Richtlinien konfigurierten Richtlinienaktionen.

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

OT Security verfügt über eine Reihe vordefinierter (sofort einsetzbarer) Richtlinien. Darüber hinaus können Sie die vordefinierten Richtlinien bearbeiten oder neue benutzerdefinierte Richtlinien definieren.

Hinweis: Standardmäßig sind die meisten Richtlinien aktiviert. Informationen zum Aktivieren/Deaktivieren von Richtlinien finden Sie unter Richtlinien aktivieren oder deaktivieren.

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 OT Security ist die Verwendung von Gruppen. Bei der Konfiguration einer Richtlinie gehört jeder Richtlinienparameter zu einer Gruppe, nicht zu einzelnen Entitäten. Dadurch wird der Prozess für die Richtlinienkonfiguration optimiert. Wenn beispielsweise die Aktivität „Firmware-Update“ als verdächtige Aktivität gilt, wenn sie zu bestimmten Tageszeiten (z. B. während der Arbeitszeit) auf einem Controller 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.

Für die Richtlinienkonfiguration werden die folgenden Arten von Gruppen 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 mit ähnlichen Kommunikationsmustern definieren.

- **E-Mail-Gruppen** – Gruppieren Sie mehrere E-Mail-Konten, die E-Mail-Benachrichtigungen für bestimmte Ereignisse erhalten. Sie können z. B. nach Rolle, Abteilung usw. gruppieren.
- **Port-Gruppen** – Gruppieren Sie Ports, die auf ähnliche Weise verwendet werden. Zum Beispiel Ports, die auf Rockwell-Controllern offen sind.
- **Protokollgruppen** – Gruppieren Sie Kommunikationsprotokolle nach Protokolltyp (z. B. Modbus), Hersteller (z. B. von Rockwell zugelassene Protokolle) usw.
- **Planungsgruppen** – Gruppieren Sie mehrere Zeitbereiche als Planungsgruppe mit einem bestimmten gemeinsamen Merkmal. Zum Beispiel Arbeitszeiten, Wochenende usw.
- **Tag-Gruppen** – Gruppieren Sie Tags, die ähnliche Betriebsdaten in verschiedenen Controllern enthalten. Zum Beispiel Tags, die die Ofentemperatur steuern.
- **Regelgruppen** – Gruppieren Sie verwandte 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 sind. Das System wird mit einer Reihe vordefinierter Gruppen geliefert. Sie können diese Gruppen bearbeiten und eigene Gruppen hinzufügen, siehe Gruppen.

> **Hinweis**: Richtlinienparameter können nur mithilfe von Gruppen festgelegt werden. Selbst wenn eine Richtlinie für eine einzelne Entität gelten soll, 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. In der folgenden Tabelle werden die verschiedenen Schweregrade 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. Im Abschnitt **Ereignisse** wird **Alle Ereignisse** angezeigt. Auf der Seite **Richtlinie** wird das Ereignis unter der Richtlinie aufgeführt, die das Ereignis ausgelöst hat. Auf der Seite **Inventar** wird das Ereignis unter dem betroffenen Asset aufgeführt. Darüber hinaus können Sie Richtlinien so konfigurieren, dass Benachrichtigungen über Ereignisse mithilfe des Syslog-Protokolls an ein externes SIEM-System und/oder an bestimmte E-Mail-Empfänger gesendet werden.

- **Syslog-Benachrichtigung** – Syslog-Nachrichten verwenden das CEF-Protokoll sowohl mit Standardschlüsseln als auch mit benutzerdefinierten Schlüsseln (für die Verwendung mit OT Security konfiguriert). Eine Erläuterung zur Interpretation von Syslog-Benachrichtigungen finden Sie im OT Security Syslog Integration Guide.
- **E-Mail-Benachrichtigungen** – E-Mail-Nachrichten enthalten Details über das Ereignis, das die Benachrichtigung generiert hat, sowie Schritte zur Eindämmung der Bedrohung.

Richtlinienkategorien und Unterkategorien

In OT Security werden die Richtlinien nach folgenden Kategorien geordnet:

- **Konfigurationsereignisse** – Diese Richtlinien beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Es gibt zwei Unterkategorien:
    - **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. Sperrlisten und Zulassungslisten für Assets, Aktivitäten und Zeitpläne werden unterstützt.

- **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 werden. Dazu gehören auch Traffic-Muster, die für das Netzwerk ungewöhnlich sind oder 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), löst die Richtlinie ein Ereignis aus. Sie können diese Richtlinien auf bestimmte Zeitpläne und/oder bestimmte Assets beschränken. Anbieterspezifische Protokolle werden der Einfachheit halber nach Anbieter organisiert, es kann jedoch jedes Protokoll in einer Richtliniendefinition verwendet werden.

- **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 sind.

Richtlinientypen

Innerhalb jeder Kategorie und Unterkategorie gibt es eine Reihe verschiedener Typen von Richtlinien. OT Security enthält die vordefinierten Richtlinien der einzelnen Typen. Sie können auch Ihre eigenen benutzerdefinierten Richtlinien der einzelnen Typen erstellen. In den folgenden Tabellen werden die verschiedenen Richtlinientypen nach Kategorie gruppiert erläutert.

Konfigurationsereignis – Typen von Controller-Aktivitätsereignissen

Controller-Aktivitäten beziehen sich auf die Aktivitäten, die im Netzwerk stattfinden. Zum Beispiel die „Befehle“, die zwischen Assets im Netzwerk implementiert werden. Es gibt viele verschiedene Typen von Controller-Aktivitätsereignissen. Der Typ des Controllers, auf dem die Aktivität stattfindet, sowie die spezifische Aktivität definieren den Typ der Controller-Aktivität. Beispiele: Rockwell-SPS-Stopp, SIMATIC-Code-Download, Modicon-Online-Sitzung usw.

Die Parameter für die Richtliniendefinition bzw. 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.

> **Hinweis**: 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	Eine Änderung am Controller-Status durch Anpassen der Position des physischen Schlüssels. Unterstützt derzeit nur Rockwell-Controller.
Statusänderung	Betroffenes Asset, Zeitplan	Der Controller wechselte von einem Betriebsstatus in einen anderen. Zum Beispiel „Wird ausgeführt“, „Gestoppt“, „Test“ usw.
Änderung der Firmware-Version	Betroffenes Asset, Zeitplan	Eine Änderung an der auf dem Controller ausgeführten Firmware.
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.

Hinweis: 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 seit, 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.
Änderung der USB-Konfiguration	Betroffene Assets, Zeitplan	Erkennt, wenn ein USB-Gerät mit einer Windows-basierte Workstation verbunden oder von dieser getrennt 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 OT Security während des angegebenen Zeitraums erkennt.
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. Informationen zum Festlegen der anfänglichen Netzwerk-Baseline oder zum Aktualisieren der Netzwerk-Baseline finden Sie unter Festlegen einer Netzwerk-Baseline. 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 wird.
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.
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 während des angegebenen Zeitraums eine Verbindung zu einem Asset in der Ziel-Asset-Gruppe 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	OT Security betrachtet FTP als unsicheres Protokoll. Diese Richtlinie erkennt erfolgreiche Logins über FTP.
Fehlgeschlagenes ungesichertes FTP-Login	Quelle, Ziel, Zeitplan	OT Security betrachtet FTP als unsicheres Protokoll. Diese Richtlinie erkennt fehlgeschlagene Login-Versuche über FTP.
Erfolgreiches ungesichertes Telnet-Login	Quelle, Ziel, Zeitplan	OT Security betrachtet Telnet als unsicheres Protokoll. Diese Richtlinie erkennt erfolgreiche Logins über Telnet.
Fehlgeschlagenes ungesichertes Telnet-Login	Quelle, Ziel, Zeitplan	OT Security betrachtet Telnet als unsicheres Protokoll. Diese Richtlinie erkennt fehlgeschlagene Login-Versuche über Telnet.
Ungesicherter Telnet-Login-	Quelle, Ziel, Zeitplan	OT Security betrachtet Telnet als unsicheres Protokoll. Diese Richtlinie

Versuch		erkennt Login-Versuche über Telnet (für die der Ergebnisstatus nicht erkannt wurde).

Netzwerkbedrohungs-Ereignistypen

Die folgende Tabelle beschreibt die verschiedenen Typen von Netzwerkbedrohungsereignissen.

> **Hinweis**: 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 sind. 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. **Hinweis**: Für IDS-Ereignisse (Intrusion Detection System, Angriffserkennungssystem) können die Asset-Gruppen **Quelle** und **Ziel** nicht bearbeitet werden.
ARP-Scan	Betroffenes Asset, Zeitplan	Erkennt ARP-Scans

		(Netzwerkaufklärungsaktivität), die im Netzwerk ausgeführt werden. Die Richtlinie gilt für Scans, die während des angegebenen Zeitraums in der Gruppe „Betroffene Assets“ 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.

Hinweis: 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.

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. Sie können die Richtlinie so konfigurieren, 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 übergeordnete oder untergeordnete IEC-104-Einheiten gesendet werden und als riskant gelten.
DNP3-Befehle	Quell-Asset, Ziel-Asset, Zeitplan	Erkennt alle Hauptbefehle, die über das DNP3-Protokoll gesendet werden. Zum Beispiel Select, Operate, Warm/Cold Restart usw. Erkennt auch Fehler, die auf interne Indikatoren wie nicht unterstützte Funktionscodes und

		Parameterfehler zurückzuführen sind.

Richtlinien aktivieren oder deaktivieren

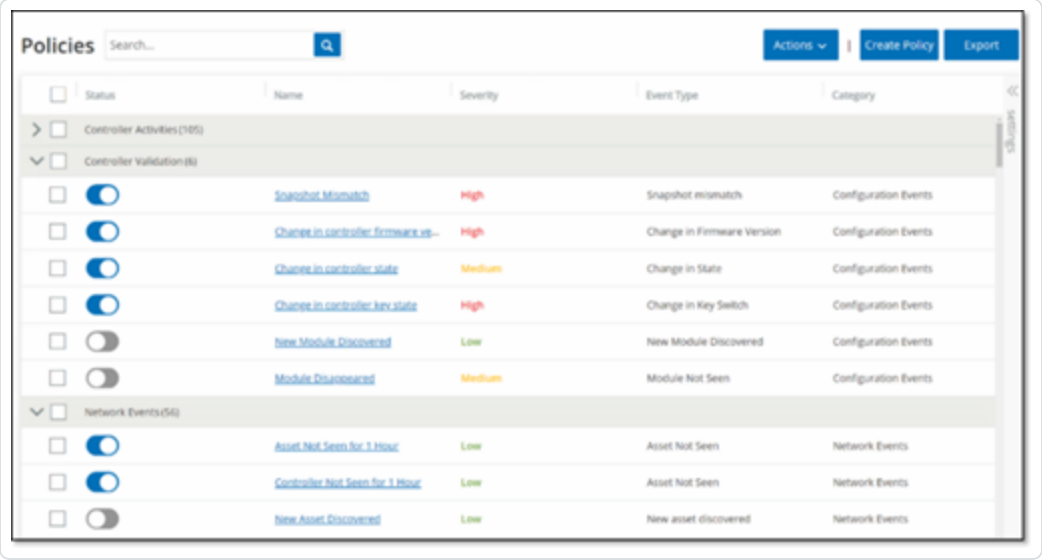
Sie können jede konfigurierte Richtlinie in Ihrem System (sowohl vorkonfiguriert als auch benutzerdefiniert) aktivieren oder deaktivieren. Sie können einzelne Richtlinien aktivieren/deaktivieren oder mehrere Richtlinien auswählen, um sie gesammelt zu aktivieren/deaktivieren.

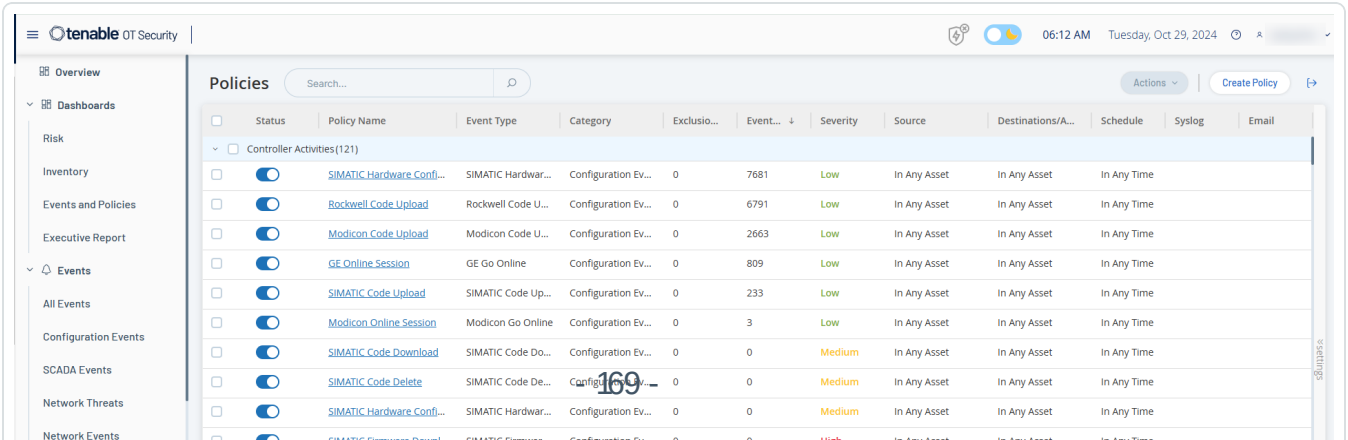
Hinweis: Viele Richtlinien sind bei der Erfassung von Daten auf Abfragen angewiesen. Wenn einige oder alle Abfragefunktionen deaktiviert sind, können die entsprechenden Richtlinien nicht angewendet werden. Sie können Abfragen über **Aktive Abfragen** aktivieren, siehe Aktive Abfragen.

So aktivieren oder deaktivieren Sie eine Richtlinie:

1. Gehen Sie zu **Richtlinien**.

   Auf der Seite werden alle im System konfigurierten Richtlinien aufgelistet, gruppiert nach Richtlinienkategorie.



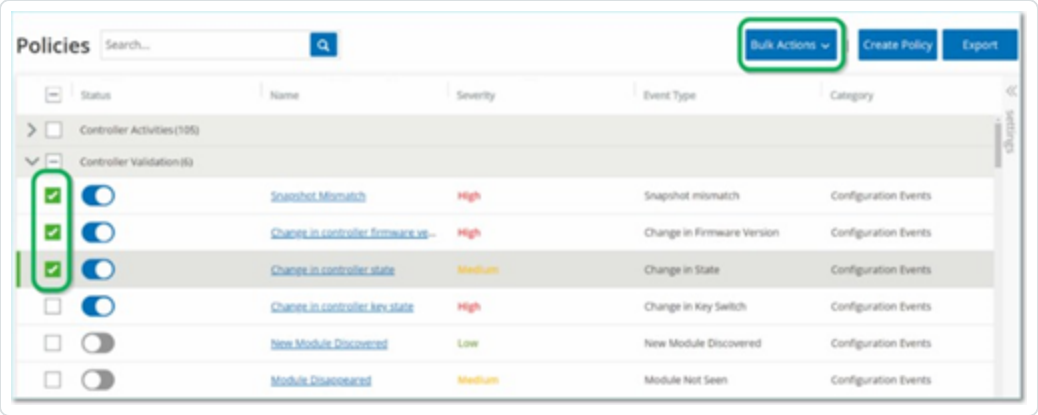


2. Um die Richtlinie zu aktivieren oder zu deaktivieren, klicken Sie auf den Umschalter **Status** neben der entsprechenden Richtlinie.

So aktivieren oder deaktivieren Sie Richtlinien:

1. Gehen Sie zu **Richtlinien**.

   Auf der Seite werden alle im System konfigurierten Richtlinien aufgelistet, gruppiert nach Richtlinienkategorie.



2. Aktivieren Sie das Kontrollkästchen neben jeder Richtlinie, die Sie aktivieren zw. 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. Wählen Sie im Dropdown-Feld **Massenaktionen** die gewünschte Aktion (**Aktivieren** oder **Deaktivieren**) aus.

   OT Security aktiviert oder deaktiviert die ausgewählten Richtlinien.

Richtlinien anzeigen

Im Bildschirm **Richtlinien** werden alle konfigurierten Richtlinien in Ihrem System aufgeführt. Die Listen sind für jede Richtlinienkategorie auf separaten Registerkarten gruppiert. Auf dieser Seite

werden sowohl vorkonfigurierte Richtlinien als auch benutzerdefinierte Richtlinien aufgelistet. 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. Informationen zum Anpassen der Liste finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.

In der folgenden Tabelle werden die Richtlinienparameter beschrieben:

Parameter	Beschreibung
Status	Zeigt an, ob die Richtlinie aktiviert oder deaktiviert ist. Wenn das System die Richtlinie automatisch deaktiviert hat, weil sie zu viele Ereignisse generiert hat, wird ein Warnsymbol neben dem Umschalter 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. Zum Beispiel P1für 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 Schweregrade.
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. Weitere Informationen zu den verschiedenen Kategorien finden Sie unter Kategorien und Unterkategorien von Richtlinien.
Quelle	Eine Richtlinienbedingung. Die Quell-Asset-Gruppe/das Quell-Netzwerksegment (d. h. das Asset, das die Aktivität initiiert hat), für die bzw. das die Richtlinie gilt.

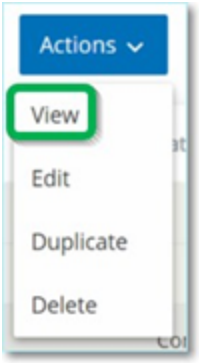
Ziel-Asset/ Betroffenes Asset	Eine Richtlinienbedingung. Die Ziel-Asset-Gruppe/ das Ziel-Netzwerksegment (d. h. das Asset, das die Aktivität erhält), für die bzw. das die Richtlinie gilt. Bei Richtlinien, die ein einzelnes Asset betreffen (ohne Quelle und Ziel), zeigt dieser Parameter das Asset an, das von dem Ereignis betroffen ist.
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, die die Ereignisbenachrichtigungen für diese Richtlinie sendet.
Unterkategorie	Die Unterkategorieklassifizierung des Ereignisses. Die Kategorie „Konfigurationsereignisse“ setzt sich aus den folgenden Unterkategorien zusammen: „Controller-Aktivitäten“ und „Controller-Validierung“. Informationen zu den verschiedenen Unterkategorien finden Sie unter Richtlinien anzeigen.
Anzahl der Ereignisse pro Richtlinie	Listet die Anzahl der Ereignisse auf, die von jeder Richtlinie generiert werden. Sie können auf die Spalte klicken, um die Liste zu sortieren, sodass Sie sich auf die Richtlinien mit den meisten Verstößen/ Ereignissen konzentrieren können.
Ausschlüsse	Listet die Anzahl der Ausschlüsse auf, die jeder Richtlinie hinzugefügt wurden. Weitere Informationen finden Sie unter Ereignisse.

Richtliniendetails anzeigen

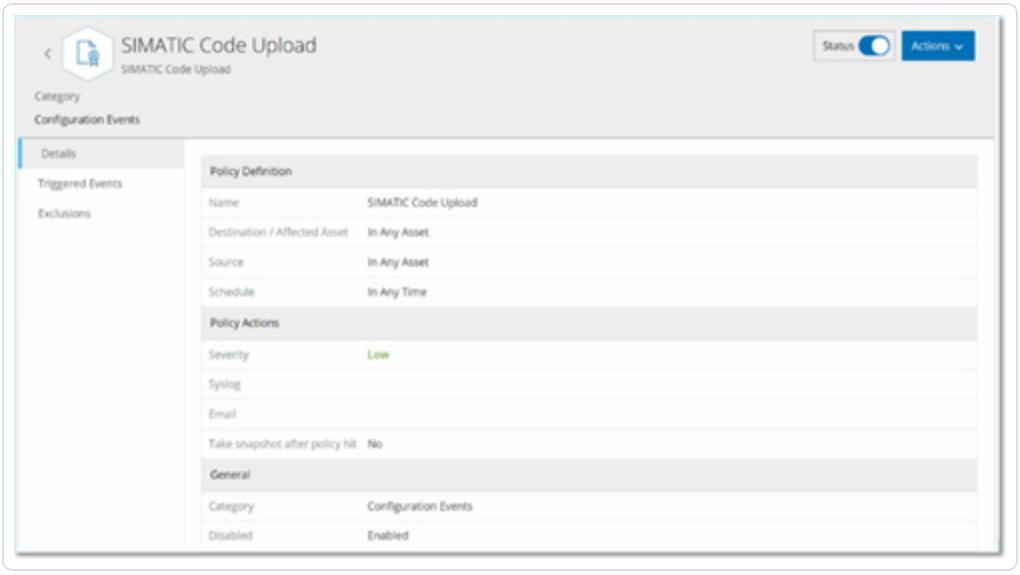
Sie können die Seite **Richtliniendetails** für eine Richtlinie öffnen, um weitere Details zur Richtlinie anzuzeigen. Auf dieser Seite werden alle Richtlinienbedingungen und -ereignisse aufgelistet, die durch die Richtlinie ausgelöst wurden.

So öffnen Sie den Bildschirm **Richtliniendetails** für eine bestimmte Richtlinie:

1. Wählen Sie auf der Seite **Richtlinien** die gewünschte Richtlinie aus.
2. Wählen Sie im Dropdown-Feld **Aktionen** die Option **Anzeigen** aus.



Die Seite „Richtliniendetails“ für die ausgewählte Richtlinie wird angezeigt.



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

Die Seite „Richtliniendetails“ enthält die folgenden Elemente:

- **Kopfleiste** – Zeigt Namen, Typ und Kategorie der Richtlinie an. Die Seite enthält außerdem 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 den folgenden Abschnitten an:

- **Richtliniendefinition** – Zeigt alle Richtlinienbedingungen an. Dies umfasst alle relevanten Felder gemäß dem Richtlinientyp.
- **Richtlinienaktionen** – Zeigt den Schweregrad sowie das Ziel (Syslog, E-Mail) von Ereignisbenachrichtigungen an. Zeigt auch an, ob die Funktion **Snapshot nach Richtlinientreffer erstellen** aktiviert ist.
- **Allgemein** – Zeigt die Kategorie und den Status der Richtlinie an.

- **Ausgelöste Ereignisse** – Zeigt eine Liste von Ereignissen an, die von dieser Richtlinie ausgelöst wurden. Außerdem werden Details zu den an dem Ereignis beteiligten Assets und die Art des Ereignisses angezeigt. Die auf dieser Registerkarte angezeigten Informationen sind identisch mit den Informationen auf der Seite **Ereignisse**, außer dass auf dieser Registerkarte nur Ereignisse für die angegebene Richtlinie angezeigt werden. Eine Erläuterung der Ereignisinformationen finden Sie unter Anzeigen von Ereignissen.

  Registerkarte **Ausschlüsse** – Wenn 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). Ausschlüsse können auf der Seite **Ereignisse** hinzugefügt werden, siehe Ereignisse. Auf der Registerkarte **Ausschlüsse** werden alle Ausschlüsse angezeigt, die für diese Richtlinie gelten. Für jeden Ausschluss werden außerdem die spezifischen ausgeschlossenen Bedingungen angegeben. Auf dieser Registerkarte können Sie einen Ausschluss löschen, was es dem System ermöglicht, die Generierung von Ereignissen für die angegebenen Bedingungen fortzusetzen.

Richtlinien erstellen

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

Hinweis: Richtlinien werden mithilfe von Gruppen definiert, die in Ihrem System konfiguriert sind. Wenn die Dropdown-Liste für einen bestimmten Parameter nicht die spezifische Gruppierung enthält, 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 eine Richtlinie nur für Controller gelten soll, 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 Richtlinien erstellen.

Hinweis: 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 Ereignisse.

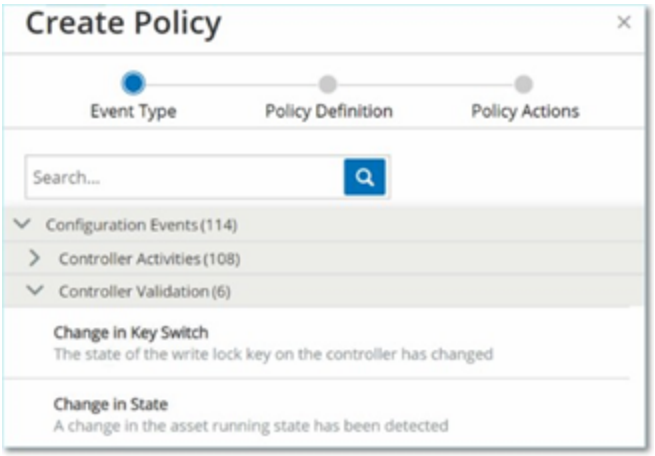
So erstellen Sie eine neue Richtlinie:

1. Klicken Sie im Bildschirm **Richtlinien** auf **Richtlinie erstellen**.

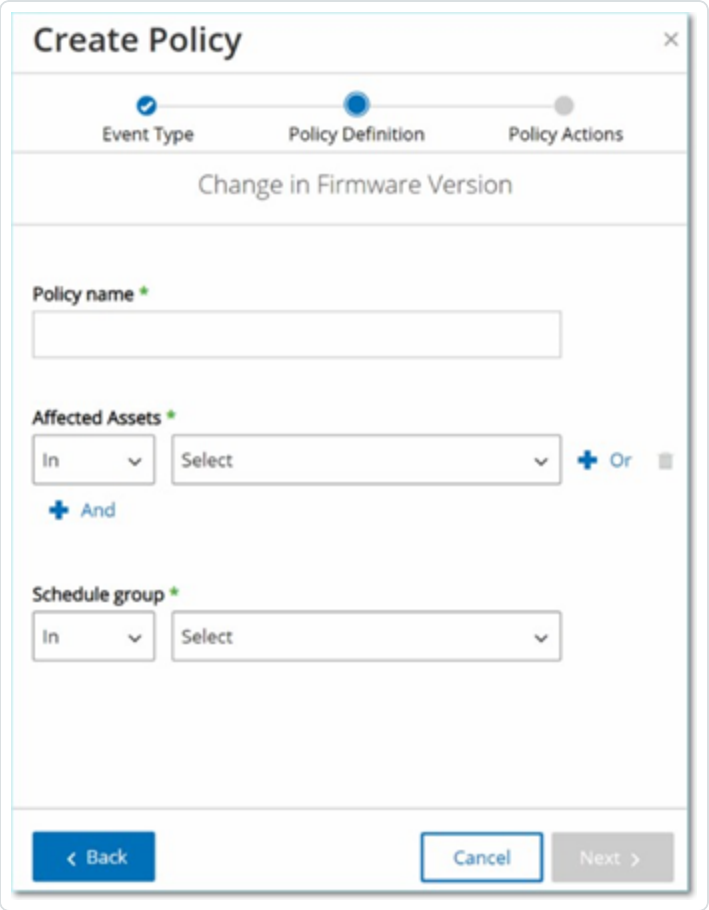
   Der Assistent **Richtlinie erstellen** wird geöffnet.

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.

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

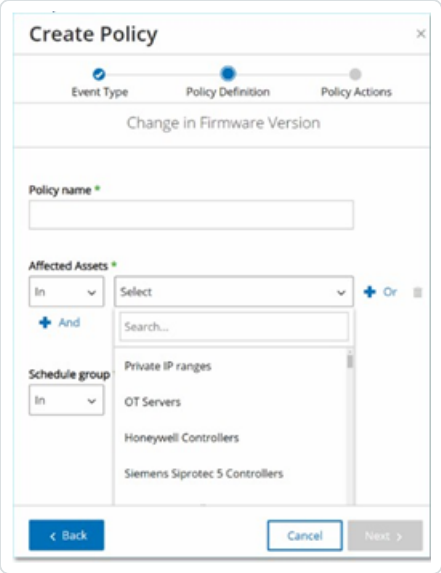
6. Führen Sie für jeden Parameter die folgenden Schritte aus:

   Wichtig: Für IDS-Ereignisse (Intrusion Detection System, Angriffserkennungssystem) können die Asset-Gruppen **Quelle** und **Ziel** nicht bearbeitet werden.

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.

> **Hinweis**: 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.

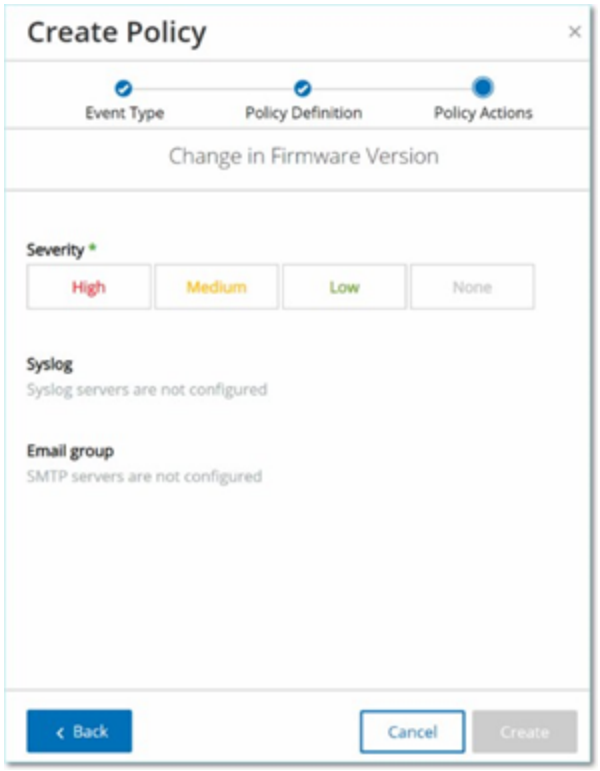
d. Wenn Sie für Asset-Parameter (d. h. „Quelle“, „Ziel“ und „Betroffene Assets“) eine zusätzliche Asset-Gruppe/ein zusätzliches Netzwerksegment mit einer „Oder“-Bedingung hinzufügen möchten, klicken Sie auf die blaue Schaltfläche **+ Oder** neben dem Feld und wählen Sie eine andere Asset-Gruppe/ein anderes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

wählen Sie eine andere Asset-Gruppe/ein anderes Netzwerksegment aus.

7. 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.

   Hinweis: 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“ in der Dropdown-Liste die zu benachrichtigende E-Mail-Gruppe aus.

    Hinweis: 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.)

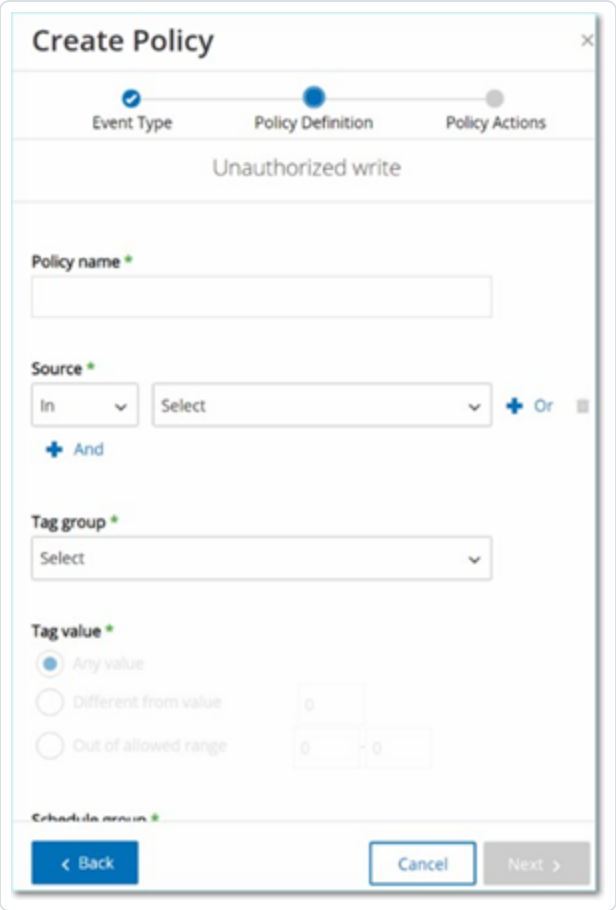
12. Klicken Sie auf **Erstellen**. Die neue Richtlinie wird erstellt und automatisch aktiviert. Die Richtlinie wird in der Liste im Bildschirm „Richtlinien“ angezeigt.

Richtlinien für nicht autorisierte Schreibvorgänge erstellen

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 Richtlinien erstellen beschrieben.



2. Wählen Sie im Abschnitt „Richtliniendefinition“ 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.

> **Hinweis**: 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 Richtlinien erstellen beschrieben durch.

Andere Aktionen zu Richtlinien

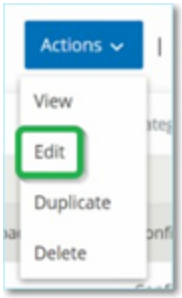
Richtlinien bearbeiten

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.

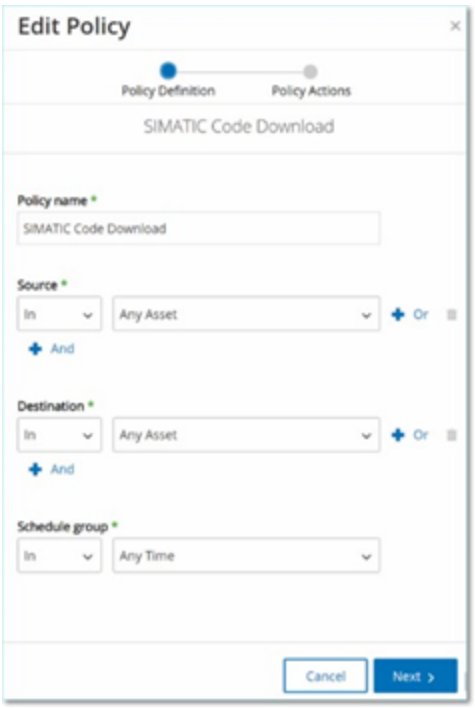
Außerdem können Sie die Parameter für **Richtlinienaktionen** für mehrere Richtlinien in einer Massenaktion bearbeiten.

So bearbeiten Sie eine Richtlinie:

1. Aktivieren Sie im Fenster **Richtlinien** das Kontrollkästchen neben der erforderlichen Richtlinie.
2. Wählen Sie im Dropdown-Feld **Aktionen** die Option **Bearbeiten** aus.



3. Das Fenster **Richtlinie bearbeiten** wird mit der aktuellen Konfiguration angezeigt.



4. Passen Sie die Parameter der **Richtliniendefinition** wie erforderlich an.

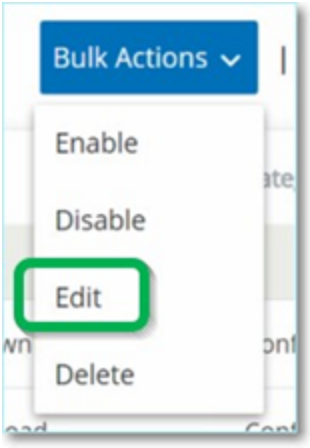
   Hinweis: Für IDS-Ereignisse (Intrusion Detection System, Angriffserkennungssystem) können die Asset-Gruppen **Quelle** und **Ziel** nicht bearbeitet werden.

5. Klicken Sie auf **Weiter**.
6. Passen Sie die Parameter der **Richtlinienaktionen** wie erforderlich an.
7. Klicken Sie auf **Speichern**.

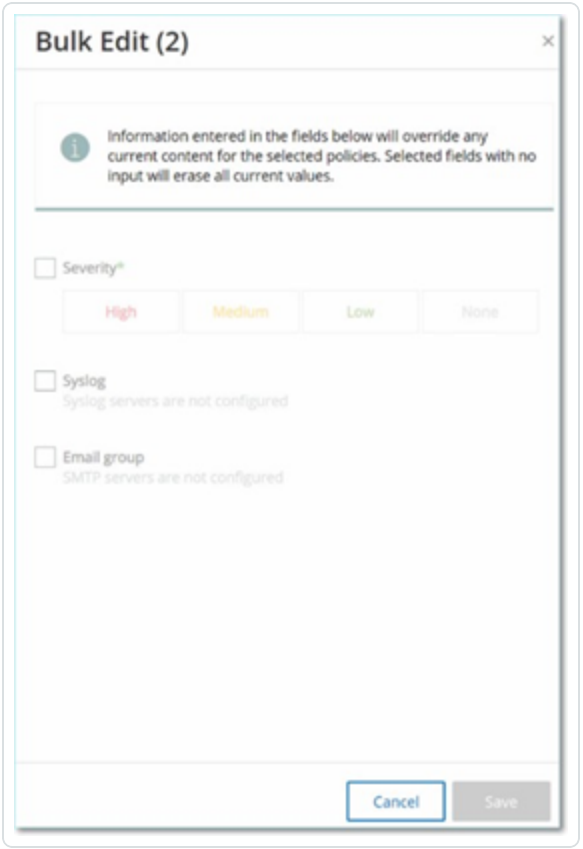
   OT Security speichert die Richtlinie mit der neuen Konfiguration.

So bearbeiten Sie mehrere Richtlinien (Massenprozess):

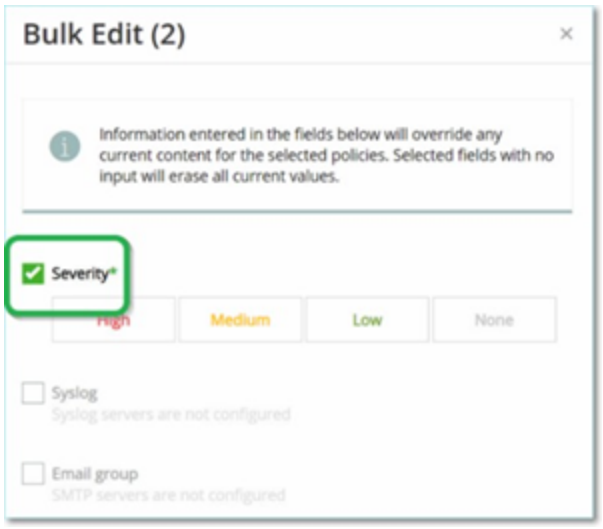
1. Aktivieren Sie im Fenster **Richtlinien** das Kontrollkästchen neben zwei oder mehr Richtlinien.
2. Wählen Sie im Dropdown-Feld **Massenaktionen** die Option **Bearbeiten** aus.



3. Das Fenster **Massenbearbeitung** wird mit den für die Massenbearbeitung verfügbaren Richtlinienaktionen angezeigt.



4. Aktivieren Sie das Kontrollkästchen neben jedem Parameter, den Sie bearbeiten möchten: **Schweregrad**, **Syslog**, **E-Mail-Gruppe**.



5. Stellen Sie jeden Parameter wie erforderlich ein.

   Hinweis: Durch die im Fenster **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.

6. Klicken Sie auf **Speichern**.

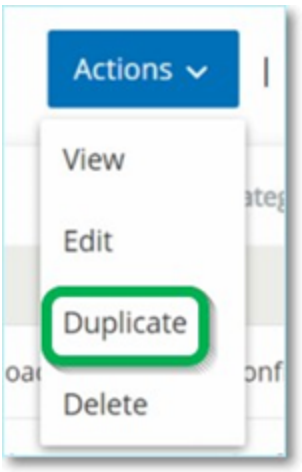
   OT Security speichert die Richtlinien mit der neuen Konfiguration.

Duplizierte Richtlinien

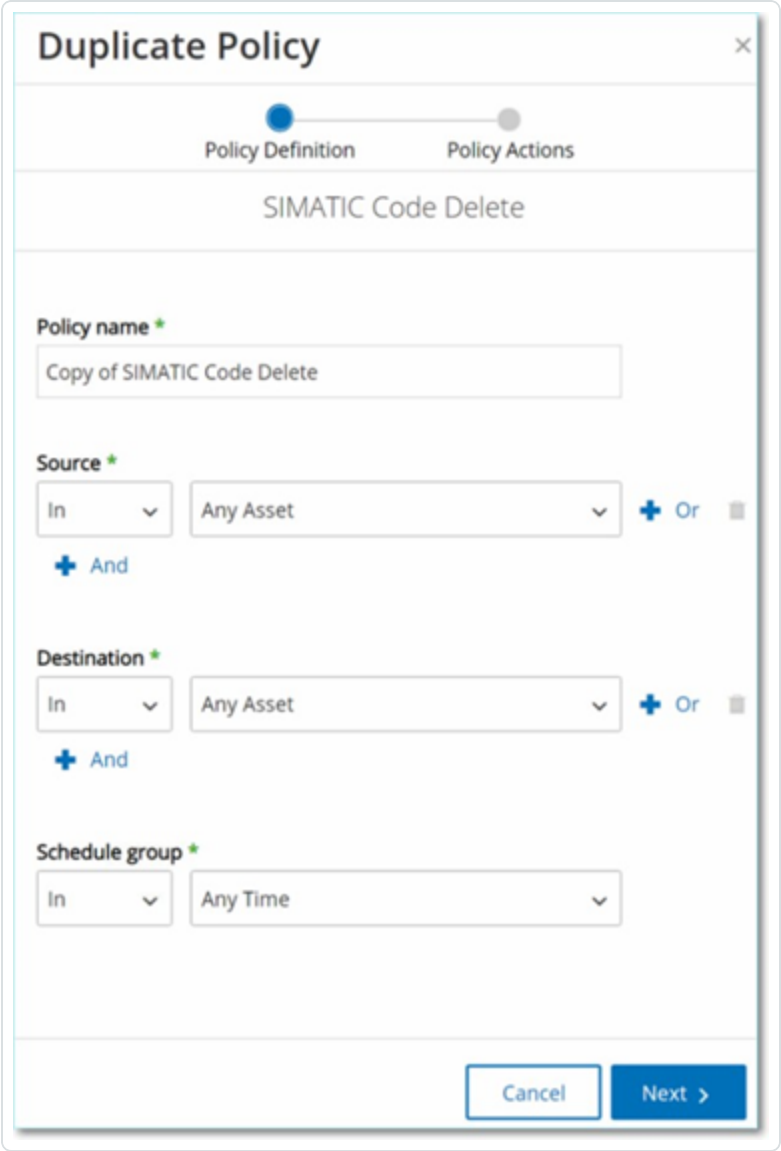
Sie können eine neue Richtlinie erstellen, die einer bestehenden Richtlinie ähnlich ist, indem Sie die ursprüngliche Richtlinie duplizieren und die gewünschten Anpassungen vornehmen. Sie können sowohl vordefinierte als auch benutzerdefinierte Richtlinien duplizieren (mit Ausnahme von **Intrusion Detection-Richtlinien**).

So duplizieren Sie eine Richtlinie:

1. Aktivieren Sie im Fenster **Richtlinien** das Kontrollkästchen neben der erforderlichen Richtlinie.
2. Wählen Sie im Dropdown-Feld **Aktionen** die Option **Duplizieren** aus.



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



4. Passen Sie die Parameter der **Richtliniendefinition** wie erforderlich an.
5. Klicken Sie auf **Weiter**.
6. Passen Sie die Parameter der **Richtlinienaktionen** wie erforderlich an.
7. Klicken Sie auf **Speichern**.

   OT Security speichert die Richtlinie mit der neuen Konfiguration.

Richtlinien löschen

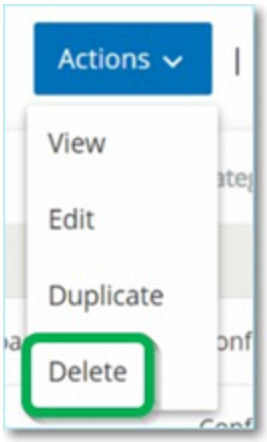
Sie können eine Richtlinie aus dem System löschen. Sie können sowohl vordefinierte als auch benutzerdefinierte Richtlinien löschen (mit Ausnahme von **Intrusion Detection-Richtlinien**, die nicht gelöscht werden können).

Sie können auch mehrere Richtlinien in einer Massenaktion löschen.

Hinweis: 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 Fenster **Richtlinien** das Kontrollkästchen neben der erforderlichen Richtlinie.
2. Wählen Sie im Dropdown-Feld **Aktionen** die Option **Löschen** aus.

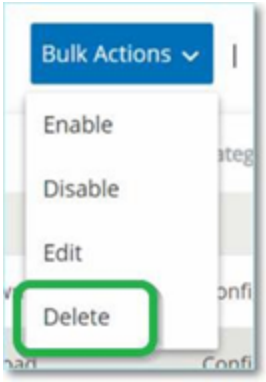


   Daraufhin wird ein Bestätigungsfenster angezeigt.
3. Klicken Sie auf **Löschen**.

   OT Security löscht die Richtlinie aus dem System.

So löschen Sie mehrere Richtlinien (Massenaktion):

1. Aktivieren Sie im Fenster **Richtlinien** das Kontrollkästchen neben jeder der erforderlichen Richtlinien.
2. Wählen Sie im Dropdown-Feld **Massenaktionen** die Option **Löschen** aus.



Daraufhin wird ein Bestätigungsfenster angezeigt.

3. Klicken Sie auf **Löschen**.

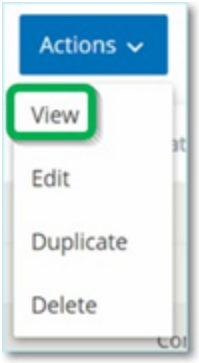
   OT Security löscht die Richtlinien aus dem System.

Richtlinienausschlüsse löschen

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

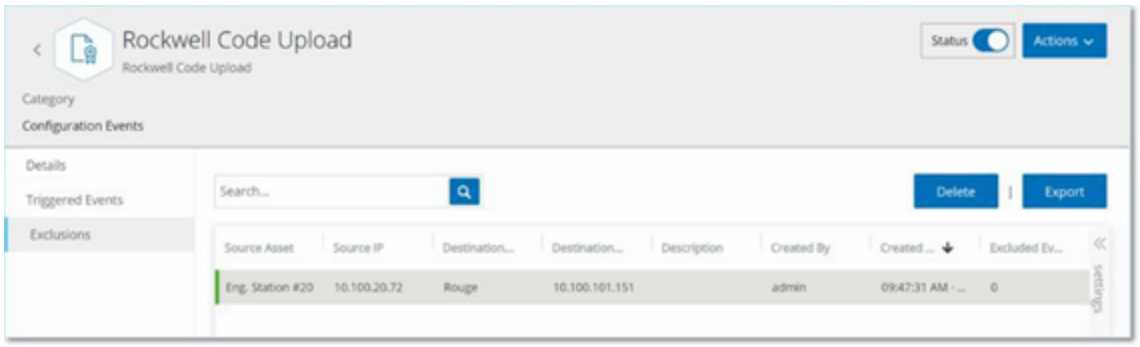
So löschen Sie einen Richtlinienausschluss:

1. Wählen Sie im Fenster **Richtlinien** die erforderliche Richtlinie aus.
2. Wählen Sie im Dropdown-Feld **Aktionen** die Option **Anzeigen** aus.



> **Hinweis**: 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**.

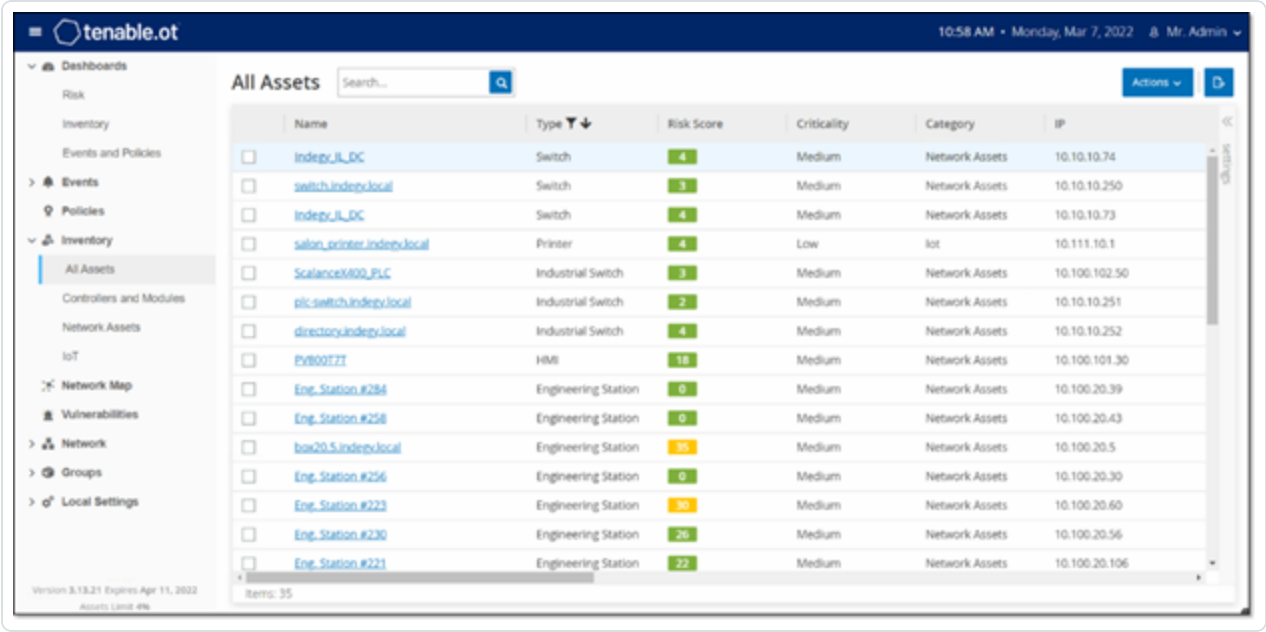
   Daraufhin wird ein Bestätigungsfenster angezeigt.
6. Klicken Sie im Bestätigungsfenster auf **Löschen**.

   OT Security löscht der Ausschluss aus dem System.

Inventar

Die automatisierte Asset-Erfassung, -Klassifizierung und -Verwaltung von OT Security 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**-Seiten angezeigt. Die Inventar-Seite enthält detaillierte Daten über Assets, was ein umfassendes Asset-Management sowie die Überwachung des Status jedes Assets und der damit verbundenen Ereignisse ermöglicht. OT Security erfasst diese Daten mit den Funktionen zur Netzwerkerkennung und der aktiven Abfrage. Die Seite **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**.

> **Hinweis**: Der Bildschirm „Netzwerk-Assets“ enthält alle Asset-Typen, 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 Assets-Listen sortieren und filtern sowie eine Suche durchführen. Informationen zum Anpassen von Tabellen finden Sie unter Elemente in der Benutzeroberfläche der Verwaltungskonsole.

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

Mit einem „*“ gekennzeichnete Parameter werden nur auf der Seite **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 Inventar).
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 Elemente in der Benutzeroberfläche der Verwaltungskonsole.
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 OT Security eingegeben. Siehe Asset-Details bearbeiten.
Zuletzt gesehen	Der Zeitpunkt, zu dem das Gerät zuletzt von OT Security 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 OT Security konfiguriert. Siehe Asset-Details bearbeiten.
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.
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

In der folgenden Tabelle werden die verschiedenen Arten von Assets beschrieben, die von OT Security identifiziert werden. Die Tabelle zeigt auch das Symbol, mit dem die einzelnen Asset-Typen in der OT Security-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
				Strom versorgung
				Backplane-Modul
Feldgeräte	Hoch/1	Ein industrielles Gerät (z. B. Sensor, Aktuator, Elektromotor), das Industrieprotokolle verwendet, um Informationen an ICS-Systeme zu senden.		Feldgerät
				Strom messgerät
				Remote-E/A
				Relay
				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
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		Workstation

		Workstations und ihre zugehörigen Komponenten.		
				OT-Workstation
				Engineering-Station
				Virtuelle Workstation
Server	Gering/3	Diese Kategorie umfasst verschiedene Arten von IT-Servern.		Server
				Dateiserver
				Webserver
				Virtueller Server
				Sicherheits-Appliance

				Tenable ICP
				Tenable EM
				Tenable Sensor
				Domänen controller
				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
		Zugangs kontrollsystem
		Beleuchtungs steuerung
		HLK-Modul
		Intelligenter Hub

				Smart-TV
				Medizinisches Gerät
				Tablet
				Mobilgerät
				Speichergerät
Endgeräte	Gering/3	Eine nicht identifizierte IP-Adresse im Netzwerk.		Endgerät

Asset-Details anzeigen

Der Bildschirm **Asset-Details** zeigt umfassende Details zu allen Daten an, die von OT Security für ein ausgewähltes 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.

So greifen Sie auf die Seite **Asset-Details** für ein bestimmtes Asset zu:

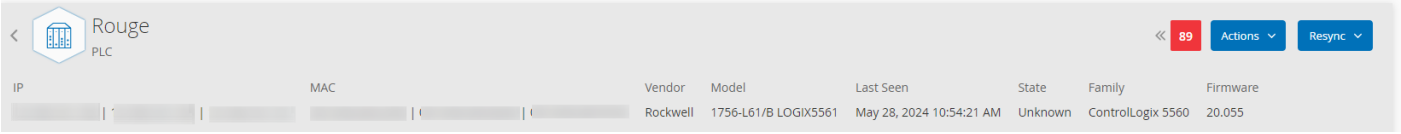
1. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf einer dieser Seiten, auf der der Asset-Name als Link angezeigt wird, auf den Asset-Namen: **Inventar**, **Ereignisse** oder **Netzwerk**.
    - Klicken Sie auf der Seite **Inventar** auf **Aktionen** > **Anzeigen**.

Die folgenden Elemente sind im Fenster **Asset-Details** enthalten (für relevante Asset-Typen):

- **Kopfleistenbereich** – Zeigt einen Überblick der wichtigen Informationen über das Asset und seinen aktuellen Zustand an. Er enthält auch ein Menü Aktionen, mit dem Sie die Auflistung für dieses Asset bearbeiten können.
- **Details** – Zeigt detaillierte Informationen an, 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 OT Security 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 an, die sich auf das Asset beziehen.
- **Angriffsvektoren** – Zeigt anfällige Angriffsvektoren an, 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 behobenen und aktiven Schwachstellen an, 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 an.
- **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.
- Link „Zurück“ – 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 Tenable Nessus-Scan auszuführen.
- **Erneut synchronisieren** – Klicken Sie auf diese Schaltfläche, um eine oder mehrere der Abfragen, die für dieses Asset verfügbar sind, manuell auszuführen. Siehe Erneute Synchronisierung durchführen.

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. OT Security zeigt nur die Abschnitte an, die für das angegebene Asset relevant sind. Die folgende Liste enthält alle möglichen Abschnittskategorien für verschiedene Asset-Typen: Übersicht, Allgemein, Projekt, Speicher, Ethernet, Profinet, Betriebssystem, System, Hardware, Geräte und Laufwerke, USB-Geräte, Installierte Software, IEC 61850 und Schnittstellenstatus.

Hinweis: OT Security zeigt nur die Details an, die aus dem Asset extrahiert werden. Möglicherweise werden nicht alle Abschnitte für alle Assets angezeigt. Zum Beispiel **Allgemein**, **Nessus-Scan-Informationen**.

Die folgende Tabelle zeigt die Details im Abschnitt **Übersicht**:

Abschnitt	Beschreibung
Name	Der Asset-Name, der entweder durch passives Monitoring oder aktives Abfragen erhalten oder automatisch unter Verwendung des Asset-Typs und eines eindeutigen Bezeichners generiert wird.
Beschreibung	Die Beschreibung des Assets vom Benutzer.
Purdue-Level	Das Purdue-Modell-Level, das dem Asset zugewiesen ist.
Status	Der aktuelle Betriebsstatus des Assets. Das Feld ist für bestimmte Asset-Typen relevant, in der Regel Controller.
Direkte IP	Die IP-Adresse, die auf diesem spezifischen Asset oder Modul vorhanden oder für dieses konfiguriert ist.
Direkte Mac	Die Mac-Adresse, die auf diesem spezifischen Asset oder Modul physisch vorhanden oder für dieses konfiguriert ist.
Zusätzliche IPs	IP-Adressen, die mit anderen Modulen verknüpft sind, die eine Backplane oder eine ähnliche Infrastruktur mit dem Asset gemeinsam nutzen, und für den indirekten Zugriff auf das Asset verwendet werden. Beispielsweise verfügt eine SPS (Controller-Modul) möglicherweise nicht über eine eigene Netzwerkschnittstelle und der Zugriff erfolgt über eine IP-Adresse, die auf einem Kommunikationsmodul

	konfiguriert ist, das in einem anderen Steckplatz installiert ist. Beachten Sie, dass das Asset möglicherweise auch über andere Verbindungen als eine Backplane verfügt.
Zusätzliche Macs	Mac-Adressen, die mit anderen Modulen verknüpft sind, die eine Backplane oder eine ähnliche Infrastruktur gemeinsam nutzen, und für den indirekten Zugriff auf das Asset verwendet werden.
Familie	Die Gerätefamilie oder Produktreihe, zu der das Asset gehört.
Anbieter	Der Hersteller oder Anbieter des Assets.
Modellname	Die spezifische Modellnummer des Assets.
Zuletzt gesehen	Das Datum und die Uhrzeit, zu der OT Security das Asset zuletzt erfasst hat. OT Security kann dieses Feld aktualisieren, wenn eine PCAP-Datei (Traffic-Capture-Datei) wiedergegeben oder eine ähnliche Analyse durchgeführt wird.
Zum ersten Mal gesehen	Das Datum und die Uhrzeit, zu der das Asset zum ersten Mal erkannt wurde. Dies kann dem Wert **Zuletzt gesehen** entsprechen oder davor liegen.
Letzte Aktualisierung	Das Datum und die Uhrzeit der letzten Aktualisierung von Asset-Details. **Hinweis**: Bei jeder manuellen Änderung an den Asset-Informationen, wie z. B. eine Aktualisierung der Beschreibung, wird dieser Wert aktualisiert, unabhängig davon, ob das Asset derzeit aktiv ist oder vor Kurzem erkannt wurde.
Quellen	Die Quellen (z. B. Sensoren, PCAPs, lokale Schnittstellen), die identifiziert wurden oder mit dem Asset verbunden sind.
Netzwerksegmente	Die Netzwerksegmente, die dem Asset zugewiesen oder mit ihm verknüpft sind.
Kritikalität	Die Wichtigkeit des Assets, die als hoch, mittel oder gering bewertet

	wird.
Risikowert	Spiegelt die potenziellen Auswirkungen des mit dem Asset verbundenen Risikos wider. Die Bewertung wird durch Faktoren wie Kritikalität, Schwachstellen, nicht aufgelöste Ereignisse (und ihre Dauer), zugehörige Assets (z. B. über Backplane) und andere relevante Überlegungen beeinflusst.

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 OT Security-„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.

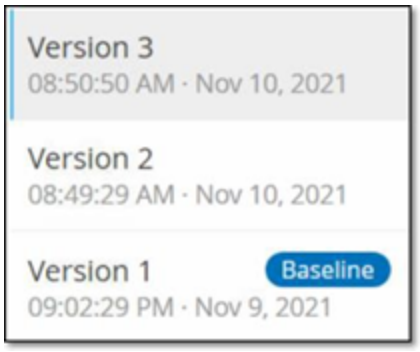
Ein Snapshot kann auf folgende Weise ausgelöst werden:

- **Routine** – Snapshots werden in regelmäßigen Abständen erstellt, wie vom Benutzer im Bildschirm mit 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-Aktivitätsereignissen.

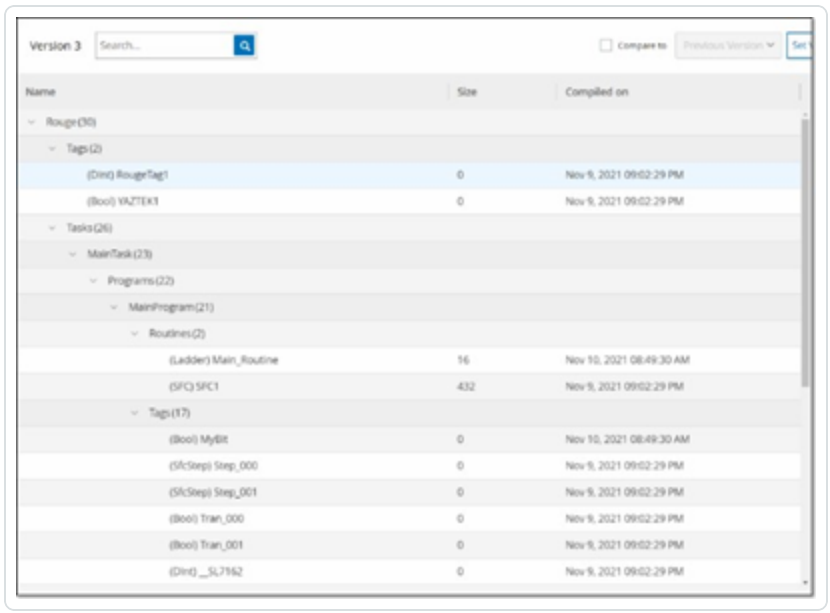
In den folgenden Abschnitten werden die verschiedenen Abschnitte der Coderevisionsanzeige sowie der Vergleich verschiedener „Snapshot“-Versionen beschrieben.

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.

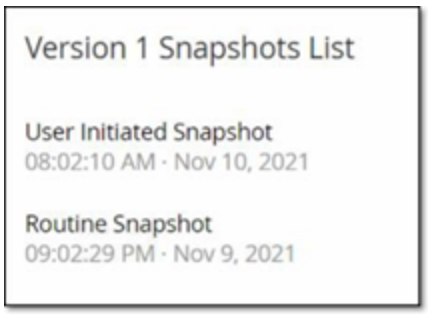
Bereich „Snapshot-Details“



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 Snapshot-Versionen vergleichen.

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.

Snapshot-Versionen vergleichen

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.

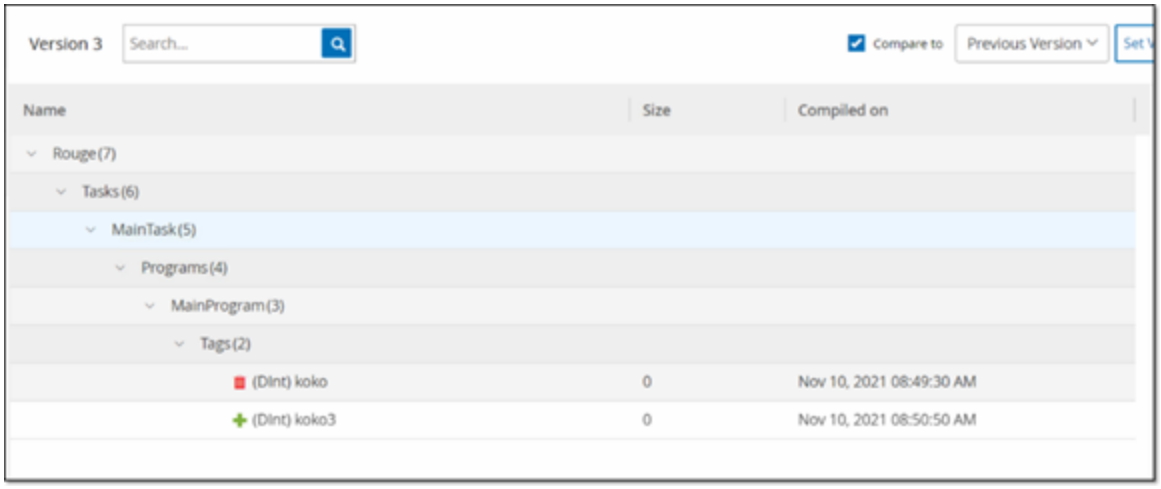
✎ Bearbeitet – Code, der in der ausgewählten Version bearbeitet wurde.

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.

   > **Hinweis**: Die Festlegung 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“. Wählen Sie im Feld neben dem Kontrollkästchen „Vergleichen mit“ die Option Baseline-Version aus dem Dropdown-Menü aus.
7. Der Bereich „Snapshot-Details“ zeigt alle Unterschiede zwischen den beiden Versionen. Für jede Änderung gibt ein Symbol die Art der aufgetretenen Änderung an.

Snapshot erstellen

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, an dem bzw. 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, an dem bzw. 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 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).
- Untersuchung der Kommunikationswege entlang der Kette und Prüfung 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.

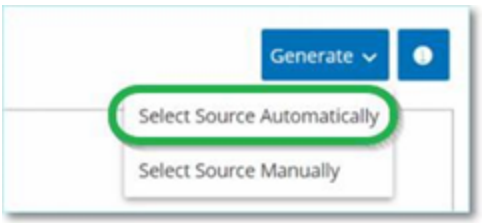
Angriffsvektoren generieren

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** – OT Security bewertet alle potenziellen Angriffsvektoren und identifiziert den anfälligsten Pfad.
- **Manuell** – Sie geben ein bestimmtes Quell-Asset an, und OT Security 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**.

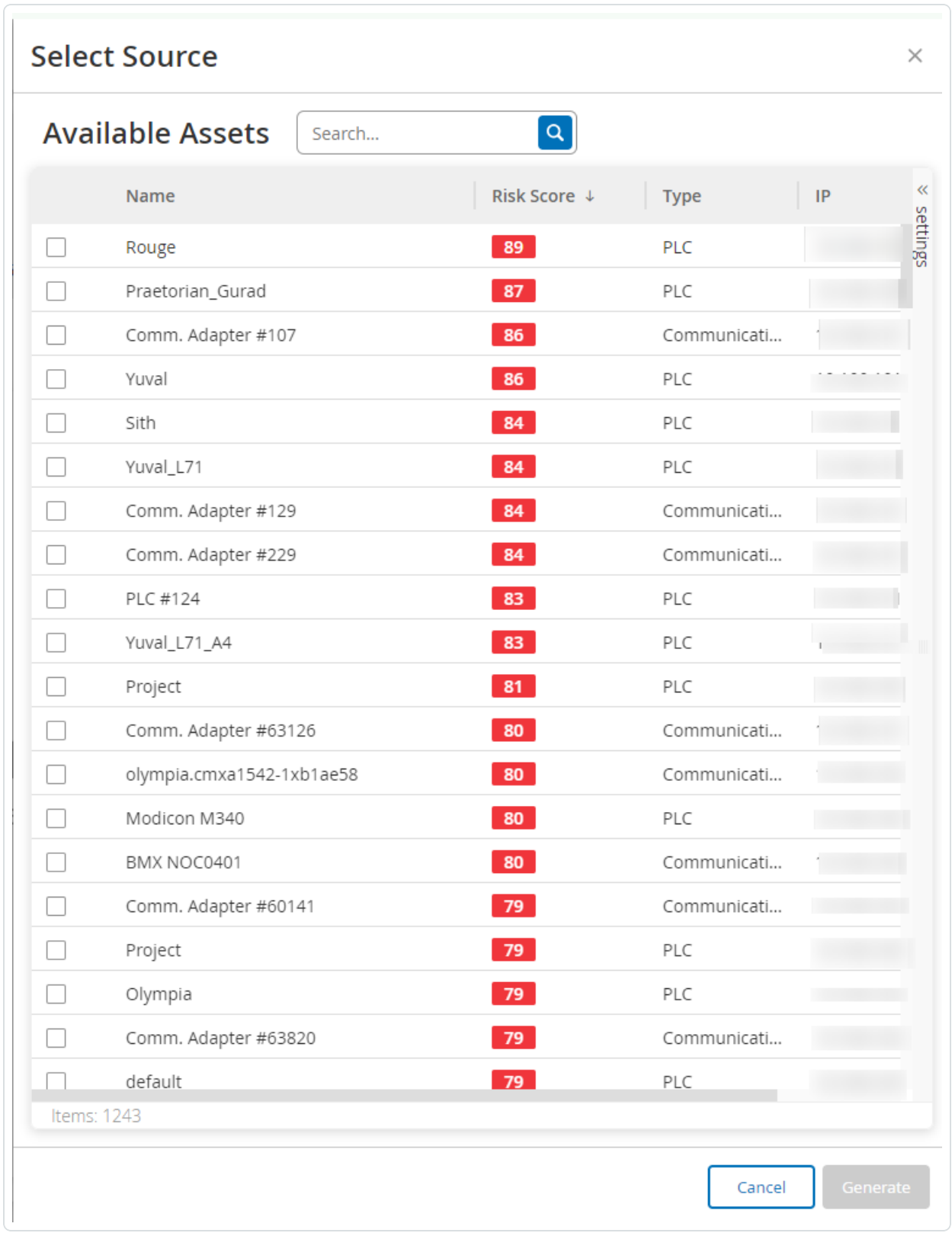


Der Angriffsvektor wird automatisch generiert und auf der Registerkarte **Angriffsvektor** angezeigt.

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.


Select Source
Available Assets
Search...
Name
Risk Score
Type
IP
settings
Rouge 89 PLC
Praetorian_Gurad 87 PLC
Comm. Adapter #107 86 Communicati...
Yuval 86 PLC
Sith 84 PLC
Yuval_L71 84 PLC
Comm. Adapter #129 84 Communicati...
Comm. Adapter #229 84 Communicati...
PLC #124 83 PLC
Yuval_L71_A4 83 PLC
Project 81 PLC
Comm. Adapter #63126 80 Communicati...
olympia.cmxa1542-1xb1ae58 80 Communicati...
Modicon M340 80 PLC
BMX NOC0401 80 Communicati...
Comm. Adapter #60141 79 Communicati...
Project 79 PLC
Olympia 79 PLC
Comm. Adapter #63820 79 Communicati...
default 79 PLC
Items: 1243
Cancel
Generate

Hinweis: 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.

Hinweis: 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, Tenable Network Monitor- oder Tenable 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 für das Scannen offener Ports werden unter Aktive Abfragen konfiguriert. 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.

   OT Security führt einen Scan auf dem ausgewählten Port durch.

So zeigen Sie das Portal für das Asset an:

Hinweis: 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.

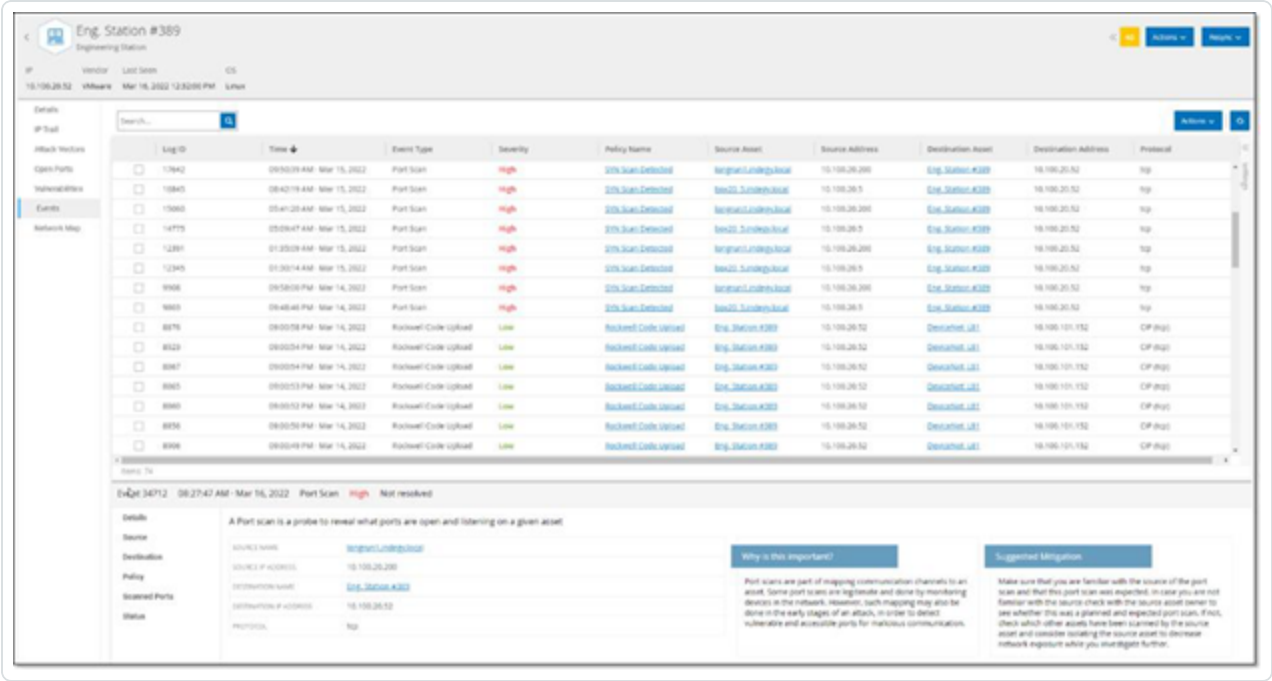
Schwachstellen

Auf der Registerkarte **Schwachstellen** wird eine Liste aller Schwachstellen angezeigt, die das angegebene Asset betreffen und die von OT Security-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. Die Schwachstellen werden in zwei Kategorien aufgeführt: **Aktiv** und **Behoben**. Jede Auflistung enthält Details über die Art der Bedrohung und ihren Schweregrad. Die auf dieser Registerkarte angezeigten Informationen sind identisch mit den Informationen auf der Seite **Schwachstellen**, mit dem Unterschied, dass auf dieser Seite 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 OT Security-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 Elemente in der Benutzeroberfläche der Verwaltungskonsole.



Im unteren Teil der Seite 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 Bereich befindet sich eine Schaltfläche **Aktionen**, mit der Sie die folgenden Aktionen für die ausgewählten Ereignisse ausführen können:

- **Auflösen** – Dieses Ereignis als „Aufgelöst“ markieren.
- **Erfassungsdatei herunterladen** – Die PCAP-Datei für dieses Ereignis herunterladen.
- **Aus Richtlinie ausschließen** – Einen Richtlinienausschluss für dieses Ereignis erstellen.

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.
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 Typen 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 und Unterkategorien): • 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.

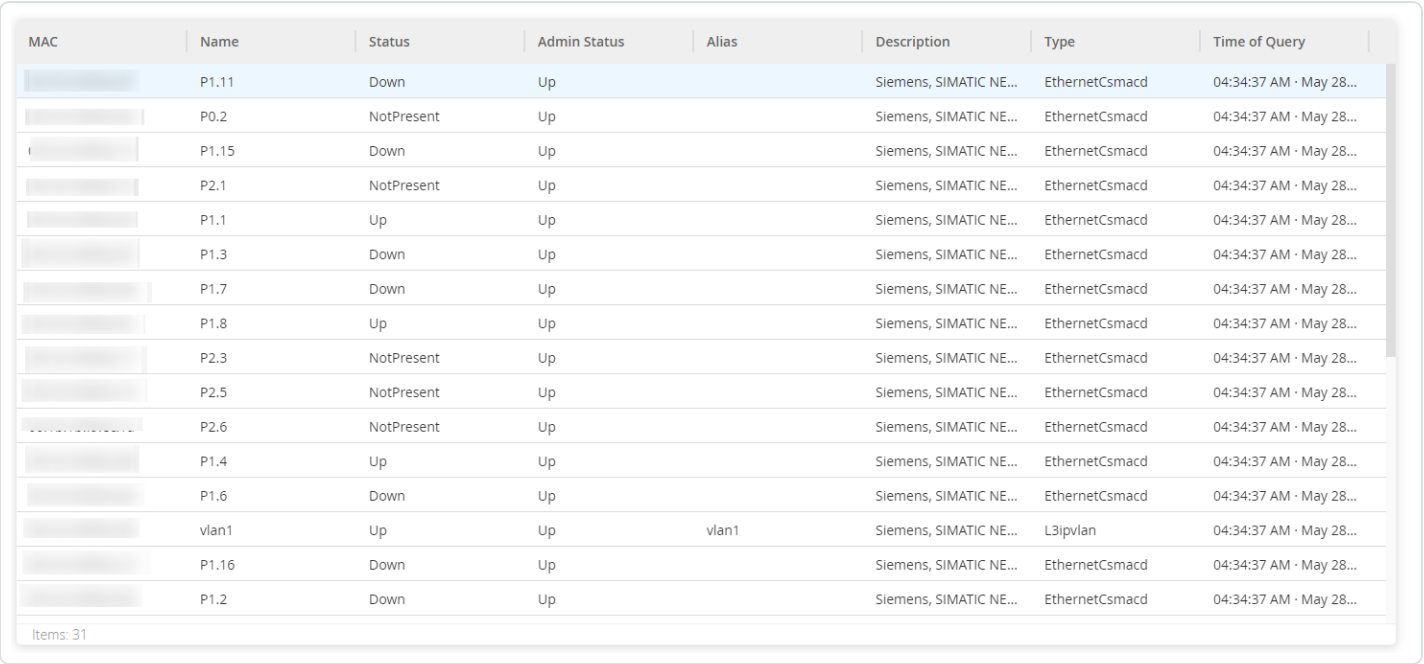
Die auf dieser Registerkarte angezeigten Informationen ähneln den im Bildschirm **Netzwerkübersicht** angezeigten Informationen, sind jedoch auf Verbindungen beschränkt, die dieses spezifische Asset betreffen. Außerdem zeigt dieser Bildschirm Verbindungen zu einzelnen Assets und nicht zu Asset-Gruppen, 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** ist für Netzwerk-Switches verfügbar und enthält Details zu den Ports auf dem Netzwerk-Switch. OT Security sammelt diese Daten mithilfe von SNMP-Abfragen an den Switch. Die angezeigten Details der jeweiligen Ports enthalten MAC-Adresse, Name, Verbindungsstatus (aktiv oder inaktiv), Alias und Beschreibung.



MAC	Name	Status	Admin Status	Alias	Description	Type	Time of Query
	P1.11	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P0.2	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.15	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.1	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.1	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.3	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.7	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.8	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.3	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.5	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P2.6	NotPresent	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.4	Up	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.6	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	vlan1	Up	Up	vlan1	Siemens, SIMATIC NE...	L3ipvlan	04:34:37 AM · May 28...
	P1.16	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...
	P1.2	Down	Up		Siemens, SIMATIC NE...	EthernetCsmacd	04:34:37 AM · May 28...

Items: 31

Hinweis: Aktivieren Sie diese Funktion in Ihrem Konto, damit die Registerkarte sichtbar ist. Um diese Funktion zu aktivieren, wenden Sie sich an den Tenable-Support.

Asset-Details bearbeiten

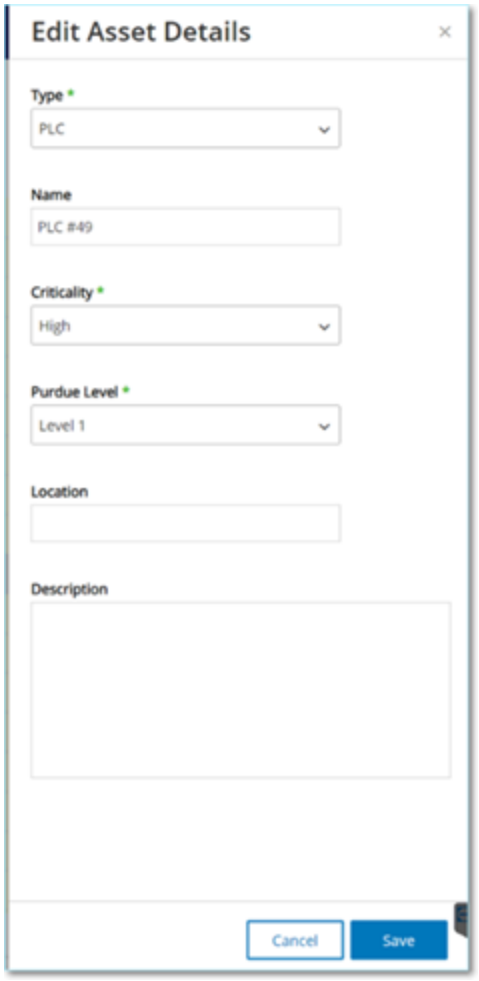
OT Security identifiziert Typ und Name des Assets automatisch anhand seiner internen Daten und seiner Aktivität im Netzwerk. Wenn das System diese Informationen nicht erfassen konnte oder Sie der Meinung sind, dass die automatische Identifizierung nicht korrekt ist, können Sie diese Parameter entweder 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.

Asset-Details über die Benutzeroberfläche bearbeiten

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 OT Security 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 auf der Seite „Asset-Details“ für dieses Asset angezeigt.
12. Klicken Sie auf **Speichern**.

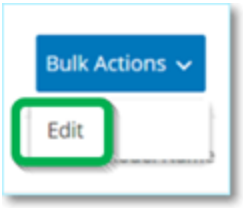
    OT Security speichert die bearbeiteten Details.

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.

   > **Hinweis**: 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** in 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).

   > **Hinweis**: Filtern Sie bei der Massenbearbeitung von Netzwerksegmenten zuerst Ihre Assets nach **Typ** und wählen Sie dann die Assets aus, die Sie in einem 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 nach Bedarf ein.

   Hinweis: Die in die Felder für die Massenbearbeitung eingegebenen Informationen überschreiben alle aktuellen Inhalte für das ausgewählte Asset. 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**.

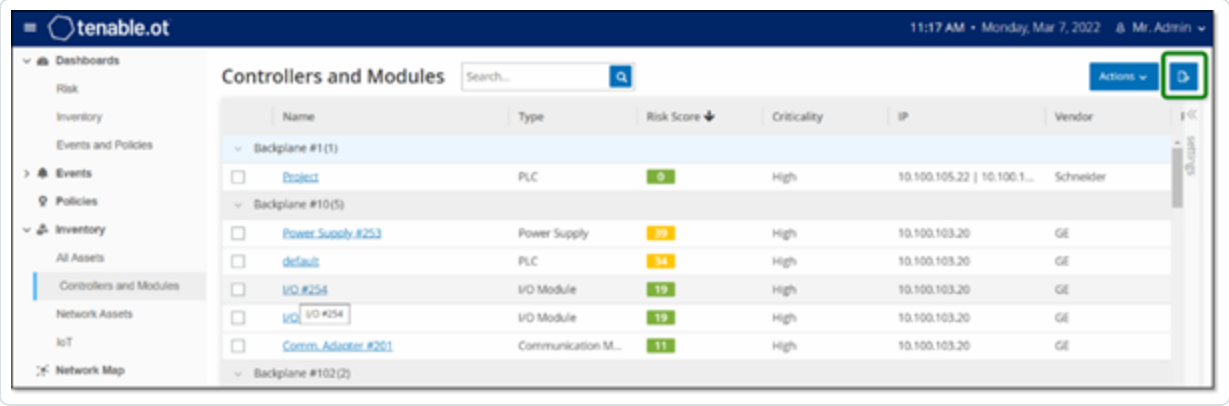
   OT Security speichert die Assets mit der neuen Konfiguration.

Asset-Details durch Hochladen einer CSV-Datei bearbeiten

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.

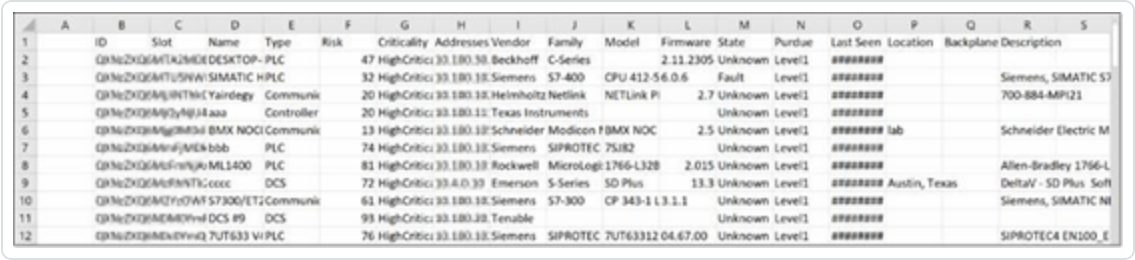
So bearbeiten Sie Asset-Details über eine CSV-Datei:

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.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1		ID	Slot	Name	Type	Risk	Criticality	Addresses	Vendor	Family	Model	Firmware	State	Purdue	Last Seen	Location	Backplane	Description	
2				DESKTOP-	PLC		47	HighCritici	10.180.50.	Beckhoff	C-Series	2.11.2305	Unknown	Level1	########				
3				SIMATIC H	PLC		32	HighCritici	10.180.10.	Siemens	S7-400	CPU 412-5	6.0.6	Fault	Level1	########			Siemens, SIMATIC S7
4				Yairdegy	Communic		20	HighCritici	10.180.10.	Helmholtz	Netlink	NETLink PI	2.7	Unknown	Level1	########			700-884-MPI21
5				aaa	Controller		20	HighCritici	10.180.11.	Texas Instruments				Unknown	Level1	########			
6				BMX NOCI	Communic		13	HighCritici	10.180.10.	Schneider	Modicon P	BMX NOC	2.5	Unknown	Level1	########	lab		Schneider Electric M
7				bbb	PLC		74	HighCritici	10.180.10.	Siemens	SIPROTEC	7SJ82		Unknown	Level1	########			
8				ML1400	PLC		81	HighCritici	10.180.10.	Rockwell	MicroLogi	1766-L32B	2.015	Unknown	Level1	########			Allen-Bradley 1766-L
9				cccc	DCS		72	HighCritici	10.4.0.10	Emerson	S-Series	SD Plus	13.3	Unknown	Level1	########	Austin, Texas		DeltaV - SD Plus Soft
10				S7300/ET2	Communic		61	HighCritici	10.180.10.	Siemens	S7-300	CP 343-1 L	3.1.1	Unknown	Level1	########			Siemens, SIMATIC NI
11				DCS #9	DCS		93	HighCritici	10.180.10.	Tenable				Unknown	Level1	########			
12				7UT633 V4	PLC		76	HighCritici	10.180.10.	Siemens	SIPROTEC	7UT63312	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.)

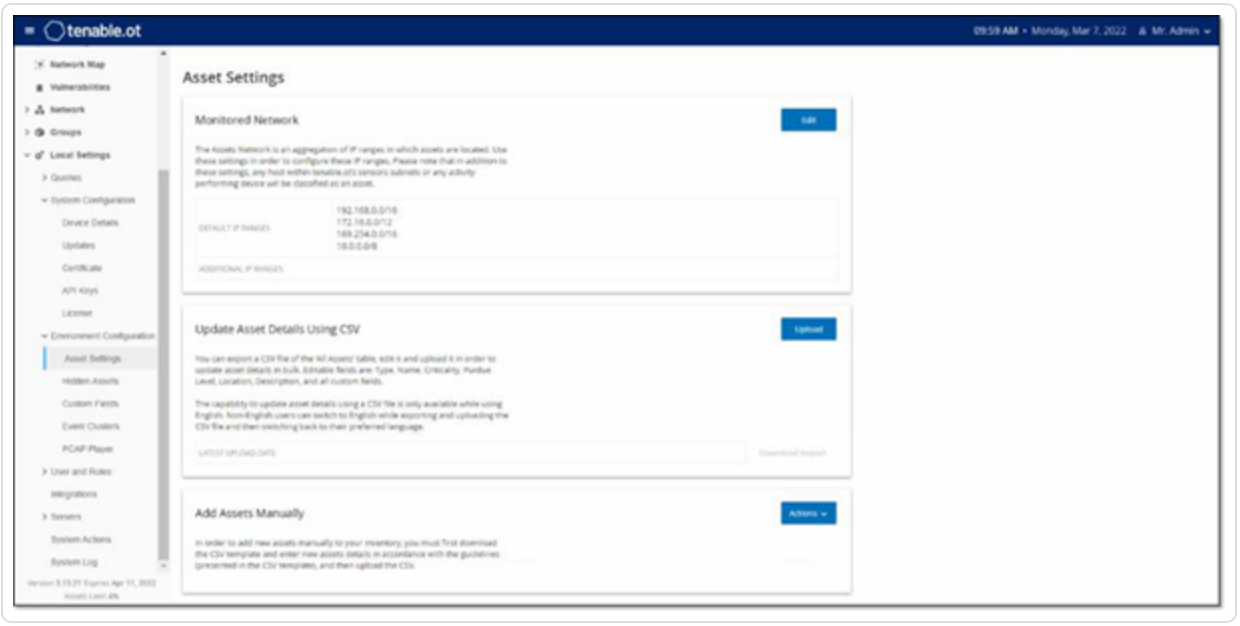
   Hinweis: Sie müssen gültige Daten für Parameter eingeben, die bestimmte Optionen erfordern (z. B. Typ, Kritikalität, Purdue-Level). Andernfalls kann das jeweilige Asset nicht aktualisiert werden.

5. Speichern Sie die Datei als CSV-Dateityp.

   Hinweis: 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**.

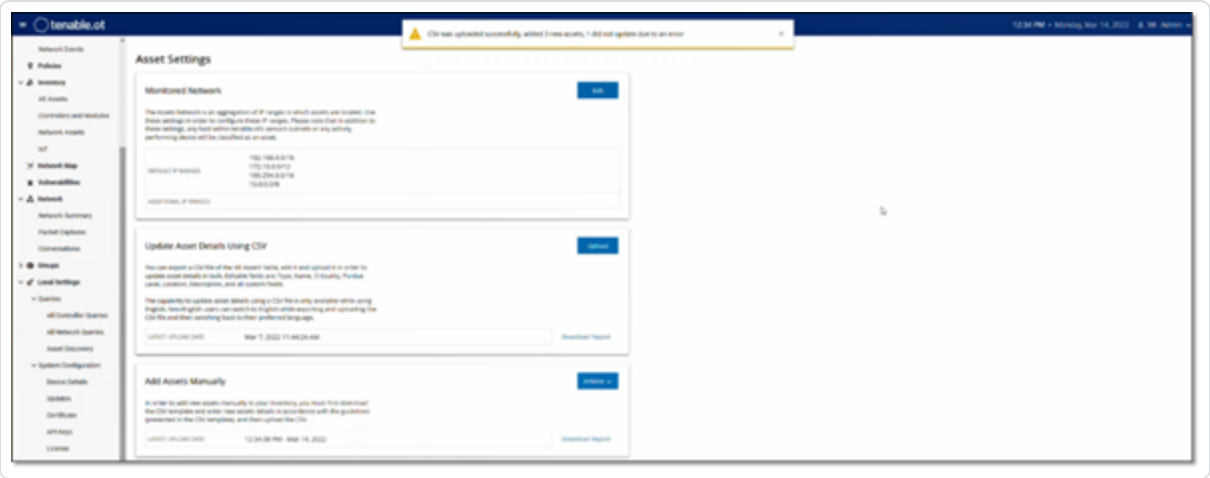
   Die Seite **Asset-Einstellungen** wird angezeigt.



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 erscheint eine Bestätigung, die die Anzahl der aktualisierten Zeilen angibt.



   Das Feld **Datum des letzten Uploads** im Abschnitt „Asset-Details per CSV aktualisieren“ wird aktualisiert.

9. Um weitere Informationen zu den Ergebnissen des Uploads zu sehen, klicken Sie im Abschnitt **Asset-Details per CSV aktualisieren** auf **Bericht herunterladen**.

   OT Security lädt eine CSV-Datei herunter, die die aktualisierten Asset-IDs auflistet und auch die fehlgeschlagenen Asset-IDs auflistet.

Assets ausblenden

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.

Sie können ein ausgeblendetes Asset über die Seite **Lokale Einstellungen** > **Umgebungskonfiguration** > **Ausgeblendete Assets** wiederherstellen.

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 **Aktionen**.

   Ein Menü wird angezeigt.
4. Wählen Sie **Asset ausblenden** aus.

   Die Seite **Ausgeblendete Assets** wird angezeigt.
5. (Optional) Fügen Sie im Feld **Kommentare** Textkommentare zu den Assets hinzu.

   > **Hinweis**: Die Kommentare werden in der Liste der entfernten Assets auf der Seite **Lokale Einstellungen** > **Umgebungskonfiguration** > **Ausgeblendete Assets** angezeigt.
6. Klicken Sie auf **Ausblenden**.

   OT Security blendet die Assets auf den Seiten **Inventar** und **Gruppen** aus.

Asset-spezifischen Tenable Nessus-Scan durchführen

Tenable Nessus ist ein Tool, mit dem IT-Geräte gescannt werden können, um Schwachstellen zu erkennen. Mit OT Security können Sie den **Basic Network Scan** von Tenable Nessus 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 verfügbar sind. Diese Aktion ist nur für relevante PC-basierte Maschinen verfügbar. Die Scan-Ergebnisse können Sie auf der Seite „Schwachstellen“ einsehen. Sie können auch benutzerdefinierte Scans erstellen, um einen bestimmten Satz von Tenable Nessus-Plugins für einen bestimmten Satz von Netzwerkressourcen auszuführen, siehe Tenable NessusPlugin-Scans.

Der Nessus-Scan in OT Security verwendet die gleichen Richtlinieneinstellungen wie ein Netzwerk-Basisscan in Tenable Nessus, Tenable Security Center und Tenable Vulnerability Management. Der einzige Unterschied sind die Leistungsoptionen in OT Security. Im Folgenden sind die Leistungsoptionen für den Nessus-Scan in OT Security aufgeführt. Diese Optionen gelten auch für den Nessus-Scan, den Sie über die Seite **Verwaltung aktiver Abfragen** starten.

- 5 Hosts gleichzeitig (max.)
- 2 gleichzeitige Prüfungen pro Host (max.)
- 15 Sekunden Zeitüberschreitung für Lesevorgänge im Netzwerk

Hinweis: Tenable Nessus ist ein invasives Tool, das am besten in IT-Umgebungen funktioniert. Tenable empfiehlt, es nicht auf OT-Geräten zu verwenden, da es deren normalen Betrieb beeinträchtigen kann.

So führen Sie einen Tenable Nessus-Scan für bestimmte Assets aus:

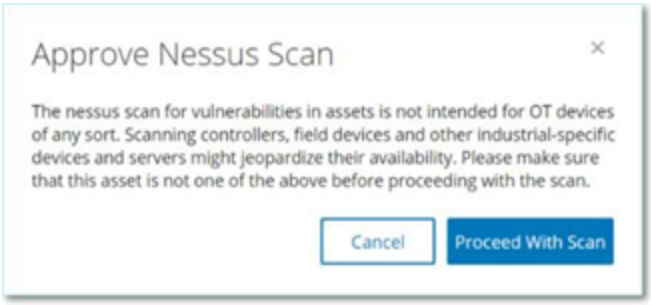
1. Gehen Sie zu **Inventar** > **Netzwerk-Assets**.

   Die Seite **Netzwerk-Assets** wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Assets, die Sie scannen möchten.

3. Klicken Sie in der oberen rechten Ecke auf **Aktionen** > **Nessus-Scan**.

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

4. Klicken Sie auf **Mit Scan fortfahren**.

   OT Security führt den Nessus-Scan aus.

Erneute Synchronisierung durchführen

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 oder nur bestimmte Abfragen ausführen.

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** auf der Seite **Assets** > **Controller und Module** angezeigt.
- **Identifizierungsabfrage** – Verwendet mehrere Protokolle, um 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. **Läuft**, **Angehalten**, **Fehler**, **Unbekannt** und **Test**).
- **ARP** – Ruft die MAC-Adresse neuer IP-Adressen ab, die im Netzwerk erkannt wurden. Das Ergebnis wird im Abschnitt **Details** > **Übersicht** angezeigt.

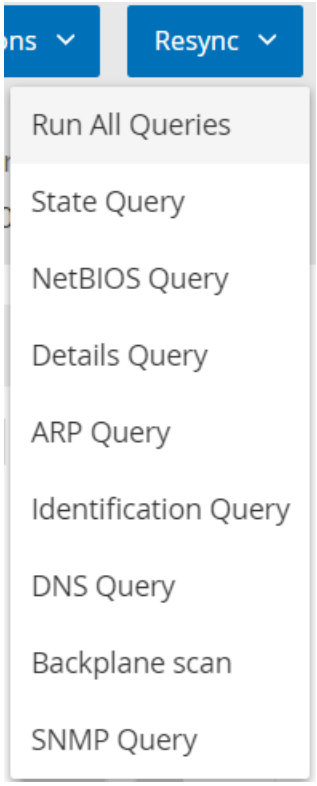
Die Schaltfläche **Erneut synchronisieren** kann unter bestimmten Bedingungen deaktiviert sein. Mögliche Gründe sind:

- Das Gerät ist nicht erreichbar oder es sind keine Abfragen verfügbar.
- Die auf der Seite **Aktive Abfragen** konfigurierte Berechtigung kann Konten ohne Administratorrechte daran hindern, bestimmte Abfragen zu initiieren.
- Abfragen sind für diese OT Security-Bereitstellung nicht aktiviert.
- Alle Abfragen im Abschnitt **Aktive Abfragen** > **Manuell** sind deaktiviert.
- Dem Asset fehlt eine bekannte IP-Adresse zum Abfragen.

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

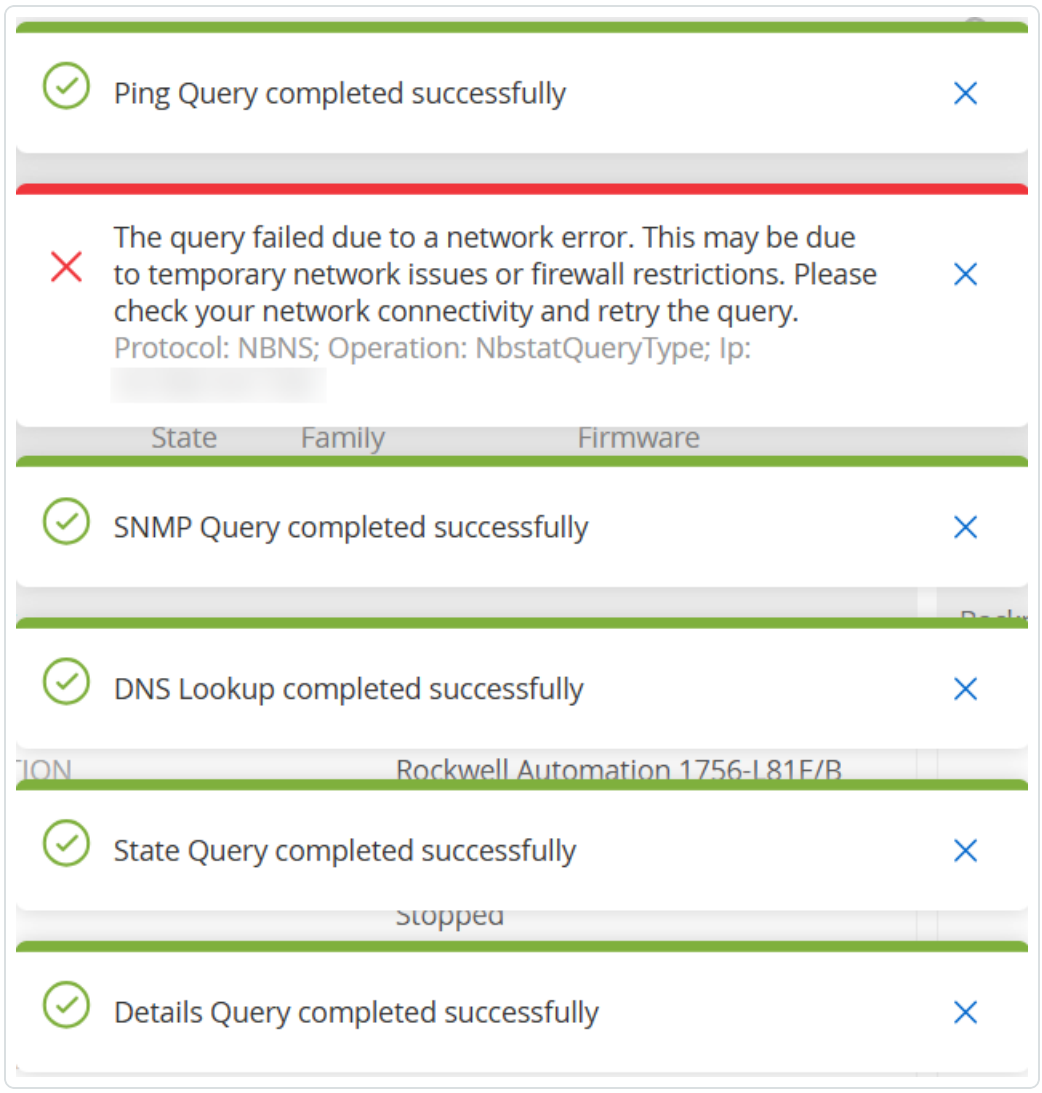
1. Klicken Sie auf der Seite **Asset-Details** für das gewünschte Asset in der oberen rechten Ecke auf **Erneut synchronisieren**.

   Eine Dropdown-Liste mit Abfragen wird angezeigt.



2. Klicken Sie auf die Abfrage, die Sie ausführen möchten, oder klicken Sie auf **Alle Abfragen ausführen**, um alle verfügbaren Abfragen auszuführen.

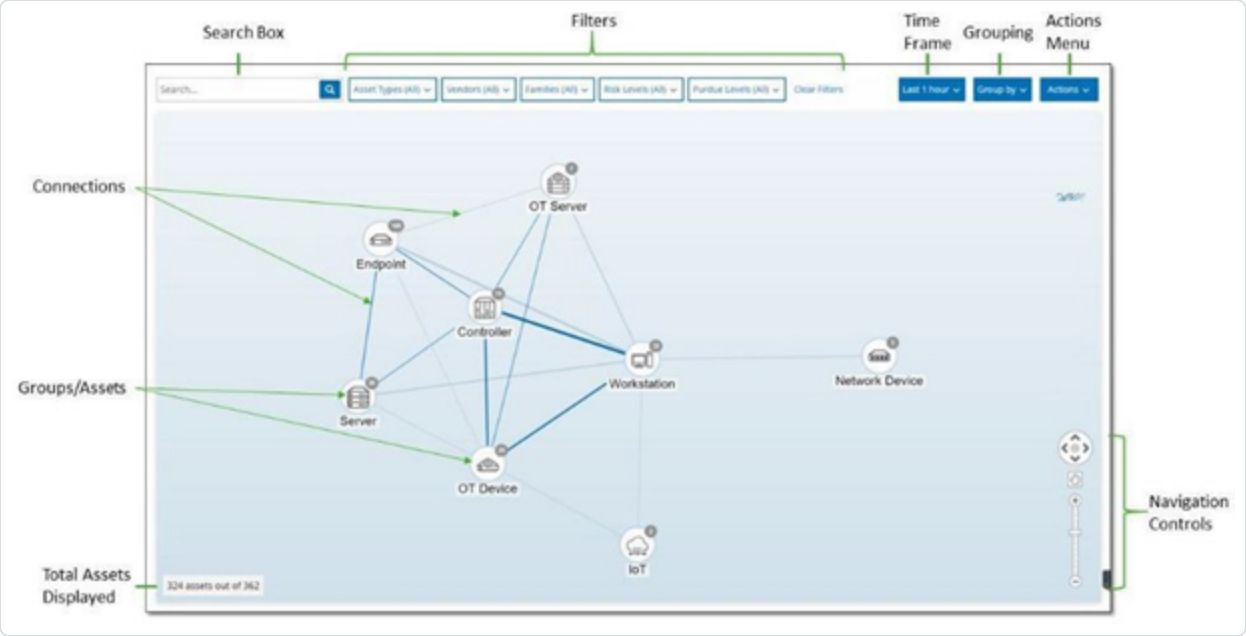
   Während die einzelnen Abfragen ausgeführt werden, wird eine Benachrichtigung mit dem Status der Abfrage angezeigt.



Für jede abgeschlossene Abfrage aktualisiert OT Security die Systemdaten für dieses Asset basierend auf den neuen Daten.

Netzwerkübersicht

Der Bildschirm **Netzwerkübersicht** bietet eine visuelle Darstellung der Netzwerk-Assets und ihrer Verbindungen im zeitlichen Verlauf, die von den Netzwerkerkennungsfunktionen von OT Security erfasst wurden. Die Netzwerkerkennung bietet detaillierte Echtzeit-Einblicke in alle Aktivitäten im Betriebsnetzwerk und konzentriert sich auf Engineering-Aktivitäten auf der Steuerungsebene wie z. B. Firmware-Downloads oder -Uploads, Code-Updates und Konfigurationsänderungen, die über proprietäre und anbieterspezifische Protokolle durchgeführt werden. Die Netzwerkübersicht zeigt die Assets nach Gruppen von verwandten Assets oder als einzelne Assets.



In der **Netzwerkübersicht** werden alle Assets und Verbindungen angezeigt, die während des angegebenen Zeitraums von Tenable erfasst wurden.

Die Seite **Netzwerkübersicht** enthält die folgenden Details:

- **Suchfeld** – Geben Sie einen Suchtext ein, um in der Anzeige nach Assets zu suchen. In der Netzwerkübersicht werden die Suchergebnisse durch Hervorheben aller Gruppen angezeigt, die mit dem Suchtext übereinstimmen. Sie können jede Gruppe aufschlüsseln, um die relevanten Assets anzuzeigen.
- **Filter** – Filtern Sie die Übersicht nach einer oder mehreren der angegebenen Kategorien: **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 **Letzte 30 Tage** festlegt. Wählen Sie im Dropdown-Feld „Zeitraum“ einen anderen Zeitraum aus.
- **Gruppierung** – Geben Sie die Kategorie an, 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 Netzwerk-Baseline festlegen.
  - **Automatisch anordnen** – Hiermit können Sie die Übersicht automatisch für die aktuell angezeigten Entitäten optimieren.
- **Gruppen/ Assets** – Die Übersicht enthält ein Symbol für jede Gruppe von Assets, wobei jeder Asset-Typ durch ein eindeutiges Symbol darstellt 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).

  > **Hinweis**: 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 aktuell 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

Auf der Seite **Netzwerkübersicht** können Assets nach verschiedenen Kategorien gruppiert angezeigt werden. Es werden Verbindungen zwischen Gruppen von Assets angezeigt. Sie können auf ein Asset klicken, um die Gruppe aufzuschlüsseln und die darin enthaltenen Elemente anzuzeigen. Sie können auch mehrere Gruppen gleichzeitig aufschlüsseln. OT Security bietet mehrere Ebenen eingebetteter Gruppen, sodass Sie bei jeder Aufschlüsselung eine detailliertere Ansicht der enthaltenen Assets erhalten.

Im Folgenden sind die Gruppierungen aufgeführt, die Sie auf die Hauptanzeige anwenden können, sowie die Aufschlüsselungsoptionen für die jeweilige Auswahl.

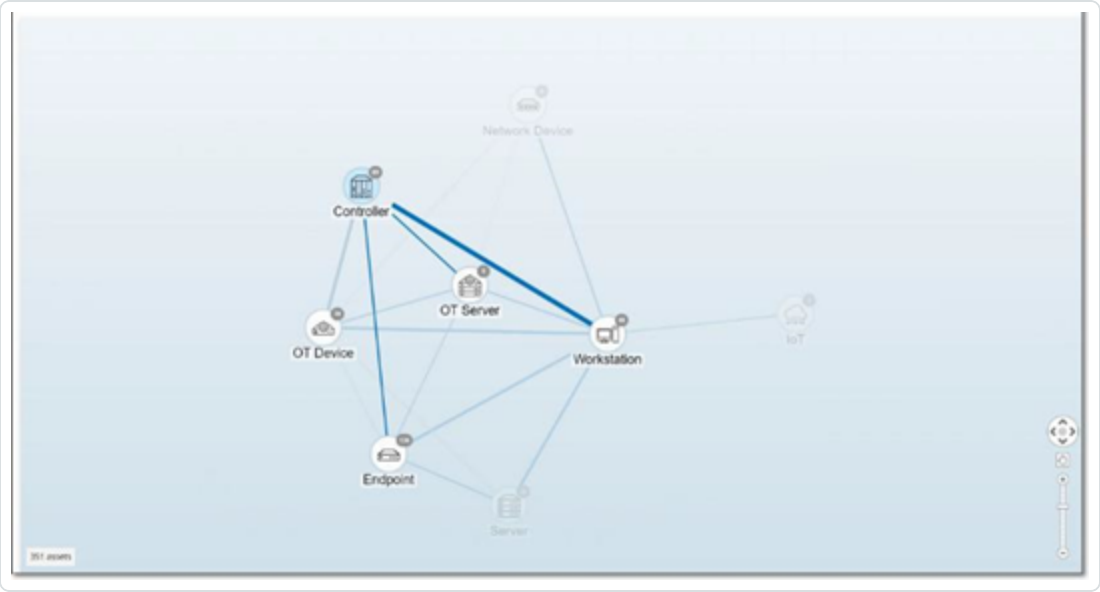
Wenn die Übersicht nach **Asset-Typ** (Standardeinstellung) gruppiert ist, sieht die Aufschlüsselungshierarchie wie folgt aus: **Asset-Typ** > **Anbieter** > **Familie** > **Einzelnes Asset**.

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**. Die enthaltenen Gruppen/Assets sind von einem Kreis umgeben, der jeweils eine einzelne Ebene darstellt.

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

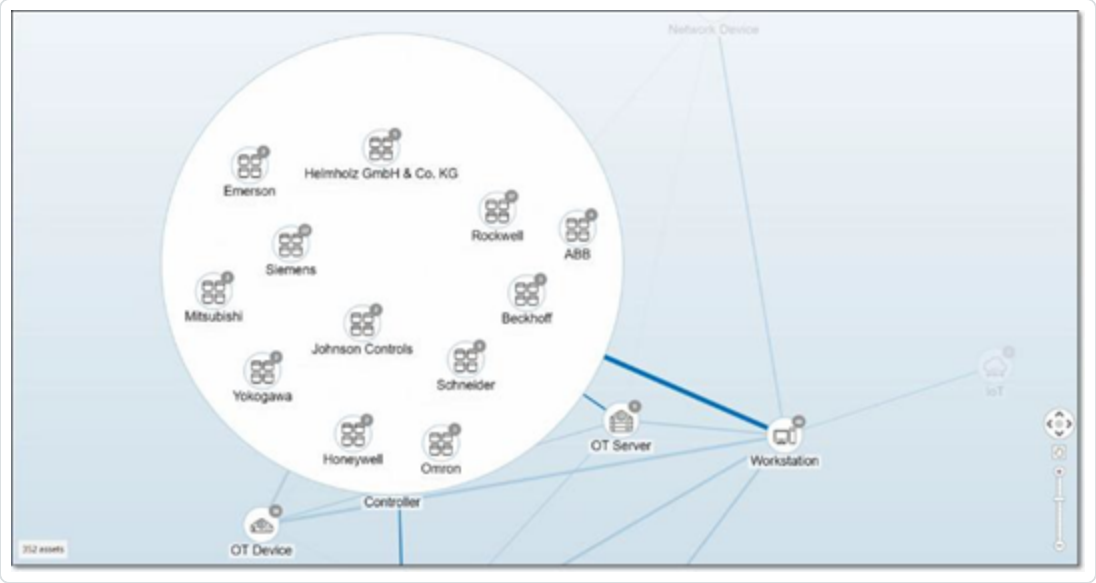
So schlüsseln Sie eine Asset-Typ-Gruppe auf:

1. Standardmäßig wird der Bildschirm **Netzwerkübersicht** mit nach Asset-Typ gruppierten Assets geöffnet.

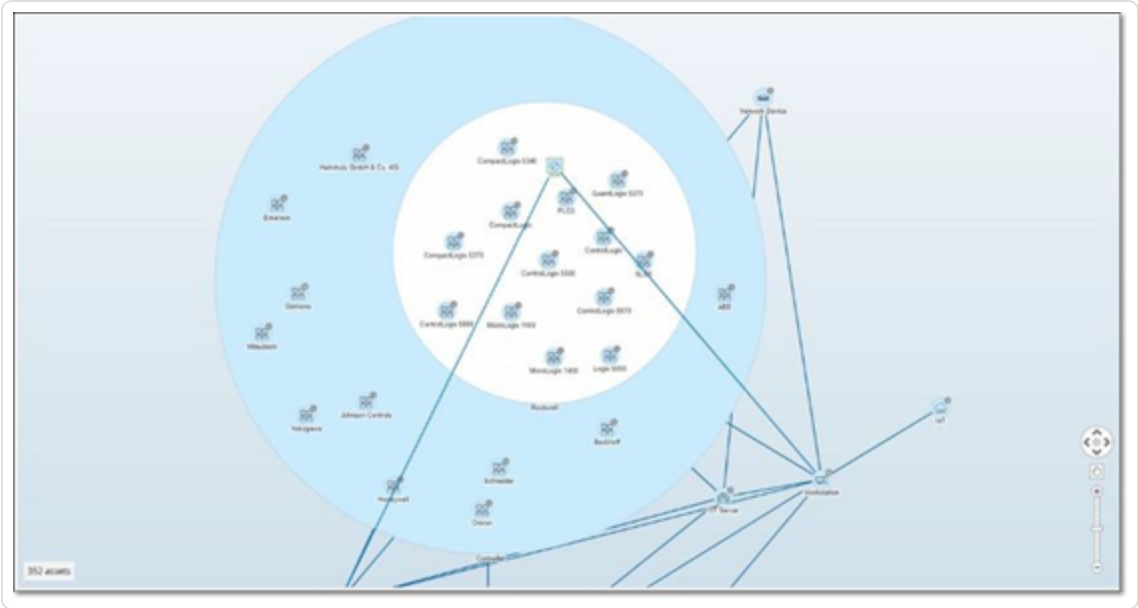


2. Doppelklicken Sie auf das Symbol der Gruppe, die Sie aufschlüsseln möchten (z. B. „Controller“).

   Die Gruppe wird erweitert und zeigt die Gruppen der Anbieter innerhalb dieser Gruppe an.

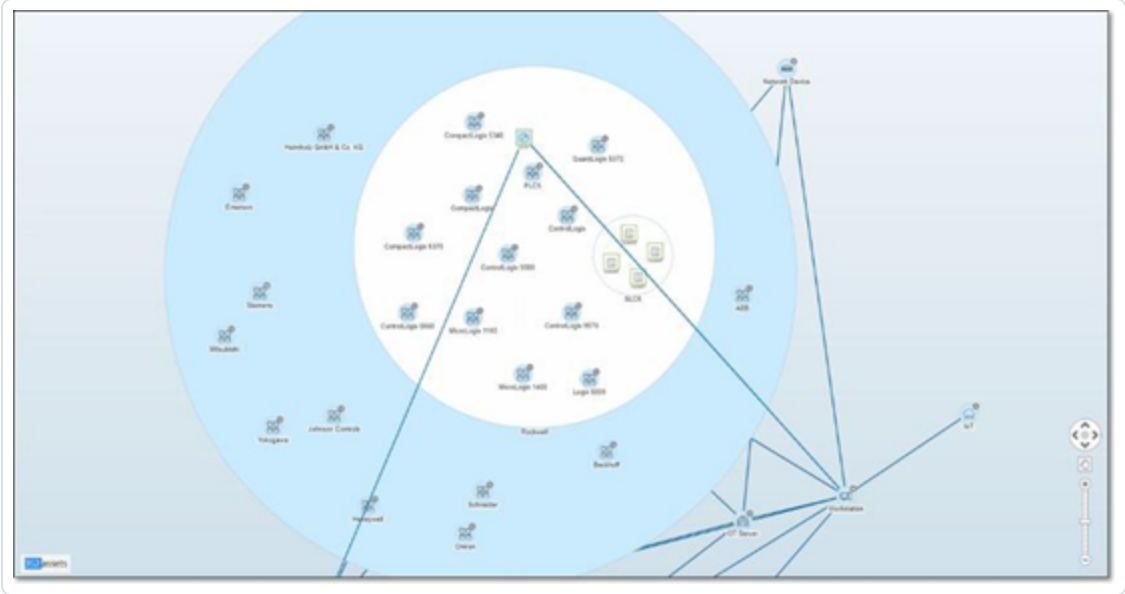


3. Zur weiteren Aufschlüsselung klicken Sie auf eine Anbietergruppe (z. B. Rockwell).



4. Um noch weiter aufzuschlüsseln, klicken Sie auf eine Familiengruppe (z. B. SLC5).

   Die einzelnen Assets innerhalb dieser Gruppe werden angezeigt.



5. Sie können jetzt auf ein bestimmtes Asset klicken, um Details für dieses Asset und seine Verbindungen anzuzeigen, siehe Inventar.

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.

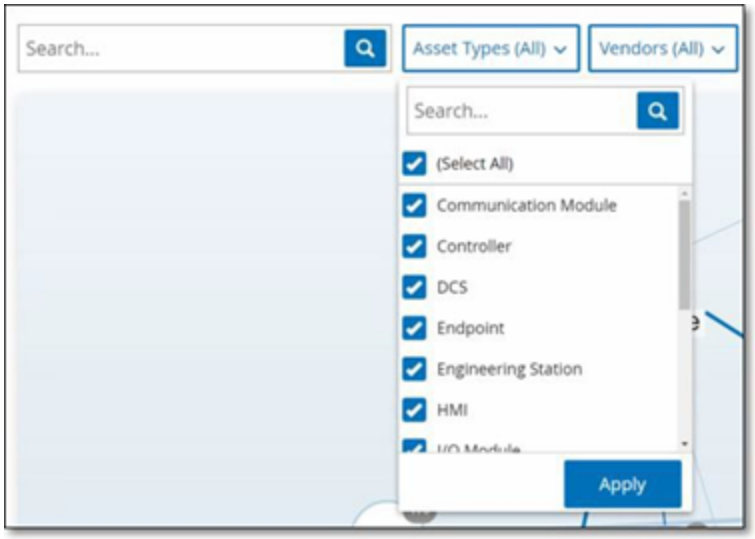
So entfernen Sie jegliche Gruppierung:

1. Klicken Sie auf die Schaltfläche **Gruppieren nach**.
2. Wählen Sie **Keine Gruppierung** aus.

   In der Übersicht werden alle einzelnen Assets ohne Gruppierung angezeigt.

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 oder deaktivieren Sie die Kontrollkästchen für jedes Element, das Sie in die Anzeige einschließen bzw. aus der Anzeige ausschließen möchten.

   Hinweis: 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**.

   In der Übersicht werden nur die ausgewählten Elemente angezeigt.

Anzeigen von Asset-Details

Sie können auf ein bestimmtes Asset klicken, 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 als Link fungierenden Asset-Namen klicken, um zum Bildschirm **Asset-Details** mit detaillierteren Informationen über das Asset zu gelangen.

Netzwerk-Baseline festlegen

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.

Assets, die während der Baseline-Stichprobe nicht interagiert haben, lösen eine Richtlinienwarnung für jede Konversation aus (in der Annahme, dass sie im Geltungsbereich der angegebenen Richtlinienbedingungen liegt). Damit Richtlinien vom Typ „Netzwerk-Baseline-Abweichung“ erstellt werden können, müssen Sie zuerst eine anfängliche Netzwerk-Baseline im Bildschirm **Netzwerkübersicht** erstellen. Sie können die Netzwerk-Baseline jederzeit durch Festlegen einer neuen Netzwerk-Baseline aktualisieren.

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 in die Netzwerk-Baseline aufgenommen werden sollen.

   Die **Netzwerkübersicht** für den ausgewählten Zeitraum wird angezeigt.

2. Wählen Sie in der oberen rechten Ecke **Aktionen** > **Als Baseline festlegen** aus.

   OT Security konfiguriert die neue Netzwerk-Baseline und wendet sie auf alle Richtlinien vom Typ „Netzwerk-Baseline-Abweichung“ an.

Schwachstellen

OT Security 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 Programme, mit denen Tenable Nessus diese Schwachstellen erkennen kann.

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

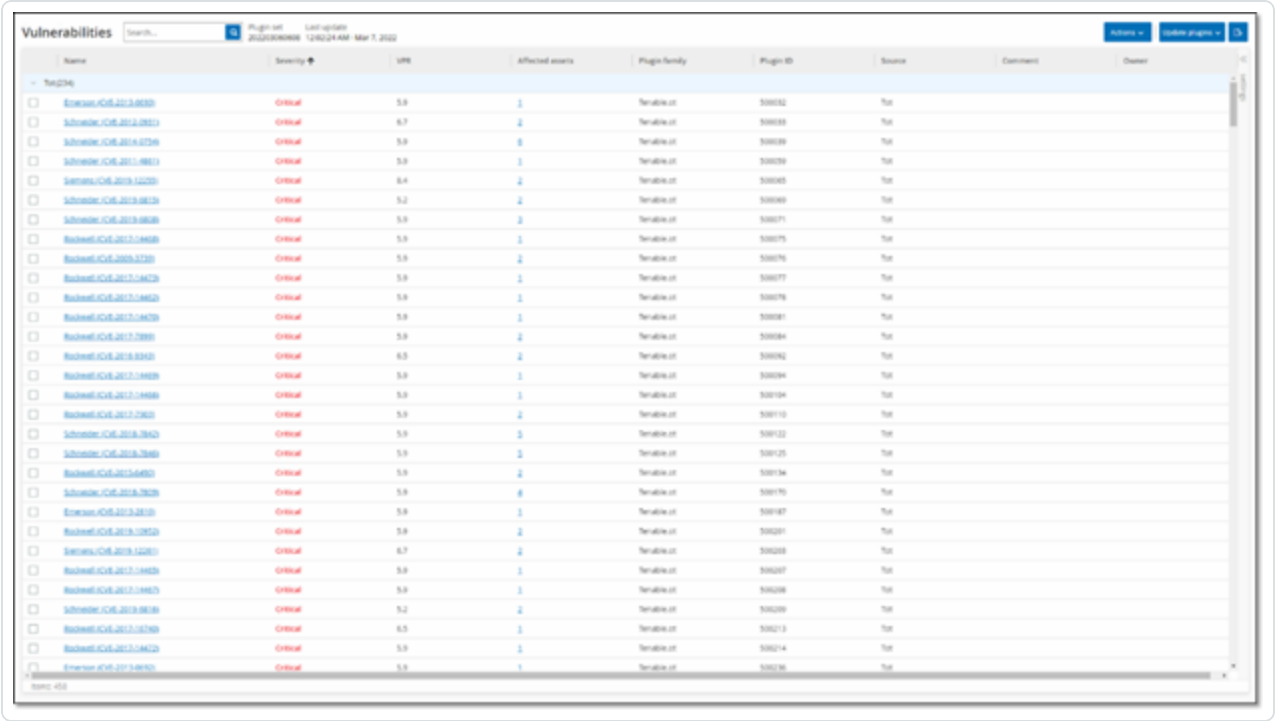
Plugins enthalten Schwachstelleninformationen, einen generischen Satz von Behebungsmaßnahmen sowie den Algorithmus, mit dem auf das Vorhandensein des Sicherheitsproblems getestet wird.

Informationen zum Aktualisieren Ihres Plugin-Satzes finden Sie unter Umgebungs.

Schwachstellen

Die Seite **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 Elemente in der Benutzeroberfläche der Verwaltungskonsole.



Auf der Seite **Schwachstellen** werden die folgenden Details angezeigt:

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, Hoch oder Kritisch.
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 Ausgabe 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

So zeigen Sie die Plugin-Details an:

1. Klicken Sie in der Zeile der Schwachstelle, für die Sie Details anzeigen möchten, auf den Namen der Schwachstelle.

Das Fenster mit Schwachstellendetails wird angezeigt.

Hier finden Sie die folgenden Informationen:

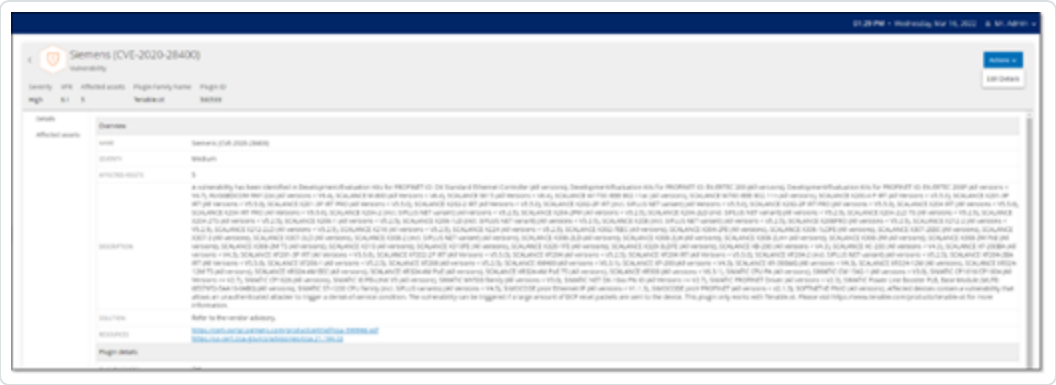
- **Kopfleiste** – Enthält grundlegende Informationen zur angegebenen Schwachstelle. Um Schwachstellendetails zu bearbeiten, wählen Sie im Menü **Aktionen** die Option **Details bearbeiten** aus. Siehe Schwachstellendetails bearbeiten.
- **Registerkarte „Details“** – Zeigt die vollständige Beschreibung der Schwachstelle und enthält Links zu relevanten Ressourcen.
- **Registerkarte „Betroffene Assets“** – Zeigt eine Liste aller Assets, 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.

Schwachstellendetails bearbeiten

So bearbeiten Sie Schwachstellendetails:

1. Klicken Sie auf der relevanten Seite mit **Schwachstellendetails** in der oberen rechten Ecke auf die Schaltfläche **Aktionen**.

   Das Menü **Aktionen** wird geöffnet.



2. Klicken Sie auf **Details bearbeiten**.

   Der Bereich **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**.

Plugin-Ausgabe anzeigen

Die Plugin-Ausgabe für ein Asset liefert Kontext oder eine Erklärung, warum ein bestimmtes Plugin für ein Asset aufgeführt wird.

So zeigen Sie die Plugin-Ausgabedetails über die Seite „Schwachstellen“ an:

1. Gehen Sie zu **Schwachstellen**.

   Die Seite **Schwachstellen** wird angezeigt.

2. Wählen Sie in der Liste der Schwachstellen die Schwachstelle aus, für die Sie Details anzeigen möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf den Schwachstellen-Link.
   - Klicken Sie mit der rechten Maustaste auf die Schwachstelle und wählen Sie **Anzeigen** aus.
   - Wählen Sie im Dropdown-Feld **Aktionen** die Option **Anzeigen** aus.

   Die Seite mit Schwachstellendetails wird angezeigt. Im Bereich **Plugin-Ausgabe** finden Sie die folgenden Informationen:

   - Trefferdatum
   - Quelle
   - Port
   - Plugin-Ausgabe

     > **Hinweis**: Plugin-Ausgabe ist nicht für alle Plugins verfügbar.

So zeigen Sie die Plugin-Ausgabedetails über die Seite „Inventar“ an:

1. Gehen Sie zu **Inventar** > **Alle Assets**.

   Die Seite **Inventar** wird angezeigt.

2. Wählen Sie in der Liste der Assets das Asset aus, für das Sie Details anzeigen möchten, und führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf den Asset-Link.
- Klicken Sie mit der rechten Maustaste auf das Asset und wählen Sie **Anzeigen** aus.
- Aktivieren Sie das Kontrollkästchen neben dem Asset und wählen Sie dann im Dropdown-Feld **Aktionen** die Option **Anzeigen** aus.

Die Seite mit Asset-Details wird geöffnet.

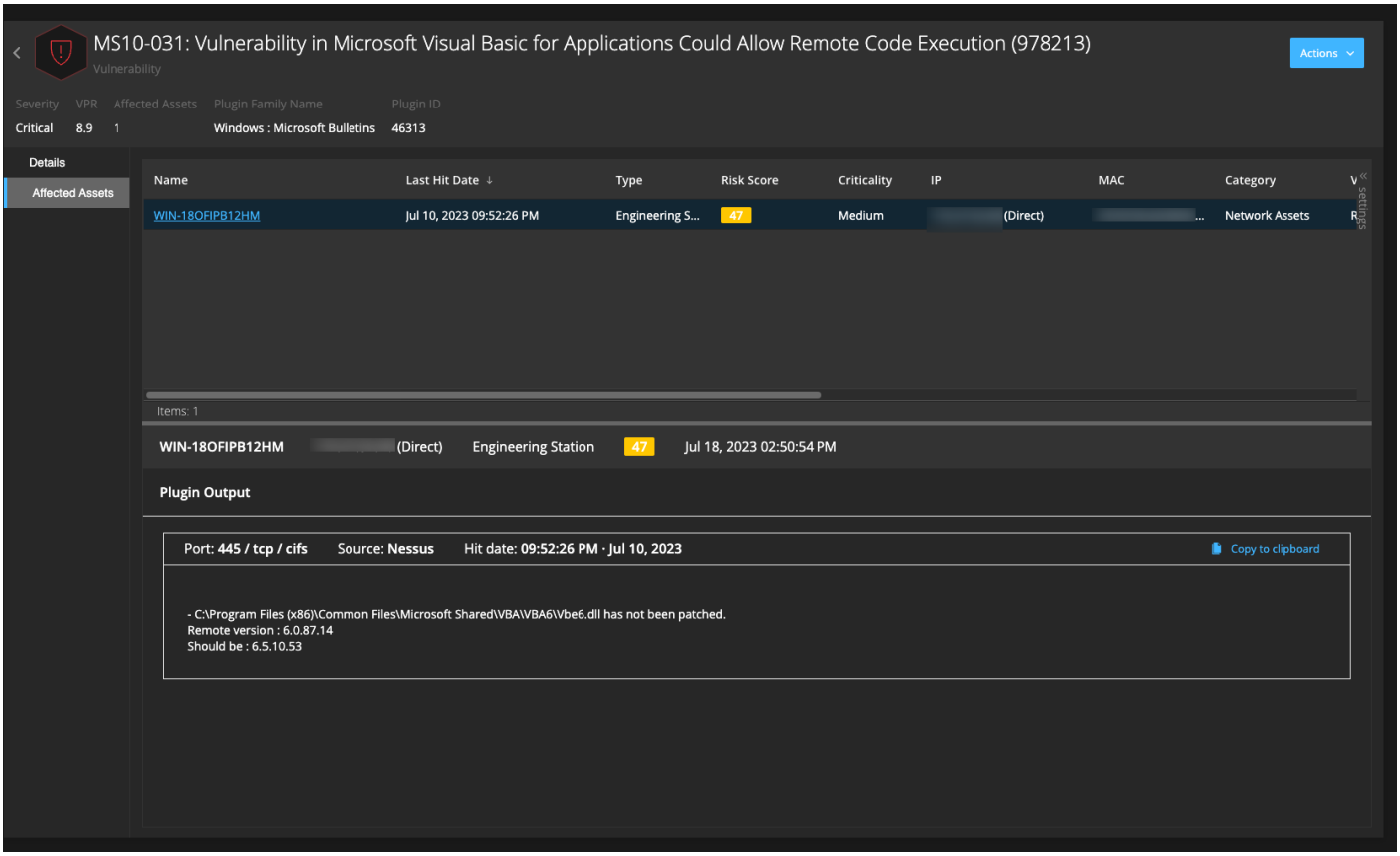
3. Klicken Sie auf die Registerkarte **Schwachstellen**.

   Die Liste der Schwachstellen wird angezeigt. Im Bereich **Plugin-Ausgabe** finden Sie die folgenden Informationen:

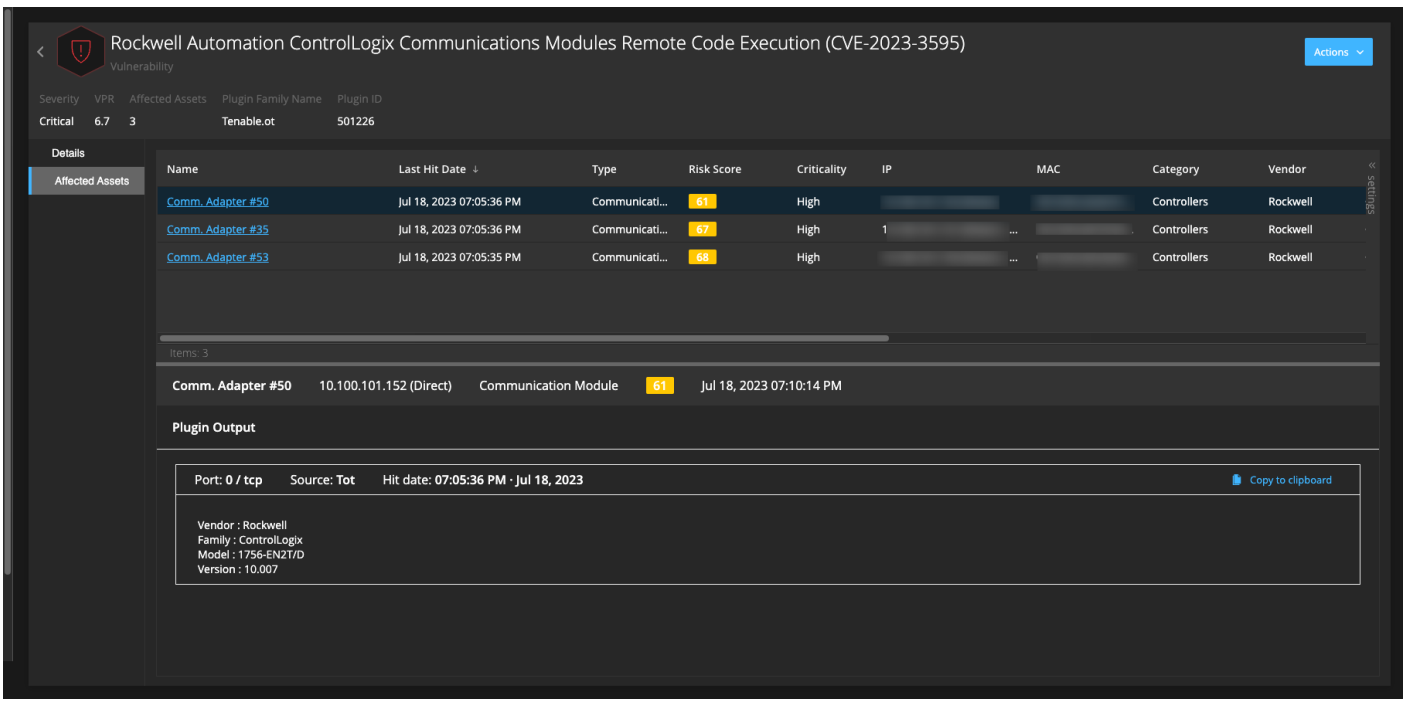
   - Trefferdatum
   - Quelle
   - Port
   - Plugin-Ausgabe

   Hinweis: Plugin-Ausgabe ist nicht für alle Plugins verfügbar.

Beispiel einer Plugin-Ausgabe für ein Tenable Nessus-Plugin



Beispiel einer Plugin-Ausgabe für ein OT Security-Plugin

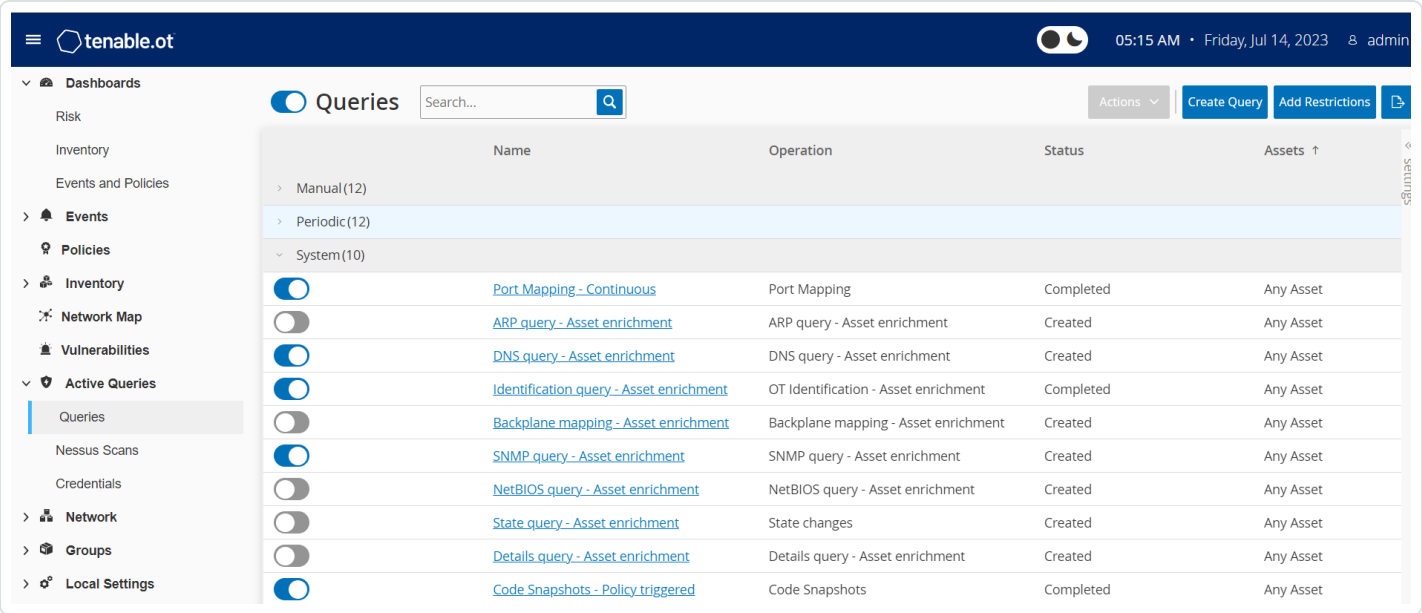


Aktive Abfragen

Im Fenster **Abfragen** von OT Security können Sie die Abfragefunktionen konfigurieren und aktivieren. Eine allgemeine Erläuterung der Abfragetechnologie finden Sie unter OT Security-Technologien. Tenable empfiehlt, die gesamte Abfragefunktionalität im Rahmen der Ersteinrichtung zu aktivieren. Sie können die einzelnen 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 besteht die Möglichkeit, Abfragen bei Bedarf zu initiieren. Klicken Sie hierzu auf den Umschalter neben der Abfrage.

Hinweis: Das Deaktivieren von Abfragen kann dazu führen, dass Assets nicht identifiziert werden. OT Security verfolgt Geräte durch passives Monitoring sowie aktive Abfragen.



Sie können Abfragen über die Seite **Aktive Abfragen** > **Abfragen** aktivieren und konfigurieren. Es gibt drei Optionen zur granularen Steuerung aktiver Abfragen: **Manuell**, **Periodisch** und **System**.

Manuell – Hiermit werden Abfragen gesteuert, die Sie ausführen können, wenn Sie ein einzelnes Asset durch Ausführen der Option **Erneut synchronisieren** für dieses Asset überprüfen. Mit manuellen Abfragen können Sie die Produktfunktionalität für bestimmte Arten von Abfragen steuern, wenn Sie ein einzelnes überwachtes Asset überprüfen. Wenn Sie die Optionen für die erneute Synchronisierung aktivieren, können Sie diese Abfragen bei der Überprüfung eines Assets

durchführen. Weitere Informationen zur Option **Erneut synchronisieren** finden Sie unter Erneute Synchronisierung durchführen.

Periodisch – Dies sind Abfragen, die in einem regelmäßigen, von Ihnen festgelegten Zeitintervall ausgeführt werden. Nach der Aktivierung wird die Abfrage gemäß dem Zeitplan ausgeführt, den Sie in der Spalte **Wird wiederholt** auf dieser Seite angegeben. Sie können alle periodischen Abfragen bei Bedarf ausführen, indem Sie mit der rechten Maustaste darauf klicken und **Jetzt ausführen** auswählen. Dies hat keine Auswirkungen auf den Zeitplan oder die Zeit, die für die nächste Abfrage festgelegt ist. Alle Abfragen, die Sie manuell erstellen, sind periodische Abfragen.

System – Dies sind Abfragen, die von OT Security automatisch basierend auf bestimmten Kriterien oder Bedingungen verarbeitet werden. Beispielsweise finden auf Asset-Anreicherung basierende Abfragen immer dann statt, wenn Tenable ein Gerät zunächst passiv oder aktiv beobachtet. Bei aktivierter Asset-Anreicherung erstellt OT Security Fingerabdrücke und identifiziert das Gerät, sobald es im Netzwerk sichtbar wird. Asset-Anreicherung steuert auch die **per Richtlinie ausgelösten Snapshots**, für die die Richtlinienkonfiguration für Controller-basierte Ereignisse gilt.

> **Hinweis**: Wenn Sie Asset-Anreicherung verwenden, stellen Sie sicher, dass die folgenden Abfragen aktiviert sind:
>
> - Port-Zuordnung – Fortlaufend
> - Identifizierungsabfrage – Asset-Anreicherung

Die Tabelle „Abfragen“ enthält die folgenden Informationen:

Spalte	Beschreibung
Umschalter zum Aktivieren oder Deaktivieren	Klicken Sie auf den Umschalter neben dem Abfragenamen, um die Abfrage zu aktivieren oder zu deaktivieren.
Name	Name der Abfrage
Vorgang	Der Abfragetyp: Erfassung, Periodisch oder System
Status	Der Status der Abfrage: **Erstellt**, **Laufend**, **Wird vorbereitet**, **Abgeschlossen** und **Fehlgeschlagen**
Assets	Die Asset-Gruppen, die von dieser Abfrage abgefragt werden müssen

	Hinweis: Sie können Ihre eigenen Asset-Gruppen erstellen, um sie in den von Ihnen konfigurierten Abfragen zu verwenden.

Abfrage erstellen

Sie können Abfragen für verschiedene Projekte und Funktionen erstellen, um zu steuern, welche Abfrage wann ausgeführt wird.

Sie können beispielsweise benutzerdefinierte Abfragen für die folgenden Szenarien konfigurieren:

- Unterschiedliche Wartungszeiten für verschiedene Teile der Anlage
- Unterschiedliche Projekte und Kritikalität für verschiedene Assets
- Unterschiedliche Abfragen für OT-Funktionen und IT-Funktionen

So erstellen Sie eine Abfrage:

1. Gehen Sie zu **Aktive Abfragen** > **Abfragen**.

   Das Fenster **Abfragen** wird angezeigt.

2. Klicken Sie auf **Abfrage erstellen**.

   Der Bereich **Abfrage erstellen** wird angezeigt.

3. Wählen Sie den gewünschten Abfragetyp unter der folgenden Optionen aus:

   - **Erfassung** – Dies sind Abfragen, die Live-Assets in dem von OT Security überwachten Netzwerk erkennen.

     - Bei der **Asset-Erfassung** wird das Internet Control Message Protocol (ICMP) oder Ping verwendet, um IP-Adressen zu erkennen, die live sind und antworten.
     - Bei der **aktiven Asset-Verfolgung** wird regelmäßig versucht, ein bekanntes, überwachtes Asset anzupingen, um sicherzustellen, dass es noch aktiv und verfügbar ist.
     - Bei der **Controller-Erfassung** wird eine Reihe von Multicast-Paketen an das

Netzwerk gesendet, um Controller oder ICS-Geräte zu veranlassen, ihre Informationen direkt an OT Security zu senden.

- **IT** – Mit diesen Abfragen können zusätzliche Datenpunkte von überwachten IT-Assets abgerufen werden, die von OT Security beobachtet wurden. Mit Ausnahme von NetBIOS erfordern diese IT-Abfragen Zugangsdaten.
    - Die **NetBIOS-Abfrage** versucht, alle Geräte zu erkennen, die im Broadcast-Bereich von OT Security Sensor oder OT Security selbst auf NetBIOS lauschen. Dieser Abfragetyp ist geeignet, um Windows-Geräte in der Nähe zu identifizieren.
    - Die **SNMP-Abfrage** verwendet SNMP V2- oder SNMP V3-Zugangsdaten, um Identifizierungsdetails von der Netzwerkinfrastruktur oder vernetzten Geräten anzufordern, die SNMP unterstützen. OT Security fragt die SNMP-Systembeschreibung und andere Parameter ab, um Asset-Kontext bereitzustellen und Fingerprinting zu unterstützen.
    - Die **WMI-Detailabfrage** ruft eine Vielzahl wichtiger Datenpunkte aus Windows-basierten Systemen ab. Dazu muss das abgefragte System über ein Windows-Konto (lokal oder Domäne) mit ausreichenden Berechtigungen verfügen, um den WMI-Dienst (Windows-Verwaltungsinstrumentation) abzufragen.
    - **WMI-USB-Statusabfragen** ermitteln, ob Wechseldatenträger wie USB-Laufwerke oder tragbare Festplatten an das Windows-Gerät angeschlossen sind, z. B. eine Engineering-Workstation oder ein Engineering-Server. Diese Abfrage ist eng mit der Richtlinie **Änderung der USB-Konfiguration auf Windows-Computern** verbunden, da sie eine Voraussetzung für die ordnungsgemäße Funktion dieser Richtlinie ist.
- **OT** – Diese Abfragen wurden entwickelt, um Controller und eingebettete Geräte auf sichere Weise unter Verwendung ihrer proprietären Protokolle nach weiteren Informationen abzufragen. OT Security führt schreibgeschützte Abfragen durch, um Geräteinformationen zu sammeln. In einigen Fällen fragt OT Security mehr als nur Details zur Geräteidentifizierung ab und kann Informationen wie z. B. den SPS-Ausführungsstatus oder andere an die Backplane angeschlossene Module anzeigen. OT Security versucht, Geräte abzufragen, die auf proprietäre Protokollen lauschen, die

von OT Security unterstützt werden.

4. Klicken Sie auf **Weiter**.

   Der Bereich **Abfragedefinition** wird angezeigt.

5. Geben Sie im Feld **Name** einen Namen für die Abfrage ein.
6. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Abfrage ein.
7. Wählen Sie im Dropdown-Feld **Assets** die Assets aus.

   Hinweis: Sie können auch das **Suchfeld** verwenden, um nach einem bestimmten Asset zu suchen.

8. Geben Sie im Abschnitt **Wiederholung alle** eine Zahl ein und wählen Sie **Tage** oder **Wochen** im Dropdown-Feld aus. Für bestimmte Abfragen können Sie auch **Minuten** und **Stunden** festlegen.

   Wenn Sie **Wochen** auswählen, geben Sie die Wochentage an, an denen die Abfragen ausgeführt werden sollen.

9. Legen Sie im Feld **Um** die Tageszeit fest, zu der die Abfragen ausgeführt werden sollen (im Format HH:MM:SS). Klicken Sie hierzu auf das Uhrsymbol und wählen Sie die Uhrzeit aus oder geben Sie die Uhrzeit manuell ein.
10. Klicken Sie auf den Umschalter **Abfragestatus**, um die Abfrage zu aktivieren.
11. (Nur für Asset-Erfassung) Geben Sie im Feld **IP-Bereiche** die IP-Adressen der Assets ein.
12. (Nur für Erfassungsabfragen) Wählen Sie im Dropdown-Feld **Anzahl an Assets, die gleichzeitig abgefragt werden** die Anzahl der Assets aus. Verfügbare Optionen: 10 Assets, 20 Assets oder 30 Assets.
13. (Nur für Erfassungsabfragen) Wählen Sie im Dropdown-Feld **Zeit zwischen Erfassungsabfragen** die Zeit zwischen den Erfassungsabfragen aus. Verfügbare Optionen: 1 Sekunde, 2 Sekunden oder 3 Sekunden.

Einschränkungen hinzufügen

Sie können die Ausführung von Abfragen für bestimmte Assets blockieren, wie z. B. IP-Bereiche, OT-Server, Tablets, medizinische Geräte, Domänencontroller usw.

So fügen Sie Einschränkungen hinzu:

1. Gehen Sie zu **Aktive Abfragen** > **Abfragen**.

   Das Fenster **Abfragen** wird angezeigt.

2. Wählen Sie im Dropdown-Feld **Blockierte Assets** die Assets aus, die blockiert werden sollen.

   Hinweis: Sie können das Suchfeld verwenden, um nach bestimmten Assets zu suchen.

3. Wählen Sie im Dropdown-Feld **Eingeschränkte Clients** die gewünschten Clients aus.

4. Wählen Sie im Dropdown-Feld **Ausfallzeitraum** die Dauer aus, für die Sie die Assets sperren möchten. Verfügbare Optionen: **Keine**, **Arbeitszeiten** (Working Hours).

5. Klicken Sie auf **Speichern**.

   OT Security wendet die Einschränkungen für die spezifischen Clients und Assets an.

Abfrage anzeigen

So zeigen Sie die Details einer Abfrage an:

1. Gehen Sie zu **Aktive Abfragen** > **Abfragen**.

   Das Fenster **Abfragen** wird angezeigt.

2. Führen Sie in der Zeile der Abfrage, die Sie anzeigen möchten, einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie **Anzeigen** aus.
   - Wählen Sie die Abfrage und dann im Menü **Aktionen** die Option **Anzeigen** aus.

   Es wird ein Fenster mit den Details der Abfrage angezeigt.

Abfrage bearbeiten

So bearbeiten Sie die Details einer Abfrage:

1. Gehen Sie zu **Aktive Abfragen** > **Abfragen**.

   Das Fenster **Abfragen** wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die Abfrage aus, die Sie bearbeiten möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie **Bearbeiten** aus.
   - Wählen Sie die Abfrage und dann im Menü **Aktionen** die Option **Bearbeiten** aus.

   Der Bereich **Abfrage bearbeiten** wird angezeigt.

   > **Hinweis**: Sie können eine Abfrage auch über die Seite **Abfragedetails** bearbeiten.

3. Ändern Sie die Abfrage nach Bedarf.
4. Klicken Sie auf **Speichern**.

Abfrage duplizieren

> **Hinweis**: Duplizierte Abfragen können nur für **periodische** Abfragen erstellt werden.

1. Gehen Sie zu **Aktive Abfragen** > **Abfragen**.

   Das Fenster **Abfragen** wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die Abfrage aus, von der Sie eine Kopie erstellen möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie **Duplizieren** aus.
   - Wählen Sie die Abfrage und dann im Menü **Aktionen** die Option **Duplizieren** aus.

   Der Bereich **Abfrage duplizieren** mit Details der Abfrage wird angezeigt.

   > **Hinweis**: Sie können eine Abfrage auch über die Seite „Abfragedetails“ duplizieren.

3. Benennen Sie die Abfrage um und ändern Sie die Details nach Bedarf.
4. Klicken Sie auf **Speichern**.

   OT Security speichert die Abfrage in der Tabelle „Abfragen“.

Abfrage ausführen

Bei Bedarf können Sie periodische Abfragen ausführen.

Hinweis: Die Option **Jetzt ausführen** ist nur für **periodische** Abfragen verfügbar.

So führen Sie eine Abfrage aus:

1. Gehen Sie zu **Aktive Abfragen** > **Abfragen**.

   Das Fenster **Abfragen** wird angezeigt.

2. Wählen Sie in der Liste der Abfragen die Abfrage aus, die Sie ausführen möchten, und führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die Abfrage und wählen Sie **Jetzt ausführen** aus.
   - Wählen Sie die Abfrage und dann im Menü **Aktionen** die Option **Jetzt ausführen** aus.

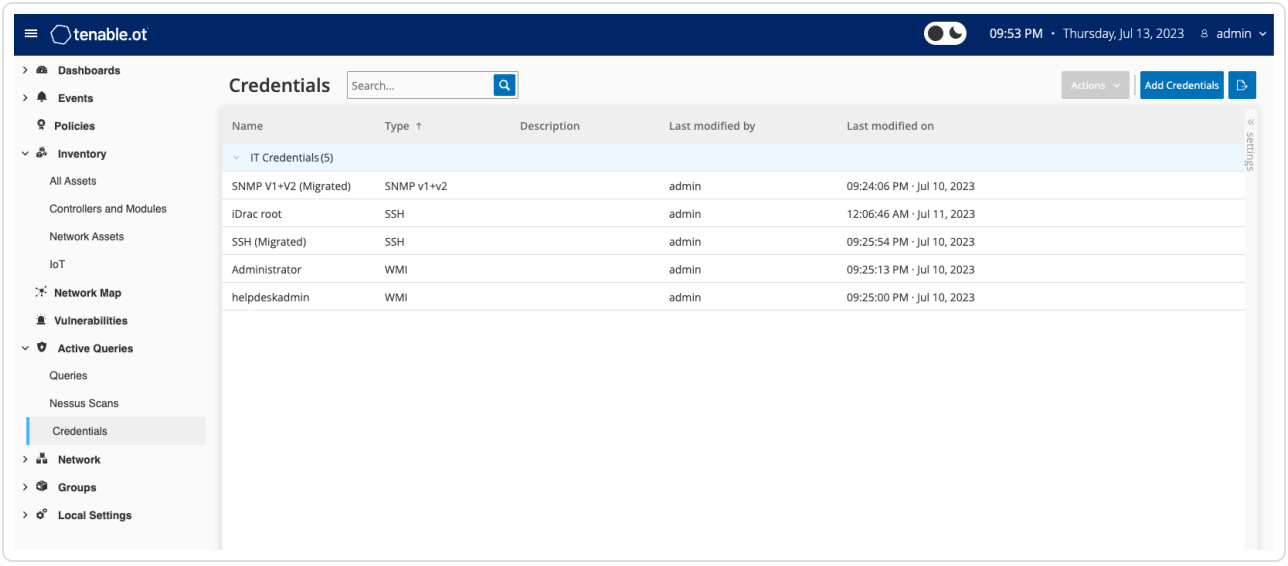
   In einer Meldung werden Sie aufgefordert, die Ausführung der Abfrage zu bestätigen.

3. Klicken Sie auf **OK**.

   OT Security führt die ausgewählte Abfrage aus.

Zugangsdaten

Verwenden Sie die Seite **Zugangsdaten**, um bei Bedarf die Zugangsdaten für das Gerät zu konfigurieren. Für die Kommunikation in ihren nativen Netzwerkprotokollen oder proprietären Protokollen benötigen Geräte keine Zugangsdaten. Für bestimmte Geräte, die von OT Security unterstützt werden, sind jedoch möglicherweise Zugangsdaten erforderlich, um die Asset-Erfassung durchzuführen.

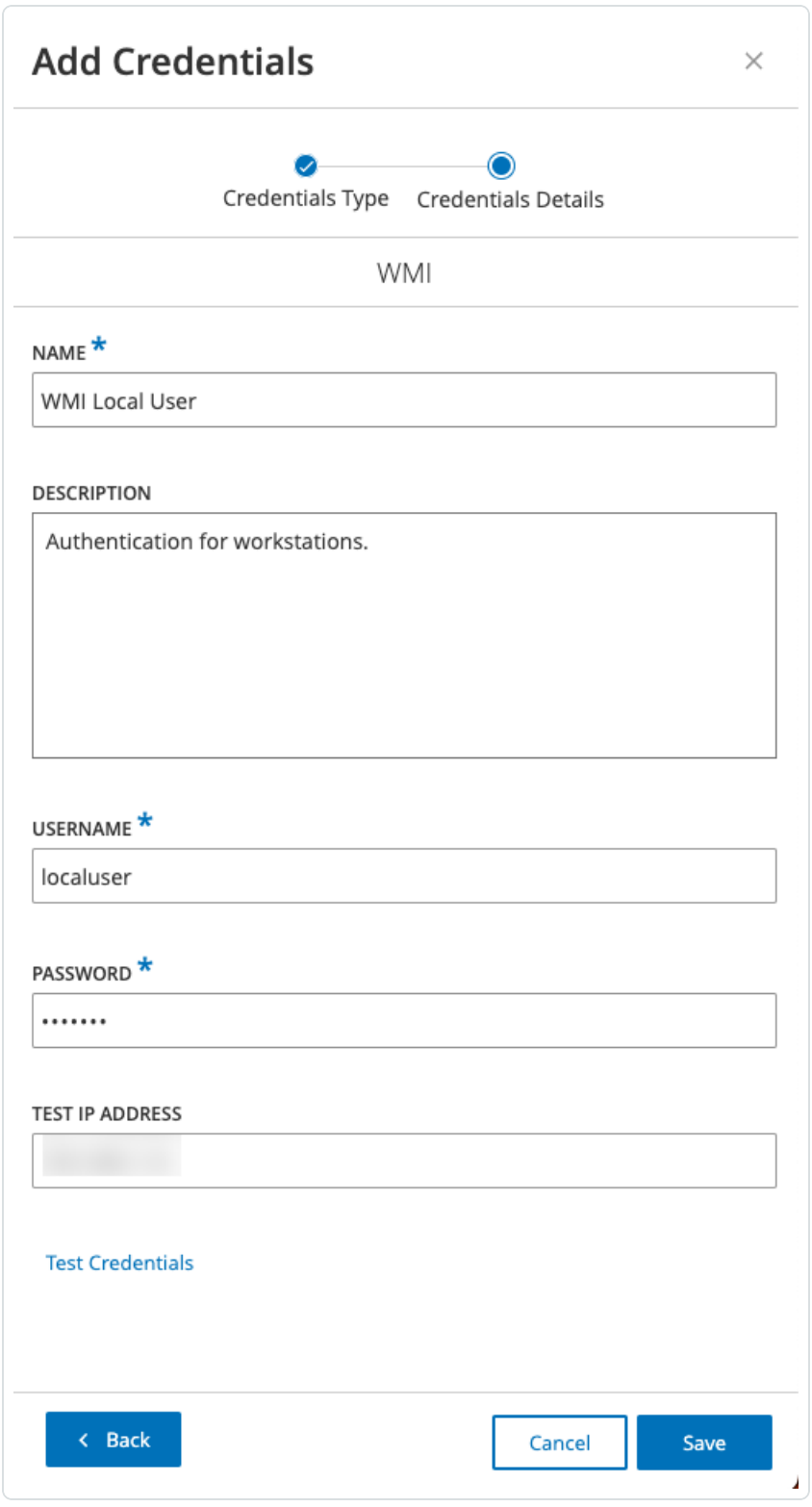


Zugangsdaten hinzufügen

So fügen Sie Zugangsdaten hinzu:

1. Klicken Sie in der oberen rechten Ecke auf **Zugangsdaten hinzufügen**.

   Der Bereich **Zugangsdaten hinzufügen** wird angezeigt.


Add Credentials
Credentials Type
Credentials Details
WMI
NAME *
WMI Local User
DESCRIPTION
Authentication for workstations.
USERNAME *
localuser
PASSWORD *
TEST IP ADDRESS
Test Credentials
Back
Cancel
Save

2. Klicken Sie im Abschnitt **Zugangsdatentyp** auf den gewünschten Gerätetyp. Verfügbare Optionen sind:

    - ABB RTU 500
    - Bachmann
    - Konzept
    - Sel
    - SicamA8000
    - SIPROTEC 5
    - SNMP v1+v2
    - SNMP v3
    - SSH
    - WMI

3. Klicken Sie auf **Weiter**.

    Der Bereich **Zugangsdatendetails** wird angezeigt.

4. Geben Sie die folgenden Details an:

    - **Name** – Ein Name für die Zugangsdaten
    - **Beschreibung** – Eine Beschreibung für die Zugangsdaten
    - **Benutzername** – Der Benutzername für das Gerät.
    - **Passwort** – Das Passwort für das Gerät.
    - **Test-IP-Adresse** – Die IP-Adresse des Geräts.

5. Klicken Sie auf **Zugangsdaten testen**, um zu überprüfen, ob OT Security das Gerät mit den Zugangsdaten erreichen kann.

6. Klicken Sie auf **Speichern**.

    Die Zugangsdaten werden in OT Security gespeichert und auf der Seite **Zugangsdaten** angezeigt.

Zugangsdaten bearbeiten

Sie können Ihre Zugangsdaten bearbeiten.

So bearbeiten Sie Zugangsdaten:

1. Führen Sie einen der folgenden Schritte aus:

    - Klicken Sie mit der rechten Maustaste auf die gewünschten Zugangsdaten und wählen Sie **Bearbeiten** aus.
    - Wählen Sie die gewünschten Zugangsdaten und dann im Menü **Aktionen** die Option **Bearbeiten** aus.

    Der Bereich **Zugangsdaten bearbeiten** wird angezeigt.

2. Ändern Sie die Details nach Bedarf.
3. Klicken Sie auf **Speichern**.

Zugangsdaten löschen

Sie können die nicht mehr benötigten Zugangsdaten löschen.

So löschen Sie Zugangsdaten:

1. Führen Sie einen der folgenden Schritte aus:

    - Klicken Sie mit der rechten Maustaste auf die gewünschten Zugangsdaten und wählen Sie **Löschen** aus.
    - Wählen Sie die gewünschten Zugangsdaten und dann im Menü **Aktionen** die Option **Löschen** aus.

    OT Security löscht die ausgewählten Zugangsdaten.

WMI-Konten

Damit OT Security WMI-Abfragen (Windows-Verwaltungsinstrumentation) durchführen kann, können Sie ein WMI-Konto einrichten. OT Security stützt sich auf WMI-Abfragen, um weitere Informationen über Windows-Systeme zu erhalten.

OT Security verwendet bei der Durchführung von WMI-Abfragen dieselben WMI-Methoden wie Tenable Nessus. Informationen zum Einrichten eines WMI-Kontos für Scans finden Sie im Abschnitt Enable Windows Logins for Local and Remote Audits (Windows-Logins für lokale und Remote-Überwachungen aktivieren) im Benutzerhandbuch zu Tenable Nessus.

Nessus-Plugin-Scans erstellen

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.

OT Security führt den Scan für reaktionsfähige Assets innerhalb der angegebenen CIDRs aus. Um Ihre OT-Geräte zu schützen, scannt OT Security jedoch nur bestätigte Netzwerk-Assets im angegebenen Bereich (Nicht-SPS). OT Security schließt Assets vom Typ **Endgerät** aus dem Scan aus.

Der Nessus-Scan in OT Security verwendet die gleichen Richtlinieneinstellungen wie ein Netzwerk-Basisscan in Tenable Nessus, Tenable Security Center und Tenable Vulnerability Management. Der einzige Unterschied sind die Leistungsoptionen in OT Security. Im Folgenden sind die Leistungsoptionen für den Nessus-Scan in OT Security aufgeführt. Diese Optionen gelten auch für den Nessus-Basisscan, den Sie über die Seite **Inventar** > **Alle Assets** starten.

- 5 Hosts gleichzeitig (max.)
- 2 gleichzeitige Prüfungen pro Host (max.)
- 15 Sekunden Zeitüberschreitung für Lesevorgänge im Netzwerk

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

Informationen zum Durchführen eines Nessus-Basisscans für ein beliebiges einzelnes Asset finden Sie unter Asset-spezifischen Tenable Nessus-Scan durchführen.

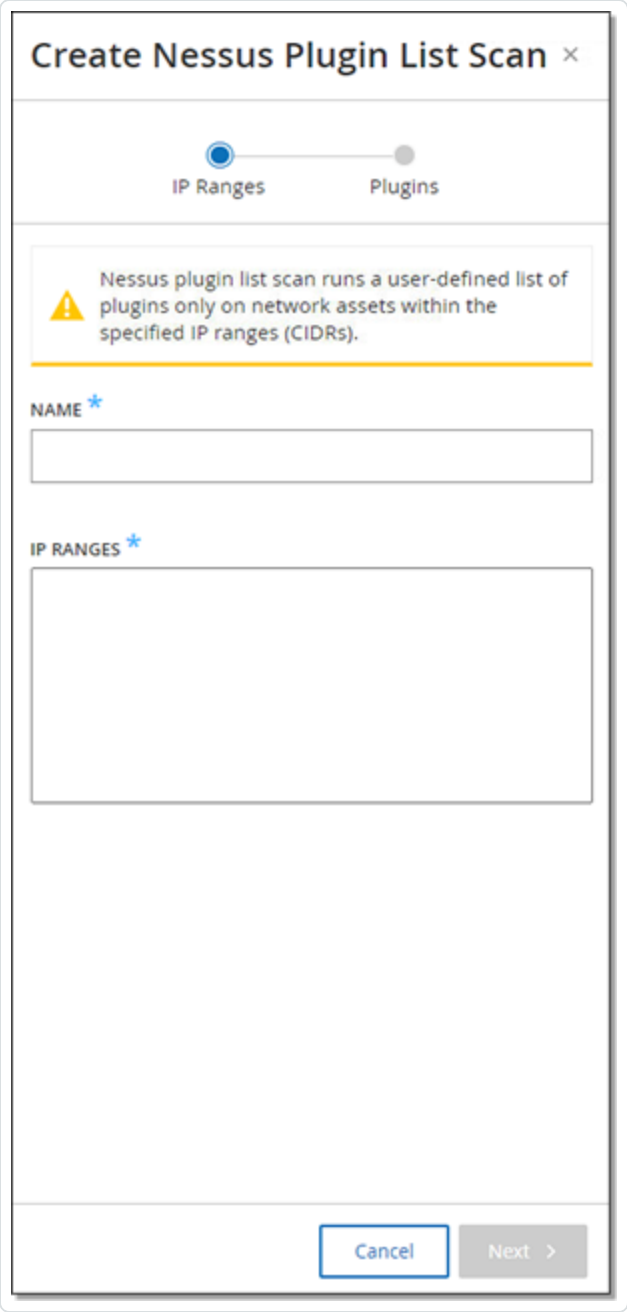
Hinweis: Sie können den Basisscan für Assets vom Typ **Endgerät** ausführen.

Einen Nessus-Plugin-Scan erstellen

So erstellen Sie einen Nessus-Plugin-Scan:

1. Gehen Sie zu **Aktive Abfragen** > **Nessus-Scans**.
2. Klicken Sie in der oberen rechten Ecke auf **Scan erstellen**.

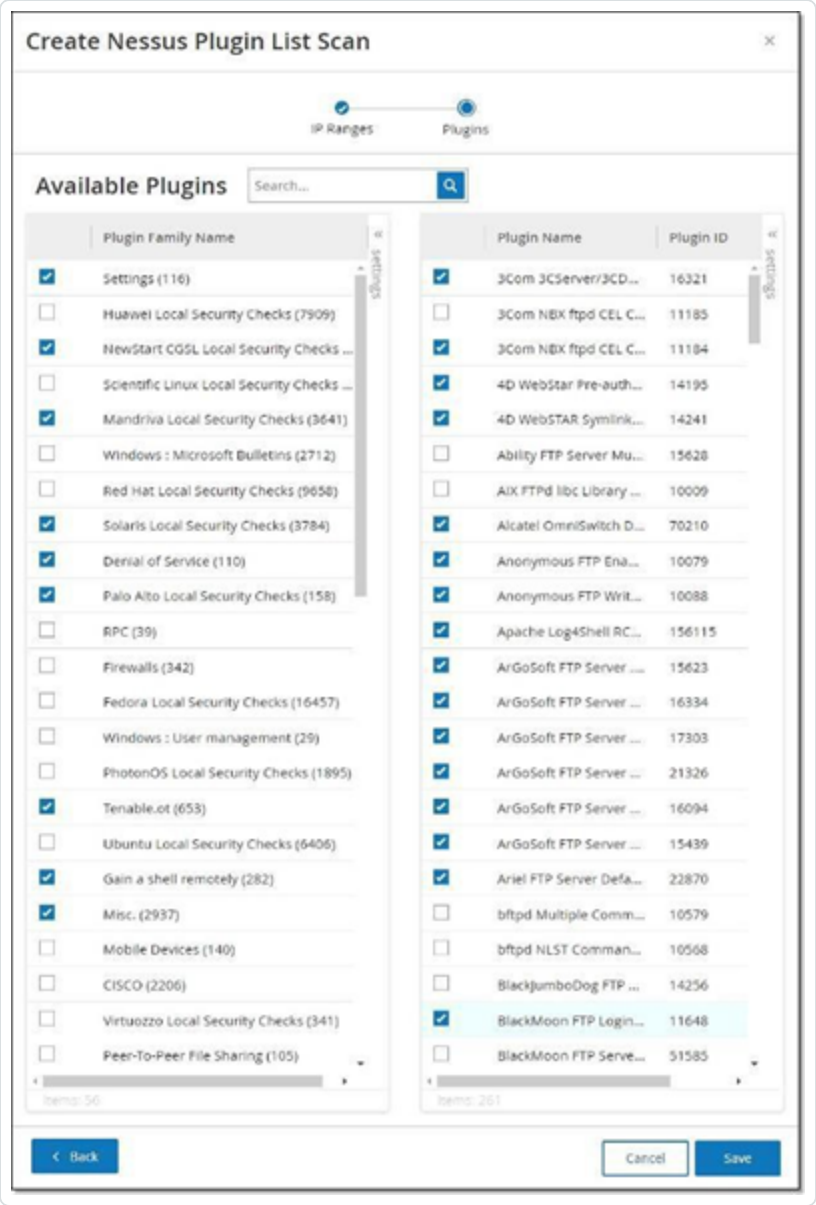
   Der Bereich **Nessus-Plugin-Listen-Scan erstellen** wird angezeigt.



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.



> **Hinweis**: OT Security listet nur die Plugins auf, die für das Gerät spezifisch sind. Sie benötigen eine aktuelle Lizenz, um neue Plugins zu erhalten. Informationen zum Aktualisieren Ihrer Lizenz finden Sie unter Die Lizenz aktualisieren.

6. Wählen Sie in der Spalte **Name der Plugin-Familie** die erforderlichen Plugin-Familien aus, die in den Scan einbezogen werden sollen. Deaktivieren Sie in der rechten Spalte nach Bedarf die

Kontrollkästchen für einzelne Plugins.

> **Hinweis**: Weitere Informationen zu Tenable Nessus-Plugin-Familien finden Sie unter https://de.tenable.com/plugins/nessus/families.

7. Klicken Sie auf **Speichern**.

   Der neue Nessus-Scan wird auf der Seite **Nessus-Scans** angezeigt.

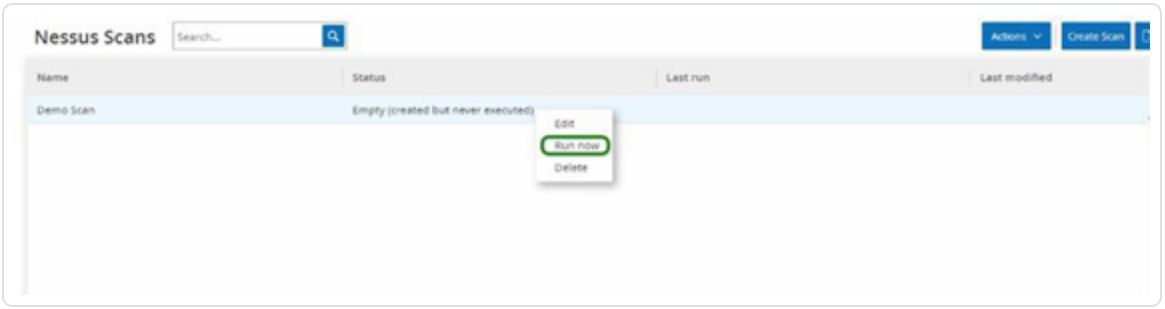
   > **Hinweis**: Um einen vorhandenen Tenable Nessus-Scan zu bearbeiten oder zu löschen, klicken Sie mit der rechten Maustaste auf den Scan und wählen Sie **Bearbeiten** oder **Löschen** aus.

Einen Nessus-Plugin-Scan ausführen

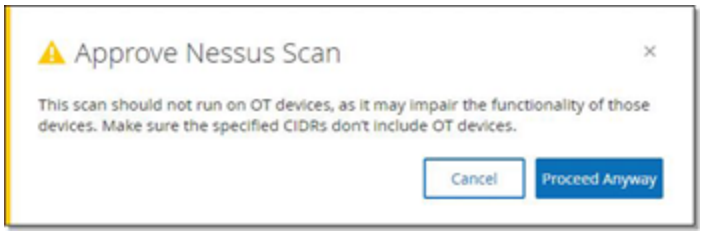
So führen Sie einen Nessus-Plugin-Scan aus:

1. Führen Sie auf der Seite **Nessus-Scans** einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf den Scan und wählen Sie **Jetzt ausführen** aus.
   - Wählen Sie den Scan aus, den Sie ausführen möchten, und klicken Sie dann auf **Aktionen** > **Jetzt ausführen**.



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



2. Wenn Sie wissen, dass keine OT-Geräte in den Scan einbezogen sind, klicken Sie auf **Trotzdem fortfahren**.

   Das Dialogfeld wird geschlossen und OT Security speichert den Scan.

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**.

   OT Security führt jetzt den Scan aus. Sie können Scans je nach aktuellem Status anhalten/fortsetzen, stoppen oder abbrechen.

Netzwerk

OT Security überwacht alle Aktivitäten in Ihrem Netzwerk und zeigt die Daten auf den folgenden Seiten an:

- **Netzwerk – Zusammenfassung** – Zeigt eine Übersicht der Netzwerkaktivität.
- **Paketerfassungen** – Zeigt eine Liste der vom System erfassten PCAP-Dateien. Siehe Paketerfassungen.
- **Konversationen** – Zeigt eine Liste aller im Netzwerk erkannten Konversationen mit Details über den Zeitpunkt, an dem sie stattgefunden haben, beteiligten Assets usw. Siehe Konversationen

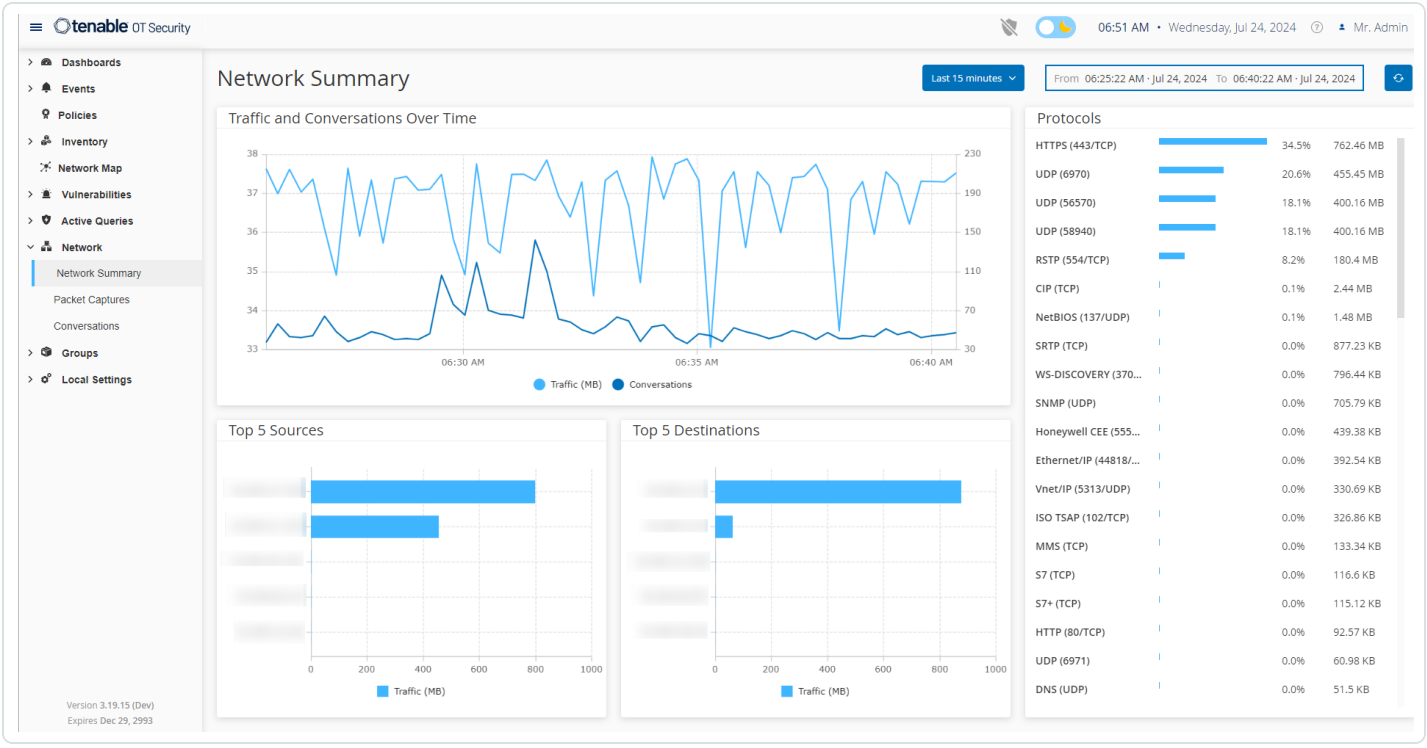
So greifen Sie auf die Seite **Netzwerk** zu:

1. Wählen Sie im linken Navigationsbereich **Netzwerk** aus.

   Die Seite **Netzwerk – Zusammenfassung** wird angezeigt.

Netzwerk – Zusammenfassung

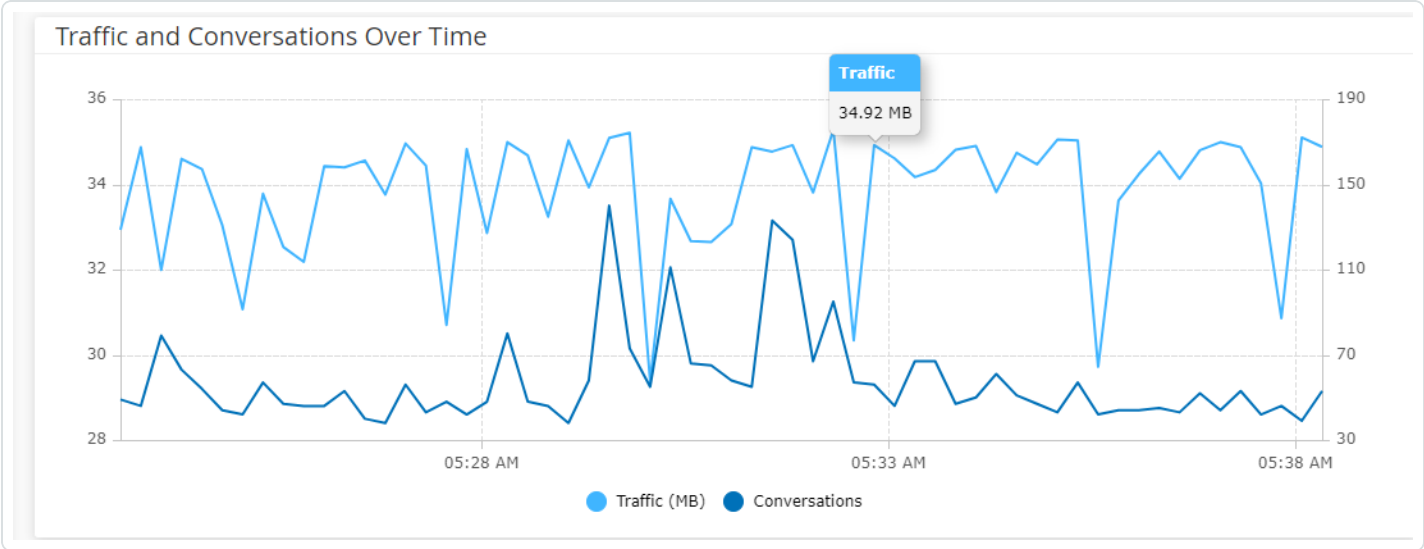
Die Seite **Netzwerk – Zusammenfassung** enthält visuelle Diagramme, die einen Überblick über die Netzwerkaktivitäten geben. Sie können die Daten für einen bestimmten Zeitraum anzeigen lassen.



Interagieren Sie mit den folgenden Widgets, um zusätzliche Details anzuzeigen.

Traffic und Konversationen im zeitlichen Verlauf

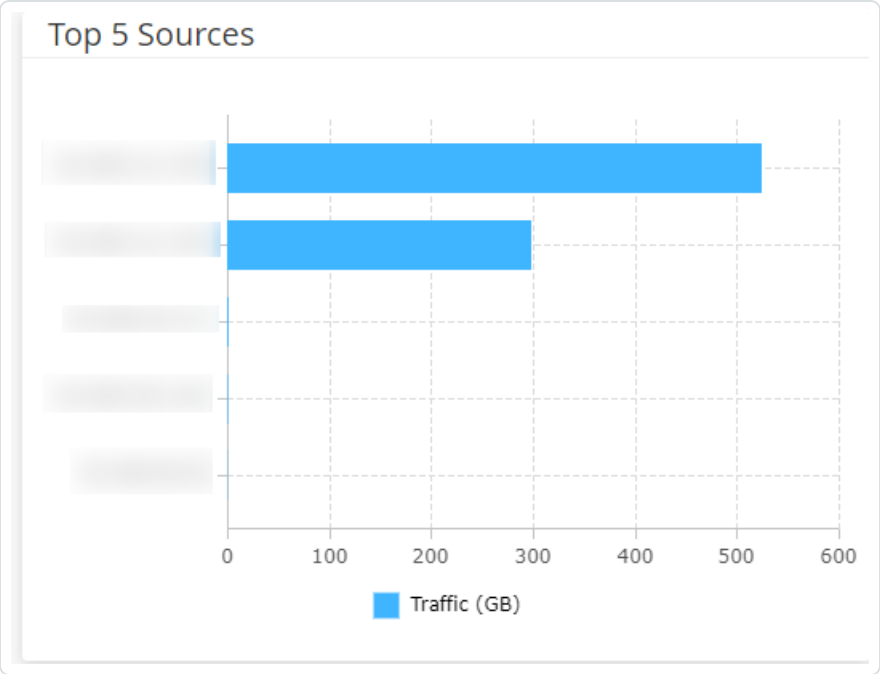
Ein Liniendiagramm zeigt das Traffic-Volumen (gemessen in KB/MB/GB) und die Anzahl der Konversationen im Netzwerk im Laufe der Zeit an. Die Legende wird oben im Diagramm angezeigt. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um spezifische Daten über den Traffic und die Konversationen in diesem Zeitsegment anzuzeigen.



Hinweis: Die Länge des Zeitsegments wird entsprechend der im Diagramm angezeigten Zeitskala angepasst. Beispiel: Die Daten eines 15-Minuten-Zeitraums werden für jede Minute separat angezeigt, während die Daten eines 30-Tage-Zeitraums für Segmente von jeweils 6 Stunden angezeigt werden.

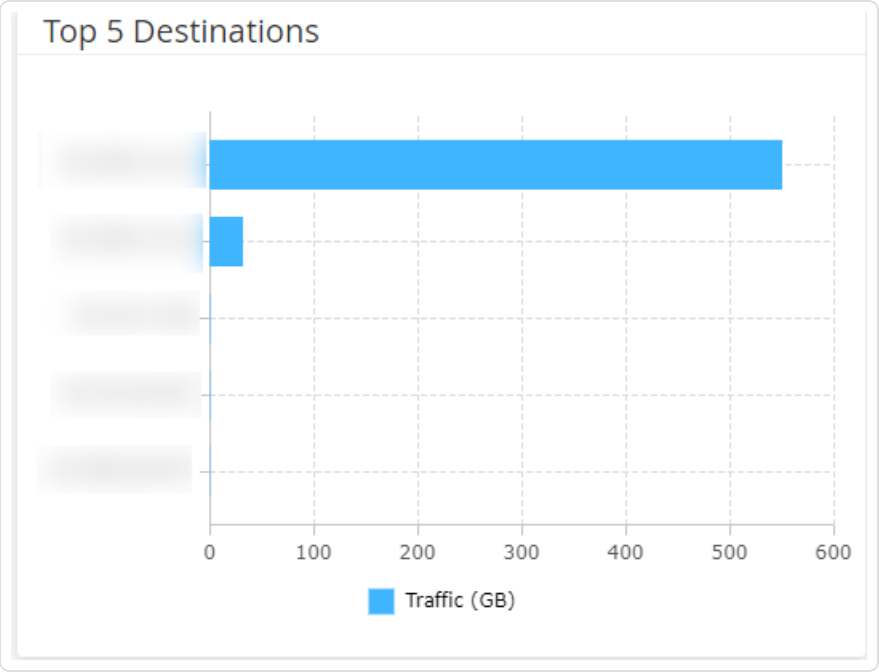
Top 5 Quellen

Das Widget „Top 5 Quellen“ zeigt die Anzahl der Konversationen und das Traffic-Volumen für jedes der Top-5-Assets an, die während eines bestimmten Zeitraums Mitteilungen über das Netzwerk gesendet haben. Sie können die Quell-Assets anhand ihrer IP-Adressen identifizieren. Wenn Sie den Mauszeiger über ein Säulendiagramm bewegen, werden die Anzahl der Konversationen und das von diesem Asset gesendete Traffic-Volumen angezeigt.



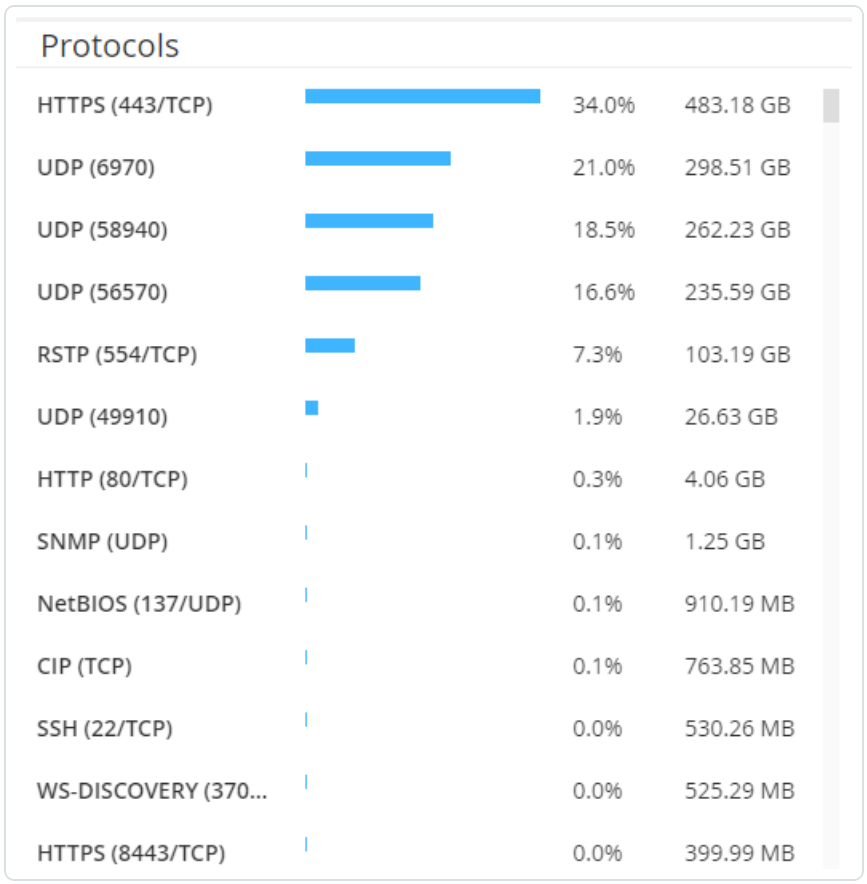
Top 5 Ziele

Das Widget „Top 5 Ziele“ zeigt die Anzahl der Konversationen und das Traffic-Volumen für jedes der Top-5-Assets an, die während eines bestimmten Zeitraums Mitteilungen über das Netzwerk empfangen haben. Sie können die Ziel-Assets anhand ihrer IP-Adressen identifizieren. Wenn Sie den Mauszeiger über ein Säulendiagramm bewegen, werden die Anzahl der Konversationen und das von diesem Asset empfangene Traffic-Volumen angezeigt.



Protokolle

Das Widget **Protokolle** enthält Daten über die Verwendung verschiedener Protokolle für die Kommunikation innerhalb des Netzwerks während eines bestimmten Zeitraums.



Die Protokolle sind von den am häufigsten verwendeten (oben) bis zu den am seltensten verwendeten (unten) angeordnet. Jedes Protokoll zeigt die folgenden Informationen:

- Ein Säulendiagramm mit der Nutzungsrate, wobei eine vollständige Säule die höchste Nutzung anzeigt und Teilsäulen das Ausmaß der Nutzung im Vergleich zum am häufigsten genutzten Protokoll angeben
- Prozentsatz der Nutzung
- Gesamtvolumen der Kommunikation

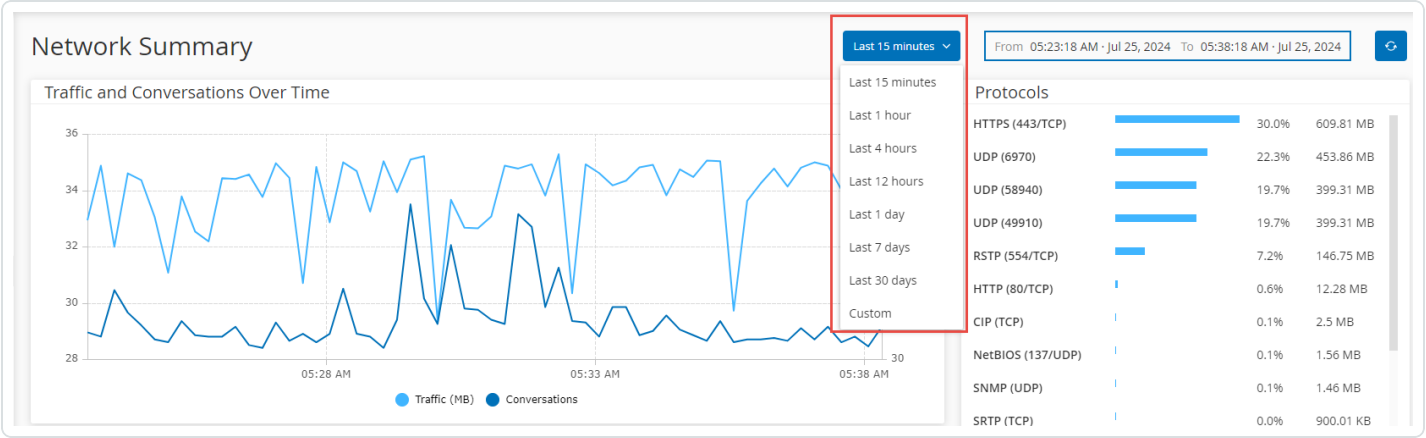
Zeitraum festlegen

Auf der Seite **Netzwerk – Zusammenfassung** werden Daten angezeigt, die die Netzwerkaktivität während eines bestimmten Zeitraums darstellen. Die Kopfleiste zeigt den Zeitraum für die aktuell angezeigten Daten. Der Standardzeitraum ist auf **Letzte 15 Minuten** festlegt. In der Kopfleiste werden außerdem die Start- und die Endzeit des Zeitraums angezeigt.

So legen Sie den Zeitraum fest:

Klicken Sie in der Kopfleiste auf das Dropdown-Feld für den Zeitraum. Die Standardeinstellung lautet **Letzte 15 Minuten**.

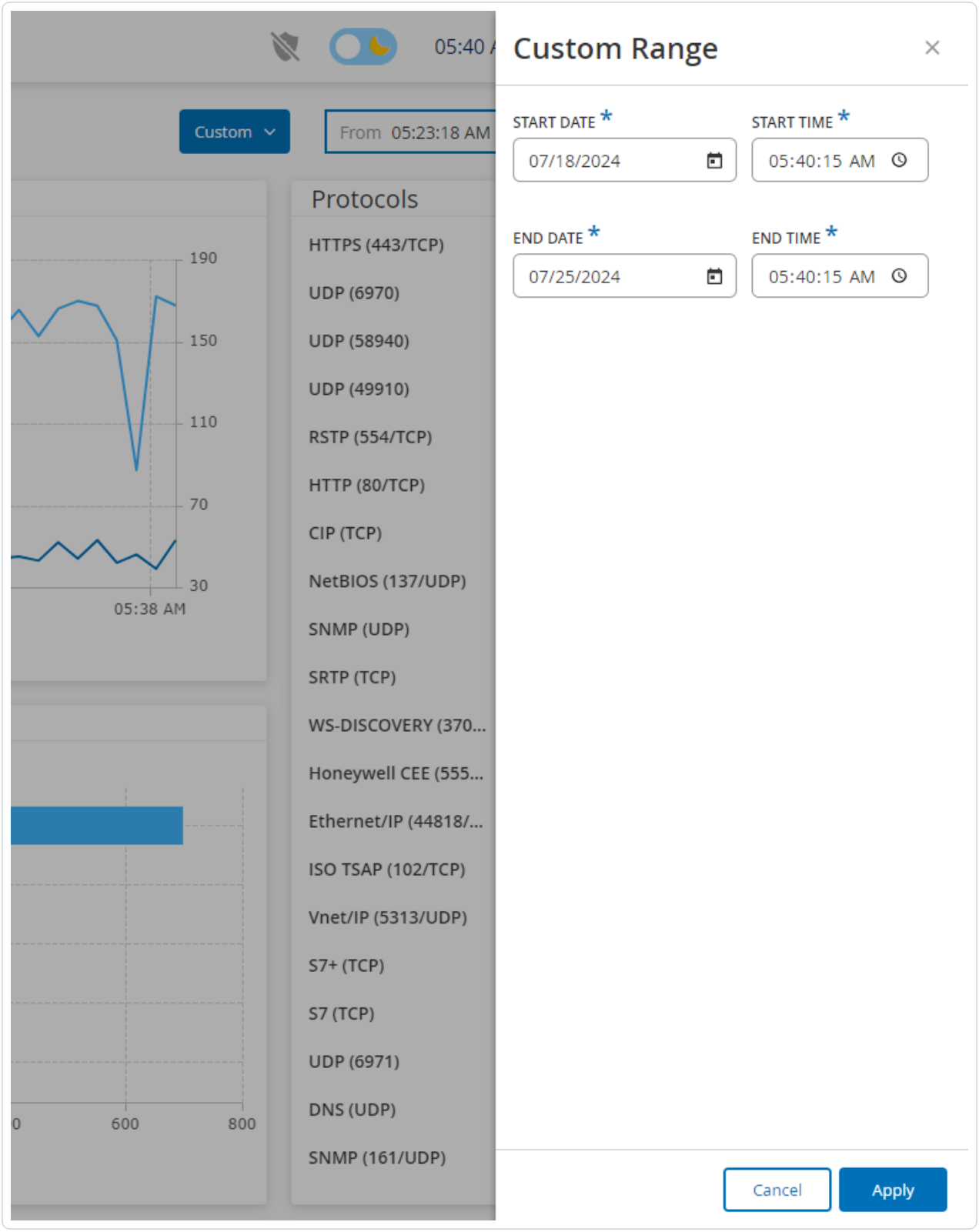
Im Dropdown-Feld werden die verfügbaren Optionen aufgeführt.



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“).
- Legen Sie einen benutzerdefinierten Zeitraum fest:
- Klicken Sie auf **Benutzerdefiniert**.

  Das Fenster **Benutzerdefinierter Bereich** wird angezeigt.



- Geben Sie das **Startdatum**, die **Startzeit**, das **Enddatum** und die **Endzeit** ein.

- Klicken Sie auf **Anwenden**.

  Nachdem Sie den Zeitraum festgelegt haben, werden in der Kopfleiste das Start- und Enddatum sowie die Start- und Endzeit neben der Zeitraumauswahl angezeigt. OT Security aktualisiert die Seite, um Daten innerhalb des ausgewählten Zeitraums anzuzeigen.

Paketerfassungen

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

Die Seite **Paketerfassungen** zeigt alle PCAP-Dateien im System an. Der Bereich **Abgeschlossen** enthält Listen aller abgeschlossenen Dateien, die zum Herunterladen verfügbar sind. Der Bereich **Laufend** enthält Details zu der Paketerfassung, die derzeit ausgeführt wird.

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

In der Tabelle mit Paketerfassungen können Sie Spalten ein- und ausblenden und die Listen sortieren und filtern sowie nach Schlüsselwörtern suchen. Weitere Informationen zum Anpassen von Tabellen finden Sie unter Tabellen anpassen.

> **Hinweis**: Sie können die PCAP-Datei für ein einzelnes Ereignis auch über die Seite **Ereignisse** herunterladen, siehe Dateien herunterladen.

Paketerfassungsparameter

Die Liste der Paketerfassungen enthält die folgenden Details:

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: **Abgeschlossen** oder **Fortlaufend**.
Sensor	Der OT Security Sensor, der das Paket erfasst hat. Für Pakete, die direkt von der OT Security Appliance erfasst wurden, wird der Wert `lokal` angezeigt.
Dateiname	Der Name der Datei.
Dateigröße	Die Größe der Datei, angegeben in KB/MB.

Anzeige der Paketerfassungen filtern

Sie können die Anzeige der Paketerfassungen filtern, um nach einer bestimmten PCAP-Datei zu suchen. Geben Sie hierzu die Parameter für Start- und/oder Endzeit an.

So filtern Sie Paketerfassungen:

1. Gehen Sie zu **Netzwerk** > **Paketerfassungen**.
2. Um nach der Startzeit zu filtern, bewegen Sie den Mauszeiger über **Startzeit** und klicken Sie auf das Symbol ▽.

   Ein Dropdown-Menü wird geöffnet.

   1. So legen Sie den Filter fest:

      a. Wählen Sie im Dropdown-Menü den gewünschten Filter aus: **Jederzeit (Standardeinstellung)**, **Begonnen vor** oder **Begonnen nach**.

      b. Wenn Sie **Begonnen vor** oder **Begonnen nach** auswählen, wird ein Fenster mit den Feldern **Datum** und **Uhrzeit** angezeigt, in denen Sie das gewünschte Datum und die Uhrzeit wählen können.

      c. Klicken Sie auf **Anwenden**.
3. Um nach der Endzeit zu filtern, bewegen Sie den Mauszeiger über **Endzeit** und klicken Sie auf das Symbol ▽.

   Ein Dropdown-Menü wird geöffnet.

1. So legen Sie den Filter fest:

    a. Wählen Sie den gewünschten Filter aus: **Jederzeit (Standardeinstellung)**, **Beendet vor** oder **Beendet nach**.

    b. Wenn Sie **Beendet vor** oder **Beendet nach** auswählen, wird ein Fenster mit den Feldern **Datum** und **Uhrzeit** angezeigt, in denen Sie das gewünschte Datum und die Uhrzeit wählen können.

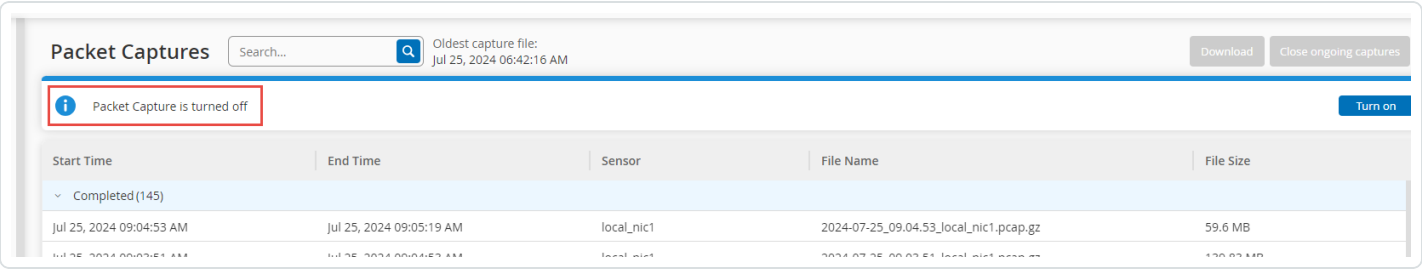
    c. Klicken Sie auf **Anwenden**.

    OT Security wendet den Filter an, und nur die innerhalb des festgelegten Zeitraums generierten Dateien werden angezeigt.

Paketerfassungen aktivieren oder deaktivieren

Sie können die Paketerfassungsfunktion unter **Lokale Einstellungen** > **Systemkonfiguration** > **Gerät** aktivieren oder deaktivieren.

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



Wichtig: Sie können die Paketerfassungsfunktion unter **Netzwerk** > **Paketerfassungen** aktivieren, aber nicht deaktivieren.

So aktivieren Sie die Paketerfassung:

1. Gehen Sie zu **Netzwerk** > **Paketerfassungen**.
2. Klicken Sie in der **Kopfleiste** auf **Aktivieren**.

    OT Security startet die Paketerfassung.

Dateien herunterladen

Sie können alle **abgeschlossenen** PCAP-Dateien auf Ihren lokalen Computer herunterladen. Anschließend können Sie die Dateien mit Tools zur Analyse von Netzwerkprotokollen wie Wireshark analysieren.

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 in einer neuen Datei zu beginnen.

So laden Sie eine abgeschlossene Datei herunter:

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

   OT Security lädt die PCAP-Datei im ZIP-Format auf Ihren lokalen Computer herunter.

So schließen Sie die aktuelle Paketerfassung manuell:

1. Gehen Sie zu **Netzwerk** > **Paketerfassungen**.
2. Klicken Sie in der **Kopfleiste** auf **Laufende Erfassungen schließen**.

   OT Security beendet die aktuelle Erfassung, und die Datei steht zum Herunterladen zur Verfügung. OT Security startet automatisch eine neue Paketerfassung.

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. Die Seite **Konversationen** zeigt eine Liste der aktuellen und vergangenen Konversationen, einschließlich detaillierter Informationen zu den Konversationen.

Sie können auf der Seite **Konversationen** die folgenden Aktionen durchführen:

- **Suchen** – Suchen Sie nach bestimmten Konversationen, indem Sie Informationen zur Identifizierung in das Feld **Suchen** eingeben.
- **Exportieren** – Verwenden Sie die Schaltfläche  „Exportieren“, um alle Daten aus der

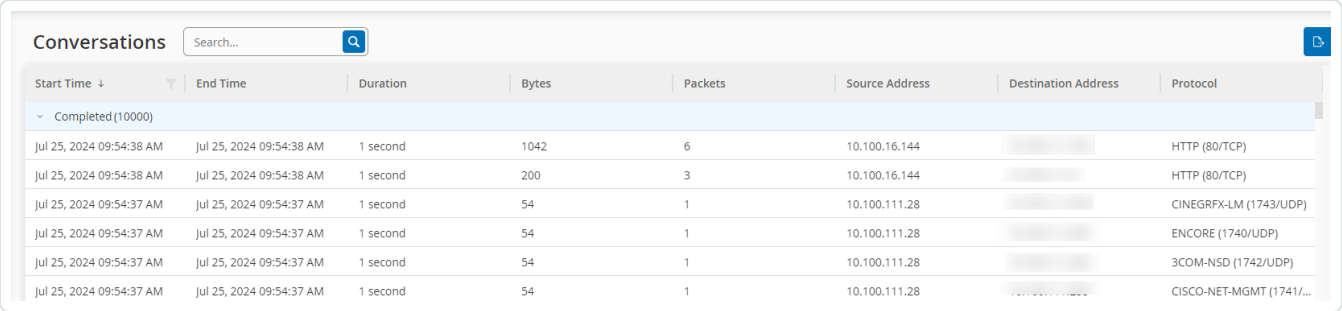
Registerkarte **Konversationen** als CSV-Datei auf Ihren lokalen Computer zu exportieren.

> **Hinweis**: Die Konversationstabelle enthält die letzten 10.000 Netzwerkkonversationen.

So greifen Sie auf die Seite **Konversationen** zu:

1. Gehen Sie zu **Netzwerk** > **Konversationen**.

   Die Seite **Konversationen** wird angezeigt.



   Die Seite „Konversationen“ enthält die folgenden Details:

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 während der Konversation gesendeten Datenpakete.
Quelladresse	Die IP-Adresse 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.

Gruppen

Gruppen sind die grundlegenden Bausteine zum Erstellen von Richtlinien. Wenn Sie eine Richtlinie konfigurieren, legen Sie jede Richtlinienbedingung mit Gruppen anstatt mit einzelnen Entitäten fest.

OT Security wird mit einigen vordefinierten Gruppen geliefert. Sie können außerdem Ihre eigenen benutzerdefinierten Gruppen erstellen. Um den Prozess der Bearbeitung und Erstellung von Richtlinien zu optimieren, empfiehlt Tenable, die benötigten Gruppen im Voraus zu konfigurieren.

Hinweis: Richtlinienparameter können nur mithilfe von Gruppen festgelegt werden. Wenn Sie möchten, dass eine Richtlinie für eine einzelne Entität gilt, müssen Sie eine Gruppe konfigurieren, die nur diese Entität umfasst.

Gruppen anzeigen

So zeigen Sie Gruppen an:

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

- **Vordefinierte Gruppen** – Diese Gruppen sind vorkonfiguriert. Sie können diese Gruppen nicht bearbeiten.
- **Benutzerdefinierte Gruppen** – Diese Gruppen können Sie erstellen und bearbeiten.

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-Mail-Adressen, 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.

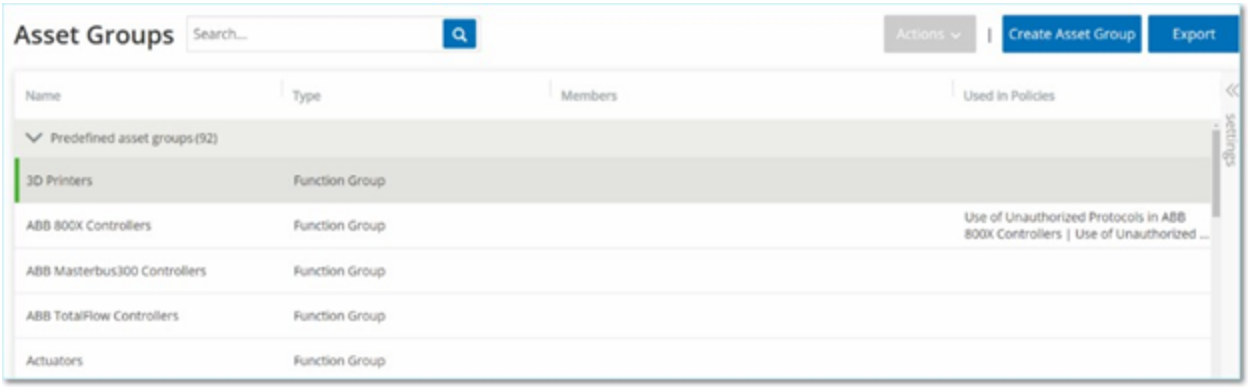
- **Planungsgruppen** – Planungsgruppen sind Zeitbereiche, mit denen die Zeit konfiguriert wird, zu der das angegebene Ereignis eintreten muss, um die Richtlinienbedingungen zu erfüllen.
- **Tag-Gruppen** – Tags sind Parameter in Controllern, die spezifische Betriebsdaten enthalten. Tag-Gruppen werden 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.

Asset-Gruppen anzeigen



Der Bildschirm **Asset-Gruppen** zeigt alle Asset-Gruppen, die derzeit im System konfiguriert sind. Die Registerkarte **Vordefinierte Asset-Gruppen** enthält Gruppen, die in das System integriert sind und die Sie nicht bearbeiten, duplizieren oder löschen können. Die Registerkarte **Benutzerdefinierte**

Asset-Gruppen enthält benutzerdefinierte Gruppen, die vom Benutzer erstellt wurden. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Asset-Gruppen“ enthält die folgenden Informationen:

Parameter	Beschreibung
Status	Zeigt an, ob die Richtlinie aktiviert oder deaktiviert ist. Wenn das System die Richtlinie automatisch deaktiviert, 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. Weitere Informationen finden Sie in Abschnitt Schweregradstufen.
Ereignistyp	Der Ereignistyp, der diese Ereignisrichtlinie auslöst.
Kategorie	Die allgemeine Kategorie des Ereignisses, das 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, für die die Richtlinie gilt. Eine Asset-Gruppe ist das Asset, das die Aktivität initiiert hat.
Name	Der Name zur Identifizierung der Gruppe.
Typ	Der Gruppentyp. 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 **Tabellenaktionen** > **Anzeigen** > Registerkarte **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 **Tabellenaktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.
In Abfragen verwendet	Zeigt den Namen der Abfrage an, die diese Asset-Gruppe 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.

Asset-Gruppen erstellen

Sie können benutzerdefinierte Asset-Gruppen erstellen, um sie bei der Konfiguration von Richtlinien zu verwenden. 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:

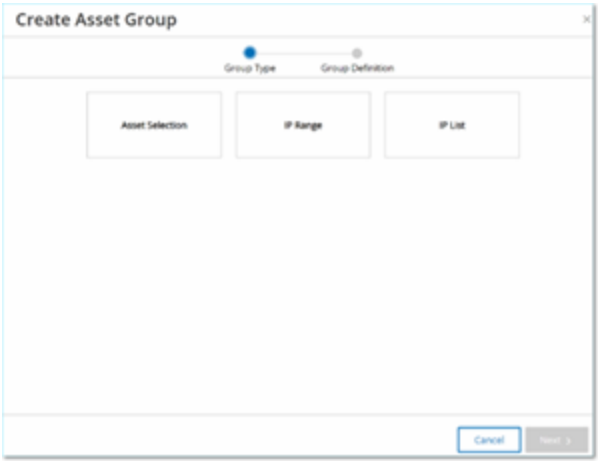
- **Asset-Auswahl** – Angabe der Assets, die in der Gruppe enthalten sind.
- **IP-Liste** – Angabe der IP-Adressen der Assets, die in der Gruppe enthalten sind.
- **IP-Bereich** – Angabe des Bereichs der IP-Adressen der Assets, die in der Gruppe enthalten sind.

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

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

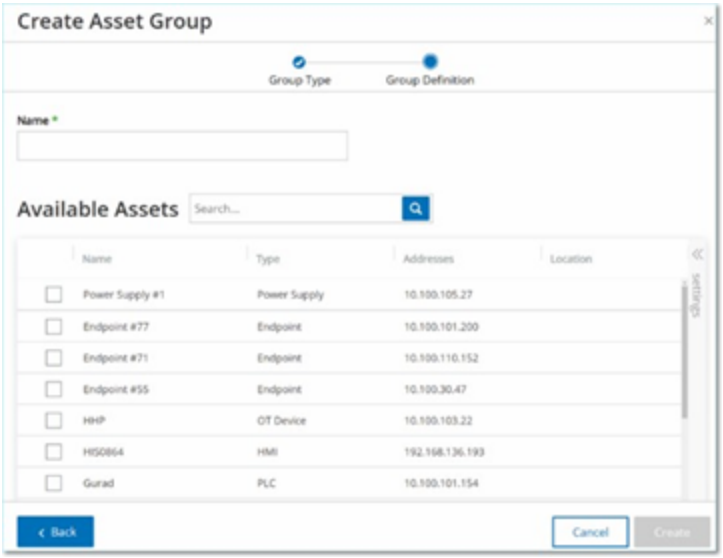
1. Klicken Sie auf **Asset-Gruppe erstellen**.

   Der Bereich **Asset-Gruppe erstellen** wird angezeigt.



2. Klicken Sie auf **Asset-Auswahl**.
3. Klicken Sie auf **Weiter**.

   Die Liste der **verfügbaren Assets** wird angezeigt.



4. 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.

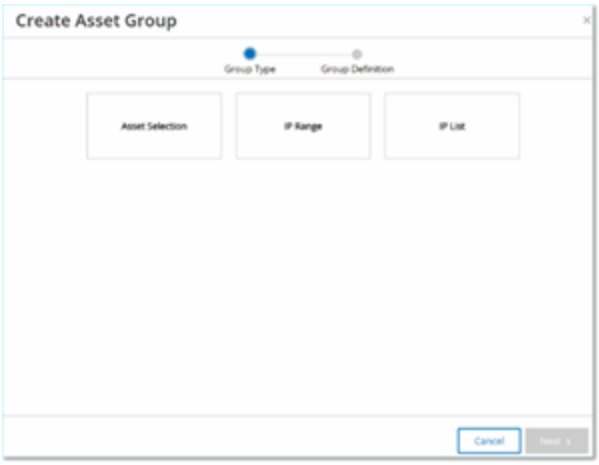
5. Aktivieren Sie das Kontrollkästchen neben jedem Asset, das Sie in die Gruppe aufnehmen möchten.
6. Klicken Sie auf **Erstellen**.

   OT Security erstellt die neue Asset-Gruppe und zeigt sie im Bildschirm **Asset-Gruppen** an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

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

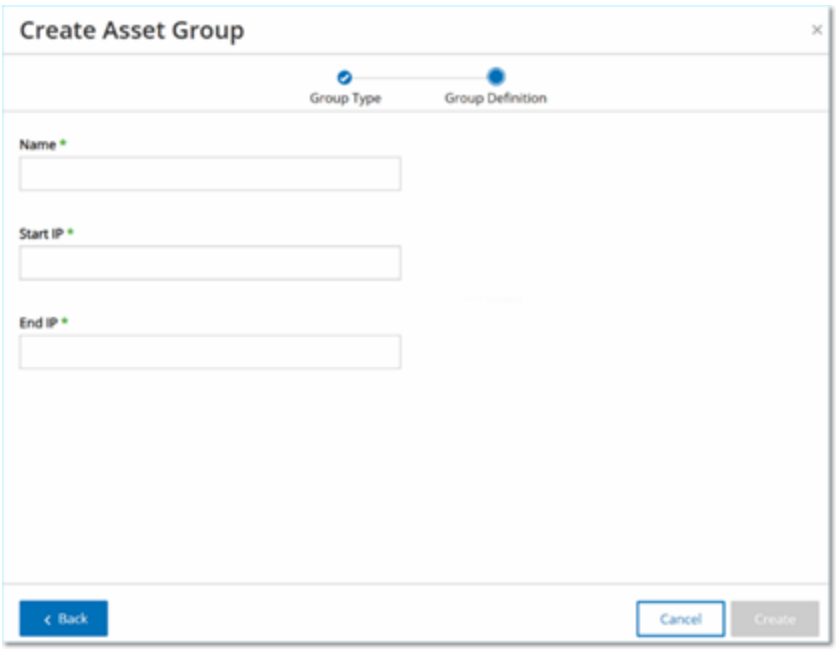
1. Klicken Sie auf **Asset-Gruppe erstellen**.

   Der Bereich **Asset-Gruppe erstellen** wird angezeigt.



2. Klicken Sie auf **IP-Bereich**.
3. Klicken Sie auf **Weiter**.

   Der Fensterbereich zur Auswahl des IP-Bereichs wird angezeigt.



4. 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.

5. Geben Sie im Feld **Start-IP** die IP-Adresse am Anfang des Bereichs ein, den Sie einschließen möchten.

6. Geben Sie im Feld **End-IP** die IP-Adresse am Ende des Bereichs ein, den Sie einschließen möchten.

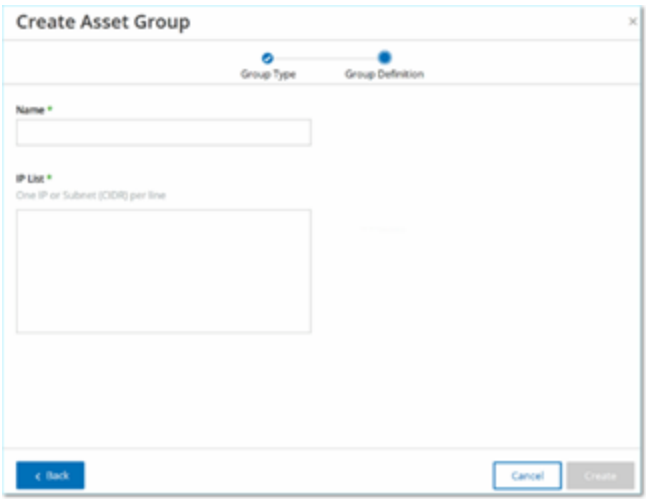
7. Klicken Sie auf **Erstellen**.

   OT Security erstellt die neue Asset-Gruppe und zeigt sie im Bildschirm **Asset-Gruppen** an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

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

1. Klicken Sie auf **Asset-Gruppe erstellen**.

   Der Bereich **Asset-Gruppe erstellen** wird angezeigt.



2. Klicken Sie auf **IP-Liste**.
3. Klicken Sie auf **Weiter**.

   Der Bereich **IP-Liste** wird angezeigt.
4. 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.
5. Geben Sie im Feld **IP-Liste** eine IP-Adresse oder ein Subnetz ein, die bzw. das in die Gruppe aufgenommen werden soll.
6. Um der Gruppe weitere Assets hinzuzufügen, geben Sie jede zusätzliche IP-Adresse oder jedes zusätzliche Subnetz in einer separaten Zeile ein.
7. Klicken Sie auf **Erstellen**.

   OT Security erstellt die neue Asset-Gruppe und zeigt sie im Bildschirm **Asset-Gruppen** an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

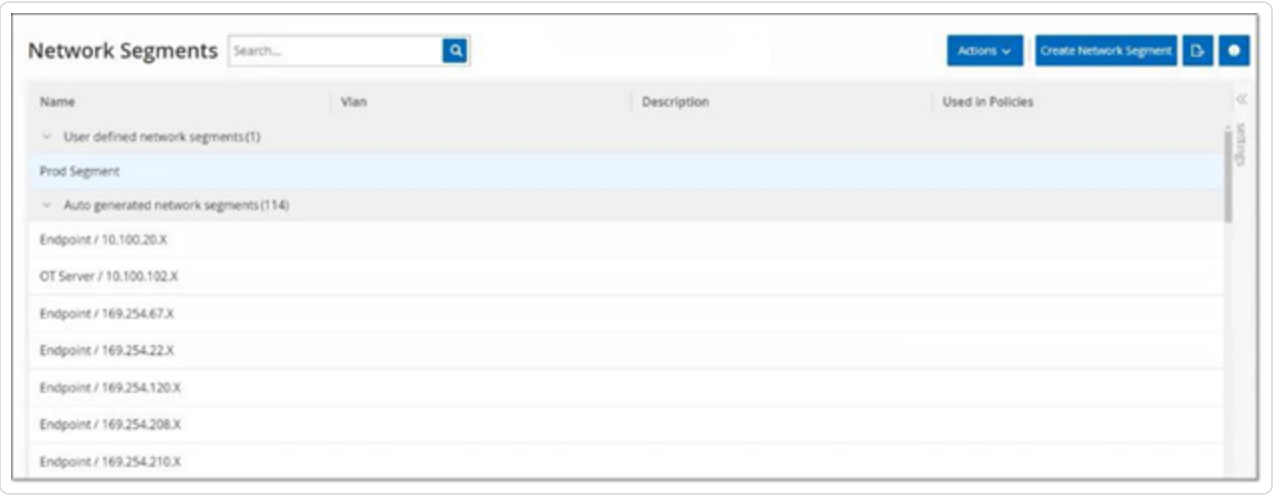
Netzwerksegmente

Durch Netzwerksegmentierung können Sie Gruppen zusammengehöriger Netzwerk-Assets erstellen und dadurch Asset-Gruppen logisch voneinander trennen. OT Security 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 wird 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. Eine Spalte im Bildschirm **Inventar** zeigt das Netzwerksegment für jedes Asset, sodass Sie Ihre Assets einfach nach Netzwerksegment sortieren und filtern können.

Netzwerksegmente anzeigen



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 Tabelle „Netzwerksegmente“ zeigt die folgenden Details:

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 **Aktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.

Sie können ein vorhandenes Netzwerksegment anzeigen, bearbeiten, duplizieren oder löschen. Weitere Informationen finden Sie unter Aktionen für Gruppen.

Netzwerksegmente erstellen

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:

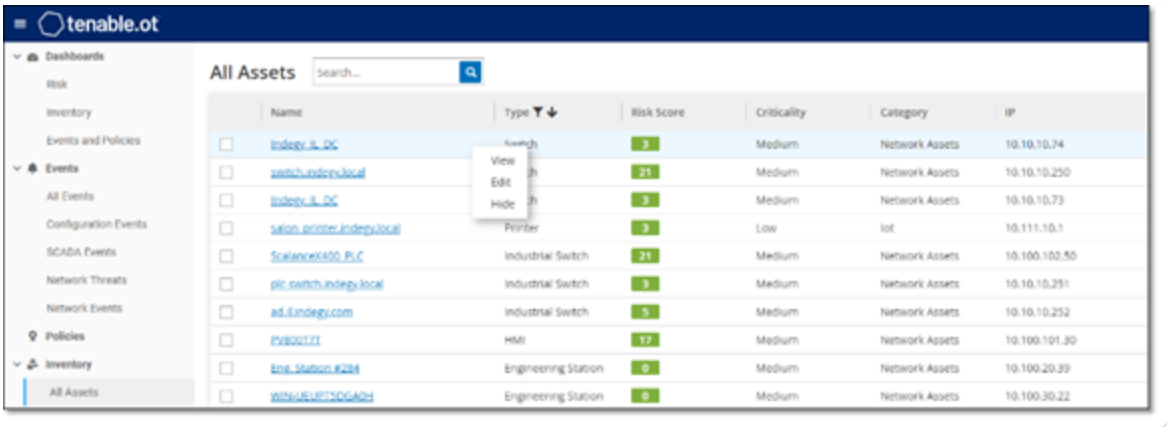
1. Klicken Sie auf **Netzwerksegment erstellen**.

   Der Bereich **Netzwerksegment erstellen** wird angezeigt.

2. Geben Sie im Feld **Name** einen Namen für das Netzwerksegment ein.
3. (Optional) Geben Sie im Feld **VLAN** eine VLAN-Nummer für das Netzwerksegment ein.
4. (Optional) Geben Sie im Feld **Beschreibung** eine Beschreibung des Netzwerksegments ein.
5. Klicken Sie auf **Erstellen**.

   OT Security erstellt das neue Netzwerksegment und zeigt es in der Liste der Netzwerksegmente an.
6. So weisen Sie die Assets dem neu erstellten Netzwerksegment zu:
   a. Gehen Sie zu **Inventar** > **Alle Assets**.
   b. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf das Asset, das Sie dem neu erstellten Netzwerksegment zuweisen möchten, und wählen Sie **Bearbeiten** aus.
- Bewegen Sie den Mauszeiger über das Asset, das Sie zuweisen möchten, und wählen Sie dann im Menü **Aktionen** die Option **Bearbeiten** aus.



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

7. Wählen Sie im Dropdown-Feld **Netzwerksegmente** das gewünschte Netzwerksegment aus.

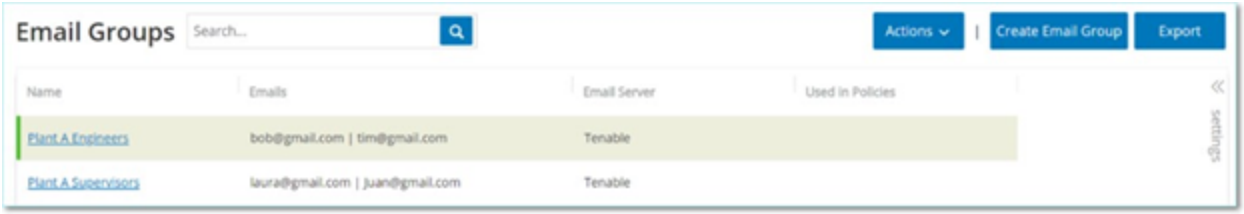
Hinweis: Einigen Assets ist mehr als eine IP-Adresse zugeordnet und Sie können für jede das benötigte Netzwerksegment auswählen.

OT Security weist das Netzwerksegment dem Asset zu und zeigt es in der Spalte **Netzwerksegment** an. 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 Ereignisbenachrichtigungen 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.

E-Mail-Gruppen anzeigen



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

Die Tabelle „E-Mail-Gruppen“ enthält die folgenden Informationen:

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

Parameter	Beschreibung
Name	Der Name zur Identifizierung der Gruppe.
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 **Aktionen** > **Anzeigen** > Registerkarte **Mitglieder**.
E-Mail-Server	Der Name des SMTP-Servers, der zum Senden von E-Mails an die 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 **Aktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.

Darüber hinaus können Sie eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen. Weitere Informationen finden Sie unter Aktionen für Gruppen.

E-Mail-Gruppen erstellen

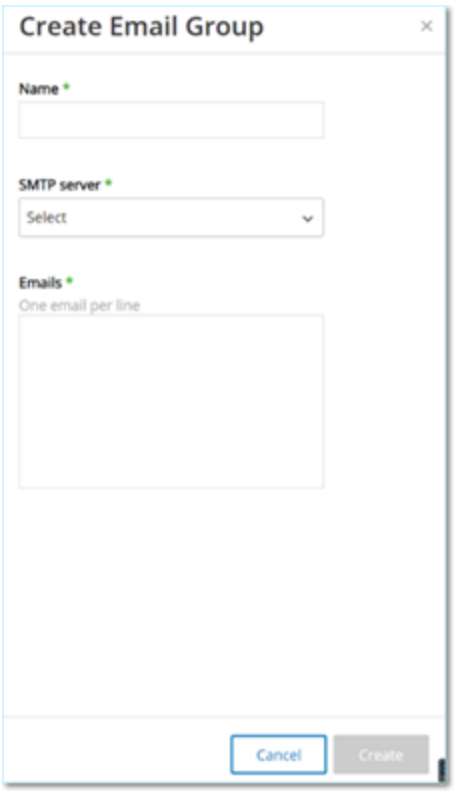
Sie können E-Mail-Gruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Indem Sie zusammengehörige E-Mail-Adressen gruppieren, legen Sie fest, dass Benachrichtigungen zu Richtlinienereignissen an alle relevanten Mitarbeiter gesendet werden.

Hinweis: 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. Klicken Sie auf **E-Mail-Gruppe erstellen**.

   Der Bereich **E-Mail-Gruppe erstellen** wird angezeigt.



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

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

4. Geben Sie im Feld **E-Mails** die E-Mail-Adresse jedes Mitglieds der Gruppe in einer separaten Zeile ein.
5. Klicken Sie auf **Erstellen**.

   OT Security erstellt die neue E-Mail-Gruppe und zeigt sie auf der Seite **E-Mail-Gruppen** an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

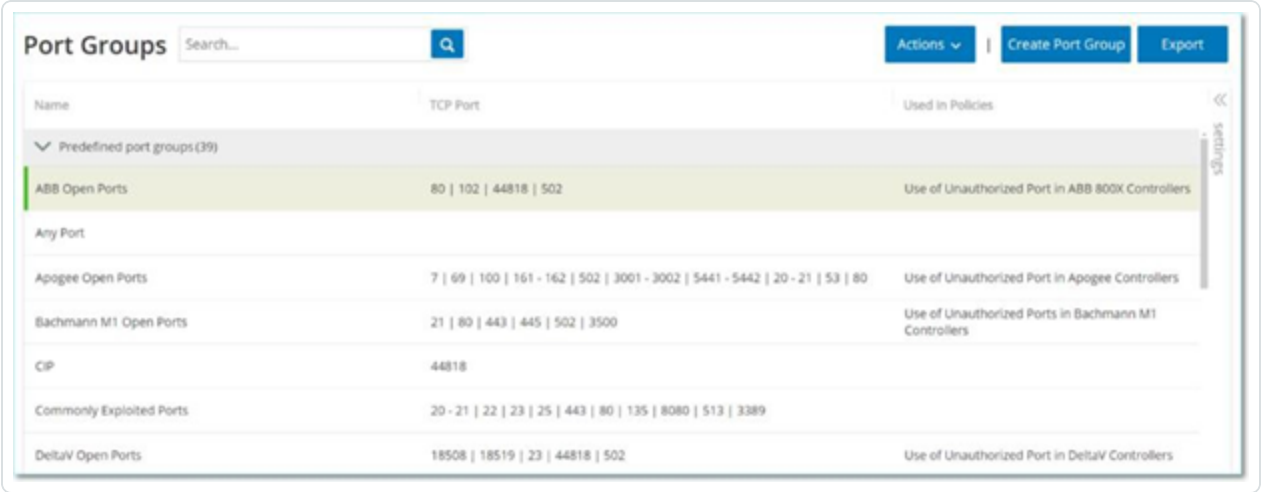
Port-Gruppen

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. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Port-Gruppen anzeigen



Die Tabelle „Port-Gruppen“ enthält die folgenden Details:

Parameter	Beschreibung
Name	Der Name zur Identifizierung der Gruppe.
TCP-Port	Die Liste der Ports und/oder Port-Bereiche, die in der Gruppe enthalten sind. **Hinweis**: Wenn in der Tabelle nicht alle Mitglieder der Gruppe angezeigt werden, klicken Sie auf **Aktionen** > **Anzeigen** > Registerkarte **Mitglieder**, um die Mitglieder anzuzeigen.

In Richtlinien verwendet	Zeigt den Namen jeder Richtlinie an, die diese Port-Gruppe in ihrer Konfiguration verwendet. **Hinweis**: Um weitere Informationen zu den Richtlinien anzuzeigen, in denen diese Gruppe verwendet wird, klicken Sie auf **Aktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.

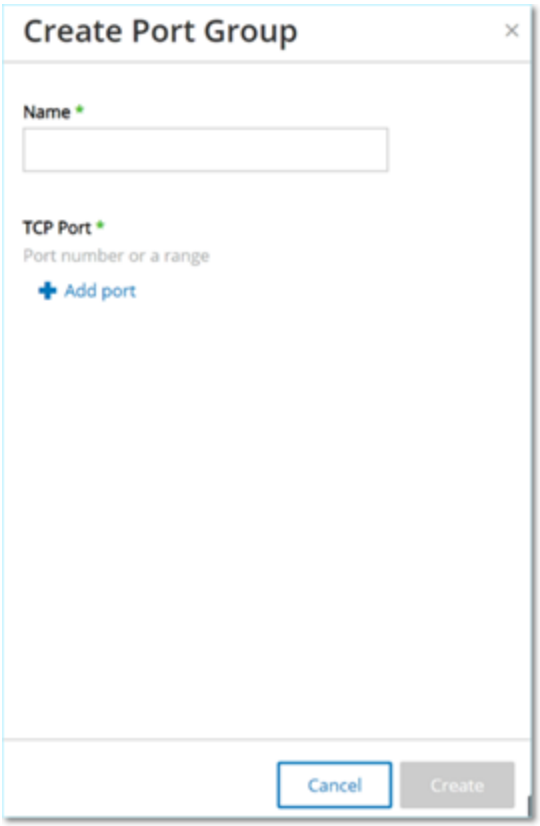
Port-Gruppen erstellen

Sie können benutzerdefinierte Port-Gruppen erstellen, die Sie bei der Konfiguration von Richtlinien verwenden können. 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. Klicken Sie auf **Port-Gruppe erstellen**.

   Der Bereich **Port-Gruppe erstellen** wird angezeigt.



2. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.

3. Geben Sie im Feld **TCP-Port** einen einzelnen Port oder einen Bereich von Ports ein, die in die Gruppe aufgenommen werden sollen.
4. So fügen Sie der Gruppe weitere Ports hinzu:
    a. Klicken Sie auf **+ Port hinzufügen**.

        Ein Feld zur Auswahl eines neuen Ports wird angezeigt.

    b. Geben Sie im neuen Feld **Port-Nummer** einen einzelnen Port oder einen Bereich von Ports ein, die in die Gruppe aufgenommen werden sollen.
5. Klicken Sie auf **Erstellen**.

    OT Security erstellt die neue Port-Gruppe und zeigt sie in der Liste der Port-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

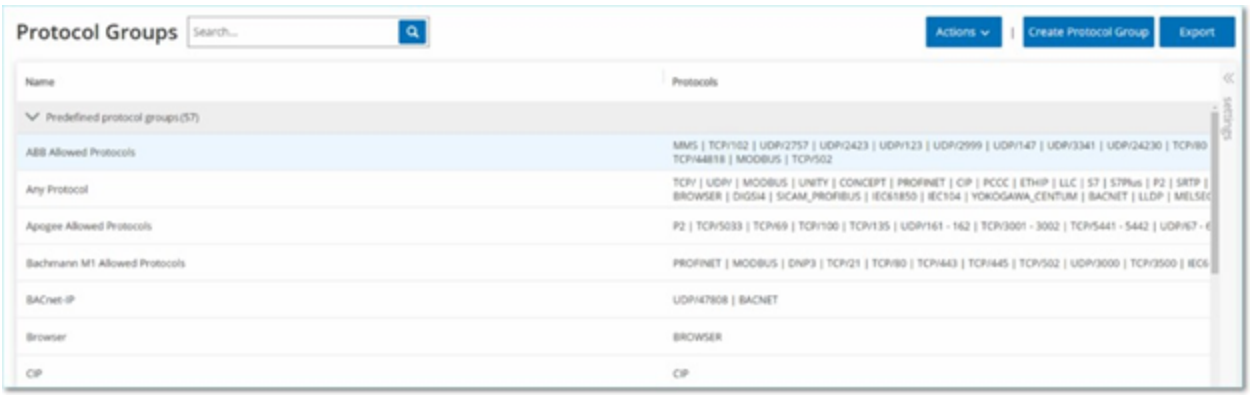
Protokollgruppen

Protokollgruppen sind Gruppen von Protokollen, die für Konversationen zwischen Assets im Netzwerk verwendet werden. Protokollgruppen sind eine Richtlinienbedingung für Netzwerkrichtlinien. Außerdem definieren sie, welche Protokolle, die zwischen bestimmten Assets verwendet werden, eine Richtlinie auslösen.

OT Security enthält eine Reihe vordefinierter Protokollgruppen, die verwandte Protokolle umfassen. Diese Gruppen stehen zur Verwendung in Richtlinien zur Verfügung. Sie können diese Gruppen nicht bearbeiten oder löschen. 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 (d. h. Modbus, PROFINET, CIP usw.) gruppiert werden. Sie können außerdem Ihre eigenen benutzerdefinierten Protokollgruppen erstellen.

Protokollgruppen anzeigen



Der Bildschirm **Protokollgruppen** zeigt alle Protokollgruppen an, die derzeit im System konfiguriert sind. Die Registerkarte **Vordefiniert** zeigt die in das System integrierten Gruppen an. Sie können diese Gruppen nicht bearbeiten oder löschen, aber Sie können sie duplizieren. Die Registerkarte **Benutzerdefiniert** zeigt die benutzerdefinierten Gruppen, die Sie erstellt haben. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Protokollgruppen“ enthält diese Details:

Parameter	Beschreibung
Name	Der Name zur Identifizierung der Gruppe.
Protokolle	Die Liste der Protokolle, die in der Gruppe enthalten sind. **Hinweis**: Wenn Sie nicht alle Mitglieder der Gruppe anzeigen können, klicken Sie auf die Registerkarte **Aktionen** > **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 **Aktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.

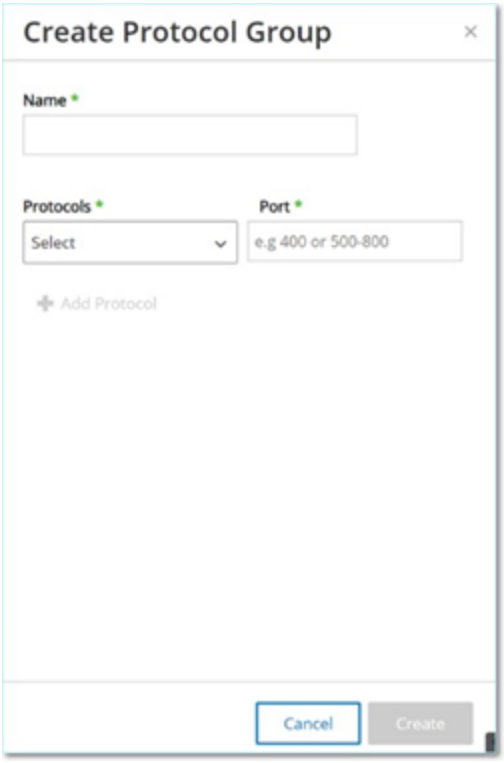
Protokollgruppen erstellen

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. Klicken Sie auf **Protokollgruppe erstellen**.

   Der Bereich **Protokollgruppe erstellen** wird angezeigt.



2. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
3. Wählen Sie im Dropdown-Feld **Protokolle** einen Protokolltyp aus.
4. Wenn das ausgewählte Protokoll TCP oder UDP ist, geben Sie im Feld **Port** eine Port-Nummer oder einen Bereich von Ports ein.

   Bei anderen Protokolltypen müssen Sie keinen Wert in das Feld **Port** eingeben.
5. So fügen Sie der Gruppe weitere Protokolle hinzu:
   a. Klicken Sie auf **+ Protokoll hinzufügen**.

      Ein neues **Protokollauswahl**-Feld wird angezeigt.

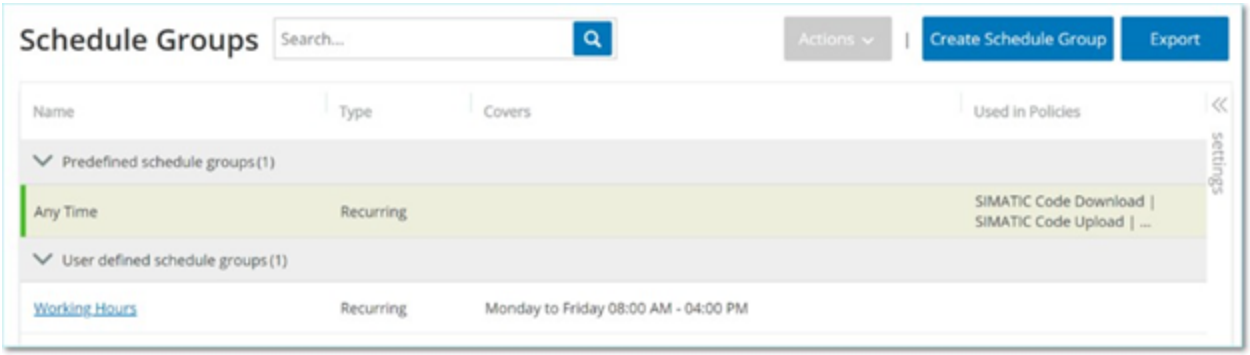
   b. Füllen Sie die neue **Protokollauswahl** wie in den Schritten 4 bis 5 beschrieben aus.
6. Klicken Sie auf **Erstellen**.

OT Security erstellt die neue Protokollgruppe und zeigt sie in der Liste der Protokollgruppen an. 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.

Planungsgruppen anzeigen



Der Bildschirm **Planungsgruppen** zeigt alle Planungsgruppen, die derzeit im System konfiguriert sind. Die Registerkarte **Vordefinierte Planungsgruppen** enthält die in das System integrierten Gruppen. Sie können diese Gruppen nicht bearbeiten, duplizieren oder löschen. Die Registerkarte **Benutzerdefinierte Planungsgruppen** zeigt die benutzerdefinierten Gruppen, die Sie erstellt haben. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Planungsgruppen“ enthält die folgenden Details:

Parameter	Beschreibung
Name	Der Name zur Identifizierung der Gruppe.
Typ	Der Gruppentyp. 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 Arbeitszeitplan 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 liegt. 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 Sie nicht alle Mitglieder der Gruppe anzeigen können, klicken Sie auf die Registerkarte **Aktionen** > **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 **Aktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.

Planungsgruppen erstellen

Sie können benutzerdefinierte Planungsgruppen erstellen, die bei der Konfiguration von Richtlinien verwendet werden. Geben Sie einen Zeitbereich oder eine Gruppe von Zeitbereichen mit gemeinsamen Merkmale an, um Ereignisse hervorzugeben, die in diesem Zeitraum stattfinden.

Es gibt zwei Arten von Planungsgruppen:

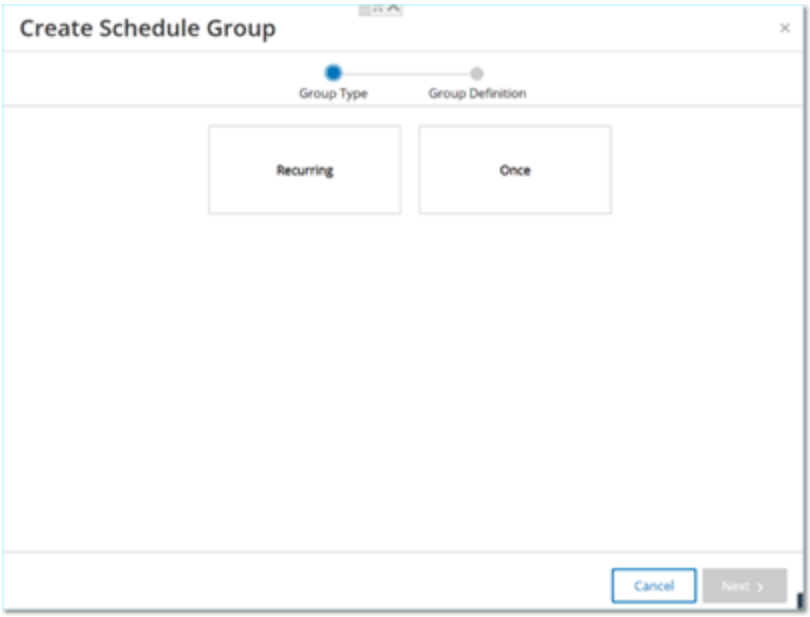
- **Wiederkehrend** – Zeitpläne, die sich wöchentlich wiederholen. Beispielsweise kann ein Arbeitszeitplan als Zeitraum von Montag bis Freitag von 9:00 bis 17:00 Uhr definiert werden.
- **Einmalig** – Zeitpläne, die an einem bestimmten Datum oder in einem bestimmten Datumsbereich liegen. Ein Zeitplan 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“:

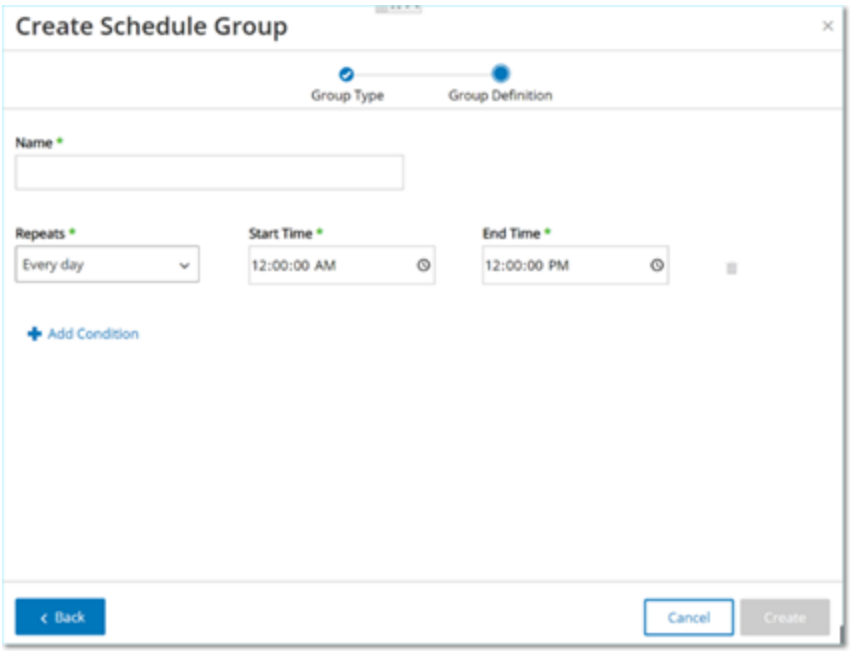
1. Klicken Sie auf **Planungsgruppe erstellen**.

   Der Bereich **Planungsgruppen erstellen** wird angezeigt.



2. Klicken Sie auf **Wiederkehrend**.
3. Klicken Sie auf **Weiter**.

   Die Parameter zum Definieren einer wiederkehrenden Planungsgruppe werden angezeigt.



4. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
5. Wählen Sie im Feld **Wird wiederholt** aus, welche Wochentage in die Planungsgruppe aufgenommen werden.

   Optionen sind: Täglich, Montag bis Freitag oder ein bestimmter Wochentag.

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

6. Geben Sie im Feld **Startzeit** die Tageszeit (HH:MM:SS AM/PM) für den Beginn des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
7. Geben Sie im Feld **Endzeit** die Tageszeit (HH:MM:SS AM/PM) für das Ende des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
8. So fügen Sie der Planungsgruppe weitere Bedingungen (d. h. zusätzliche Zeitbereiche) hinzu:
   a. Klicken Sie auf **+ Bedingung hinzufügen**.

      Eine neue Zeile mit Planungsauswahlparametern wird angezeigt.

   b. Füllen Sie die Zeitplanfelder wie oben in Schritt 5 bis 7 beschrieben aus.
9. Klicken Sie auf **Erstellen**.

OT Security erstellt die neue Planungsgruppe und zeigt sie in der Liste der Planungsgruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Richtlinien verwenden.

So erstellen Sie eine einmalige Planungsgruppe:

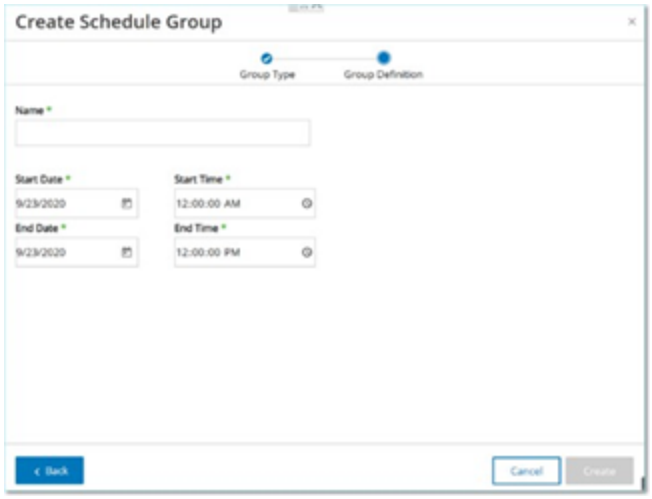
1. Klicken Sie auf **Planungsgruppe erstellen**.

   Der Assistent **Planungsgruppe erstellen** wird angezeigt.

2. Wählen Sie **Zeitraum** aus.

3. Klicken Sie auf **Weiter**.

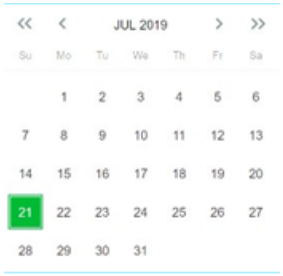
   Die Parameter zum Definieren einer Zeitraum-Planungsgruppe werden angezeigt.



4. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.

5. Klicken Sie im Feld **Startdatum** auf das Kalendersymbol .

   Ein Kalenderfenster wird geöffnet.



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

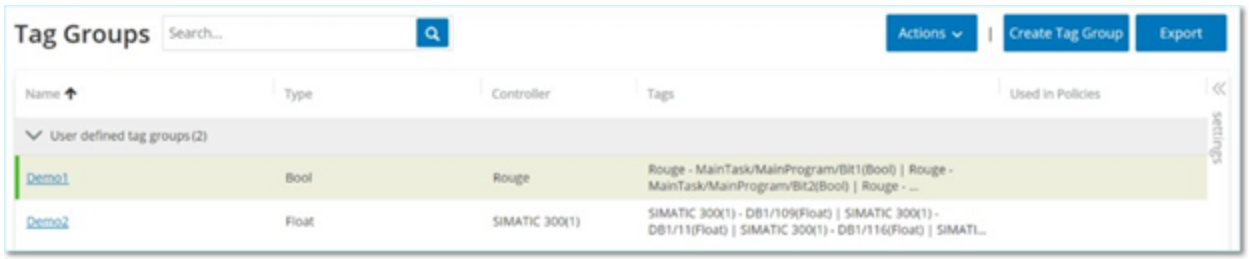
   Ein Kalenderfenster wird geöffnet.
9. Wählen Sie das Datum aus, an dem die Planungsgruppe endet. (Standard: das aktuelle Datum)
10. Geben Sie im Feld **Endzeit** die Tageszeit (HH:MM:SS AM/PM) für das Ende des Zeitbereichs ein, der in der Planungsgruppe enthalten ist.
11. Klicken Sie auf **Erstellen**.

    OT Security erstellt die neue Planungsgruppe und zeigt sie in der Liste der Planungsgruppen an. 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.

Tag-Gruppen anzeigen



Auf der Seite **Tag-Gruppen** werden alle Tag-Gruppen angezeigt, die derzeit im System konfiguriert sind.

Die Tabelle „Tag-Gruppen“ enthält die folgenden Details:

Parameter	Beschreibung
Name	Der Name zur Identifizierung der Gruppe.
Typ	Der Datentyp des Tags. Mögliche Werte sind: „Bool“, „Dint“, „Float“, „Int“, „Long“, „Short“, „Unknown (für Tags eines Typs, den OT Security 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 Sie nicht alle Tags in dieser Zeile sehen können, klicken Sie auf **Aktionen** > **Anzeigen** > Registerkarte **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 **Aktionen** > **Anzeigen** > Registerkarte **In Richtlinien verwendet**.

Sie können eine vorhandene Gruppe anzeigen, bearbeiten, duplizieren oder löschen, siehe Aktionen für Gruppen.

Tag-Gruppen erstellen

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 festgelegt werden, dass sie bestimmte Werte erkennen.

Sie können Tag-Gruppen bearbeiten, duplizieren oder löschen.

So erstellen Sie eine neue Tag-Gruppe:

1. Klicken Sie auf **Tag-Gruppe erstellen**.

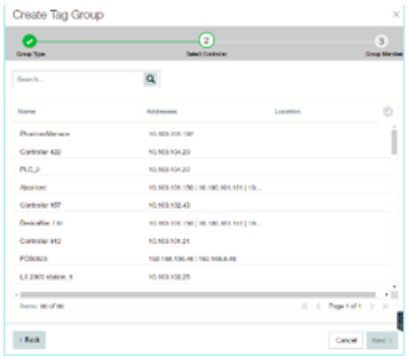
   Der Bereich **Tag-Gruppe erstellen** wird angezeigt.

2. Wählen Sie einen Tag-Typ aus.

   Optionen sind: „Bool“, „Dint“, „Float“, „Int“, „Long“, „Short“ oder „Any Type“ (was Tags verschiedener Typen umfassen kann).

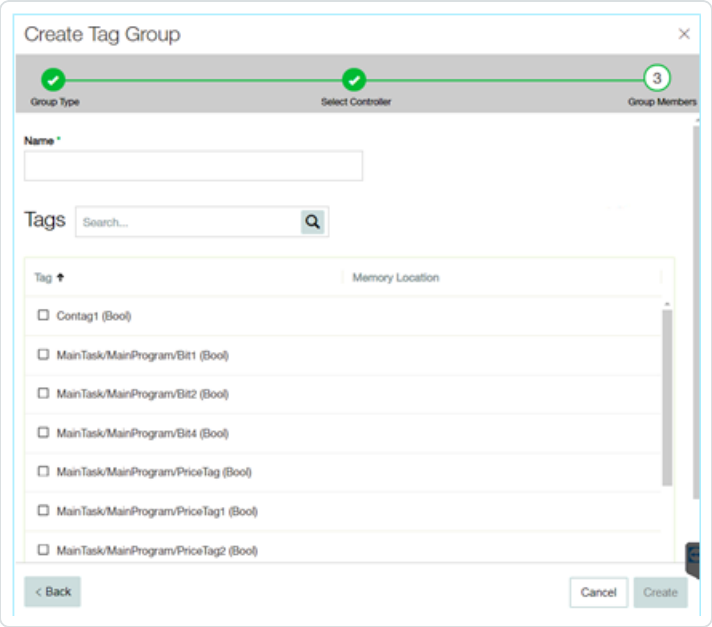
3. Klicken Sie auf **Weiter**.

   Eine Liste der Controller in Ihrem Netzwerk wird angezeigt.



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

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



6. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
7. Aktivieren Sie das Kontrollkästchen neben jedem Tag, das Sie in die Gruppe aufnehmen möchten.
8. Klicken Sie auf **Erstellen**.

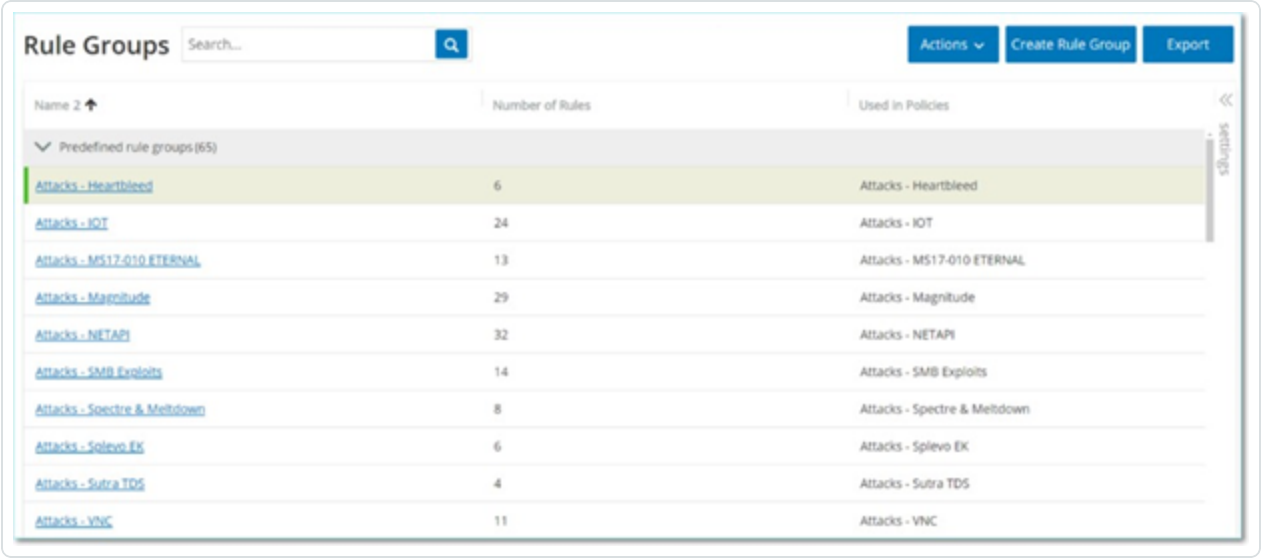
   OT Security erstellt die neue Tag-Gruppe und zeigt sie in der Liste der Tag-Gruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von SCADA-Ereignisrichtlinien verwenden.

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.

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

Regelgruppen anzeigen



Der Bildschirm **Regelgruppen** zeigt alle Regelgruppen, die derzeit im System konfiguriert sind. Die Registerkarte „Vordefiniert“ umfasst die in das System integrierten Gruppen. Sie können diese Gruppen nicht bearbeiten, duplizieren oder löschen. Die Registerkarte **Benutzerdefiniert** zeigt die benutzerdefinierten Gruppen, die vom Benutzer erstellt wurden. Sie können diese Gruppen bearbeiten, duplizieren oder löschen.

Die Tabelle „Regelgruppen“ enthält die folgenden Details:

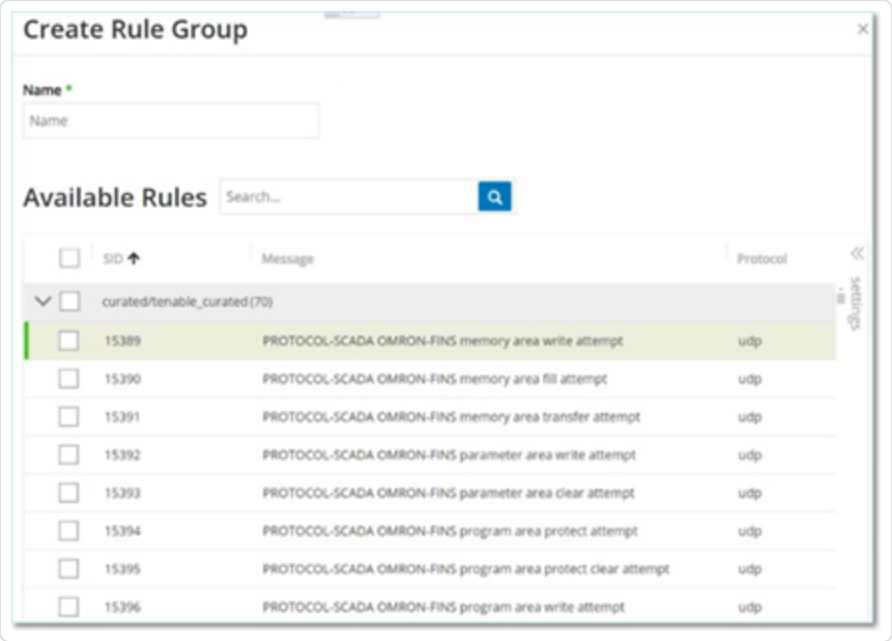
Parameter	Beschreibung
Name	Der Name zur Identifizierung der Gruppe.
Anzahl an Regeln	Die Anzahl der Regeln (SIDs), aus denen diese Regelgruppe besteht.
In Richtlinien verwendet	Zeigt die Richtlinien-ID jeder Richtlinie an, die diese Regelgruppe in ihrer Konfiguration verwendet. **Hinweis**: Um weitere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

Regelgruppen erstellen

So erstellen Sie eine neue Regelgruppe:

1. Klicken Sie auf **Regelgruppe erstellen**.

   Der Bereich **Regelgruppe erstellen** wird angezeigt.



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

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

4. Klicken Sie auf **Erstellen**.

   OT Security erstellt die neue Regelgruppe und zeigt sie in der Liste der Regelgruppen an. Sie können diese Gruppe jetzt beim Konfigurieren von Intrusion Detection-Richtlinien verwenden.

Aktionen für Gruppen

Wenn Sie eine Gruppe in einem der Gruppen-Bildschirme auswählen, 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. Siehe

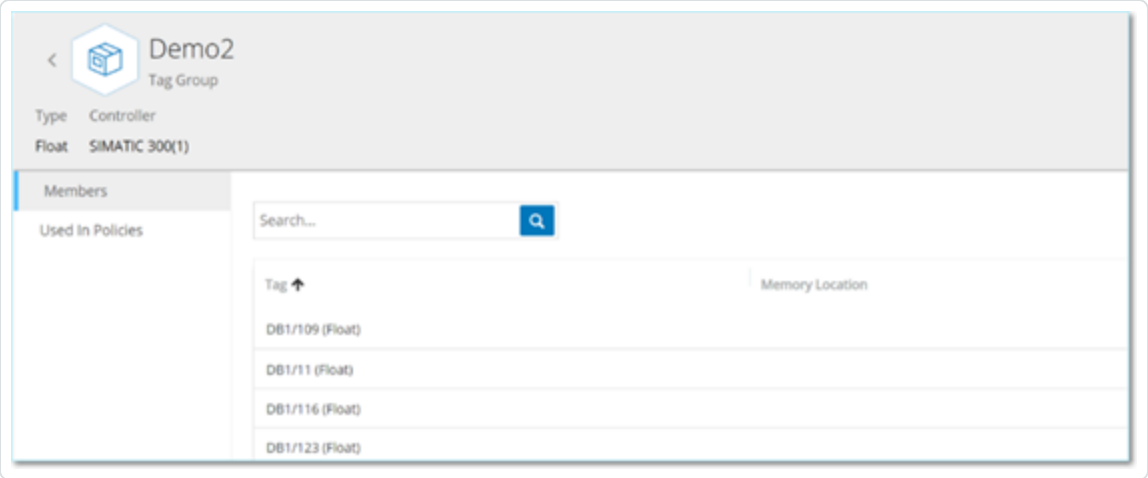
Gruppendetails anzeigen

- **Bearbeiten** – Hier können Sie die Details der Gruppe bearbeiten. Siehe Gruppe bearbeiten
- **Duplizieren** – Ermöglicht das Erstellen einer neuen Gruppe mit einer ähnlichen Konfiguration wie die angegebene Gruppe. Siehe Gruppe duplizieren
- **Löschen** – Ermöglicht das Löschen der Gruppe aus dem System. Siehe Gruppe löschen

> **Hinweis**: Sie können vordefinierte Gruppen nicht bearbeiten oder löschen. Einige vordefinierte Gruppen können auch nicht dupliziert werden. Sie können das Menü **Aktionen** auch aufrufen, indem Sie mit der rechten Maustaste auf eine Gruppe klicken.

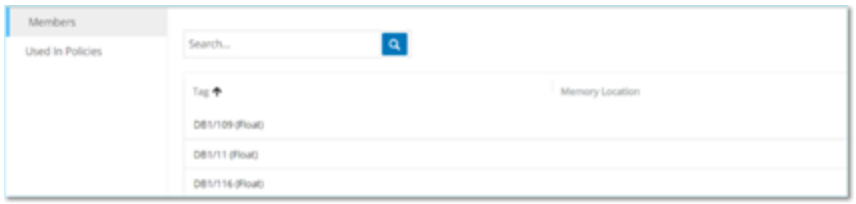
Gruppendetails anzeigen

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



Der Bildschirm **Gruppendetails** enthält eine Kopfleiste, die den Namen und Typ der Gruppe zeigt. Er hat zwei Registerkarten:

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

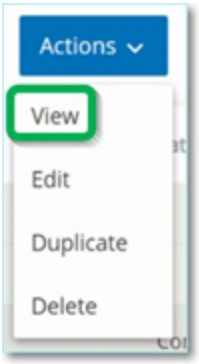


- **In Richtlinien verwendet** – Zeigt eine Liste für jede Richtlinie, für die die angegebene Gruppe als Richtlinienbedingung verwendet wird. Die Richtlinienliste enthält einen Umschalter zum Aktivieren/Deaktivieren der Richtlinie. Weitere Informationen finden Sie unter Richtlinien anzeigen.

So zeigen Sie Details einer Gruppe an:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Aktionen**.
   - Klicken Sie mit der rechten Maustaste auf die erforderliche Gruppe.

     Ein Menü wird angezeigt.
3. Wählen Sie **Anzeigen** aus.



   Der Bildschirm mit Gruppendetails wird angezeigt.

Gruppe bearbeiten

Sie können die Details einer bestehenden Gruppe bearbeiten.

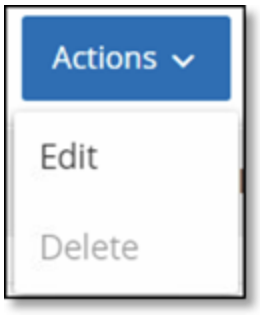
So bearbeiten Sie Details einer Gruppe:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Führen Sie einen der folgenden Schritte aus:

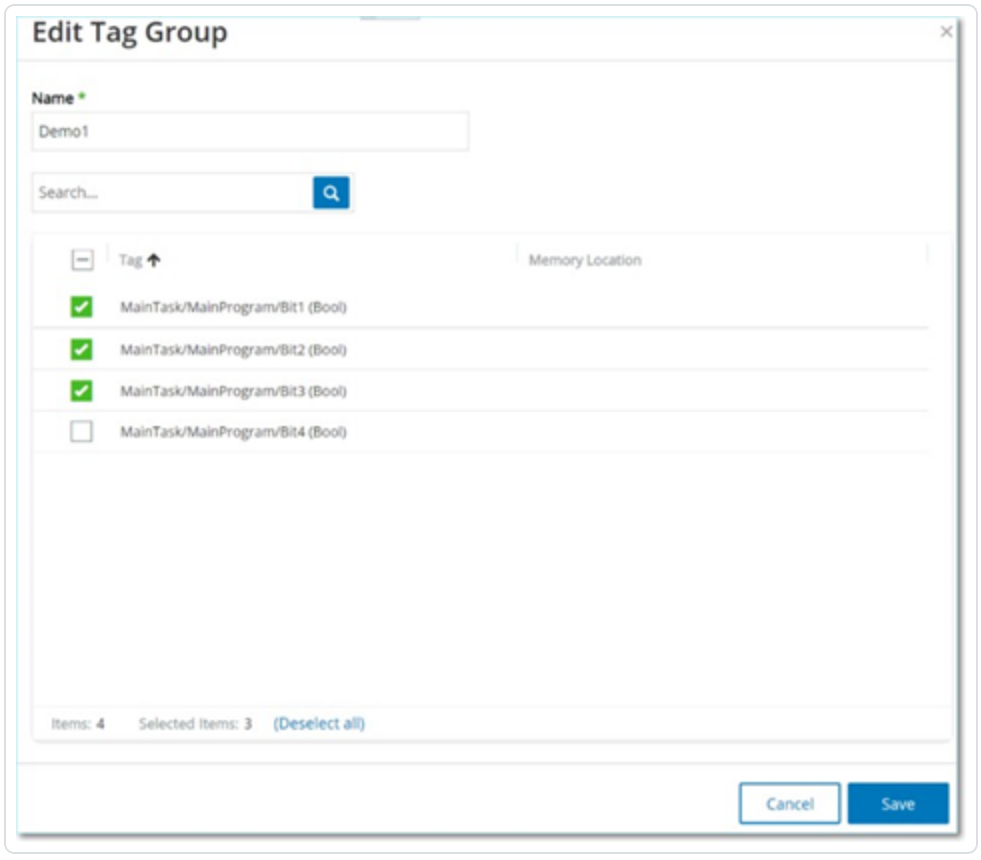
- Klicken Sie auf **Aktionen**.
- Klicken Sie mit der rechten Maustaste auf die erforderliche Gruppe.

  Ein Menü wird angezeigt.

3. Wählen Sie **Bearbeiten** aus.



4. Das Fenster **Gruppe bearbeiten** mit den relevanten Parametern für den angegebenen Gruppentyp wird angezeigt.



5. Ändern Sie die Parameter nach Bedarf.

6. Klicken Sie auf **Speichern**.

   OT Security speichert die Gruppe mit den neuen Einstellungen.

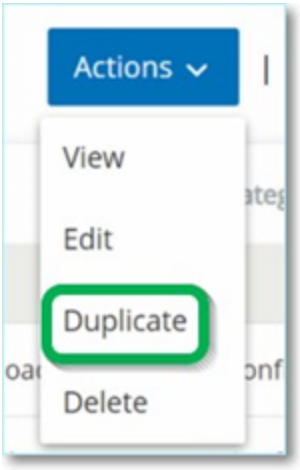
Gruppe duplizieren

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

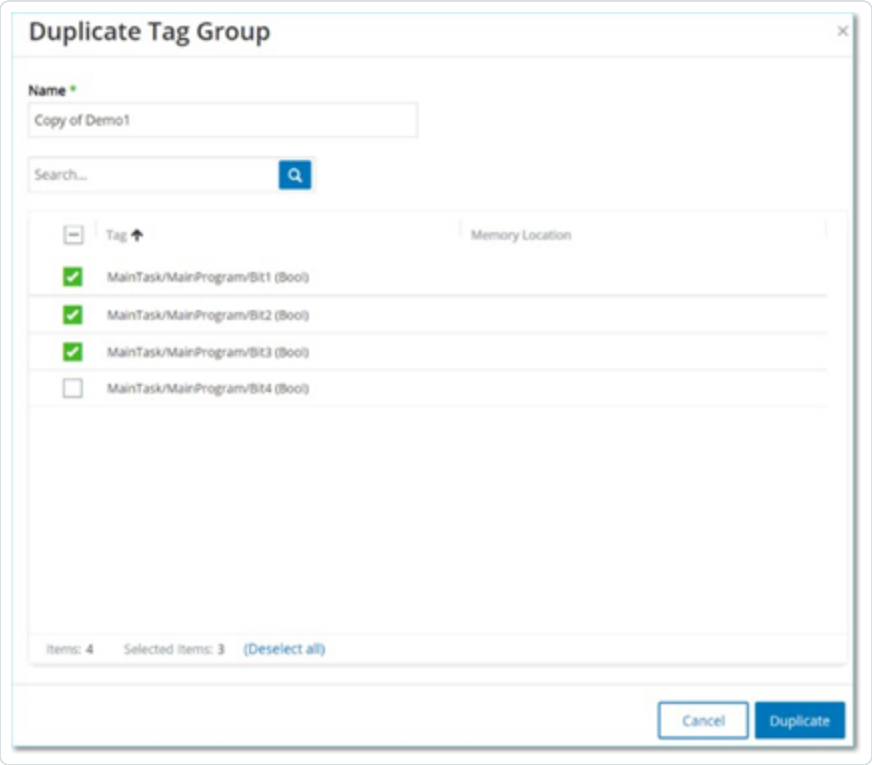
So duplizieren Sie eine Gruppe:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Wählen Sie die vorhandene Gruppe aus, auf der die neue Gruppe basieren soll.
3. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Aktionen**.
   - Klicken Sie mit der rechten Maustaste auf die erforderliche Gruppe.

     Ein Menü wird angezeigt.
4. Wählen Sie **Duplizieren** aus.



   Das Fenster **Gruppe duplizieren** mit den relevanten Parametern für den angegebenen Gruppentyp wird angezeigt.



5. Geben Sie im Feld **Name** einen Namen für die neue Gruppe ein. Standardmäßig heißt die neue Gruppe „Kopie von <Name der ursprünglichen Gruppe>“.
6. Nehmen Sie die gewünschten Änderungen an den Gruppeneinstellungen vor.
7. Klicken Sie auf **Duplizieren**.

   OT Security speichert die neue Gruppe zusätzlich zur vorhandenen Gruppe mit den neuen Einstellungen.

Gruppe löschen

Sie können benutzerdefinierte Gruppen löschen. Vordefinierte Gruppen können nicht gelöscht werden. Eine benutzerdefinierte Richtlinie, die als Richtlinienbedingung für eine oder mehrere Richtlinien verwendet wird, kann nicht gelöscht werden.

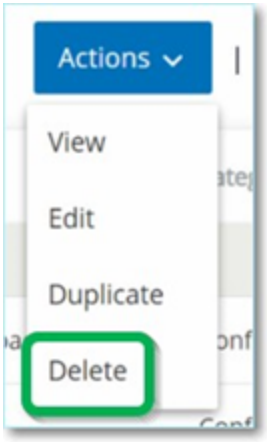
So löschen Sie eine Gruppe:

1. Wählen Sie unter **Gruppen** den gewünschten Gruppentyp aus.
2. Wählen Sie die Gruppe aus, die Sie löschen möchten.
3. Führen Sie einen der folgenden Schritte aus:

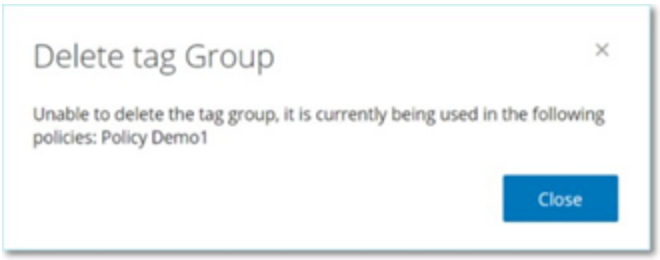
- Klicken Sie auf **Aktionen**.
- Klicken Sie mit der rechten Maustaste auf die erforderliche Gruppe.

  Ein Menü wird angezeigt.

4. Wählen Sie **Löschen** aus.



Daraufhin wird ein Bestätigungsfenster angezeigt.



5. Klicken Sie auf **Löschen**.

   OT Security löscht die Gruppe dauerhaft aus dem System.

Einstellungen

Der Abschnitt **Lokale Einstellungen** in OT Security enthält die meisten Konfigurationsseiten für OT Security. Die folgenden Seiten sind unter **Lokale Einstellungen** verfügbar:

Aktive Abfragen – Abfragefunktionen aktivieren/deaktivieren und ihre Frequenz und Einstellungen anpassen. Siehe Aktive Abfragen

Sensoren – Sensoren anzeigen und verwalten, eingehende Sensor-Kopplungsanforderungen genehmigen oder löschen und aktive Abfragen konfigurieren, die von Sensoren durchgeführt werden. Siehe Sensoren.

Systemkonfiguration

- **Gerät** – Gerätedetails und Netzwerkinformationen anzeigen und bearbeiten. Zum Beispiel Systemzeit, automatisches Ausloggen (d. h. Zeitüberschreitung bei Inaktivität).

  > **Hinweis**: Sie können DNS-Server in Tenable Core konfigurieren. Weitere Informationen finden Sie unter Manually Configure a Static IP Address im Tenable Core + Tenable OT Security Benutzerhandbuch.

- **Portkonfiguration** – Konfiguration der Ports auf dem Gerät anzeigen. Weitere Informationen zur Portkonfiguration finden Sie unter 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 Systemkonfiguration.
- **API-Schlüssel** – API-Schlüssel generieren, um Apps von Drittanbietern den Zugriff auf OT Security 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. Sie müssen ihn zur späteren Verwendung an einem sicheren Ort speichern. Siehe API-Schlüssel generieren.
- **Lizenz** – Ihre 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. Siehe Überwachte Netzwerke.
  - **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. Siehe Umgebungs.

  Hinweis: Maximal können 128 IP-Bereiche an den Tenable Network Monitor gesendet werden, daher empfiehlt Tenable, diese Grenze nicht zu überschreiten. Zusätzlich zu den angegebenen IP-Bereichen werden alle Hosts in den Subnetzen der OT Security-Plattform oder alle Geräte, die Aktivitäten ausführen, als Asset eingestuft.

  - **Ausgeblendete Assets** – Eine Liste der ausgeblendeten Assets im System anzeigen. Dies sind Assets, die aus den Asset-Listen entfernt wurden, siehe Inventar. Sie können ausgeblendete Assets über diese Seite wiederherstellen.
  - **Benutzerdefinierte Felder** – Benutzerdefinierte Felder erstellen, um Assets mit relevanten Informationen zu taggen. Ein benutzerdefiniertes Feld kann Klartext oder ein Link zu einer externen Ressource sein.
  - **Ereigniscluster** – Mehrere ähnliche Ereignisse, die innerhalb eines bestimmten Zeitraums auftreten, zusammenfassen, um ihre Überwachung zu vereinfachen. Siehe Ereigniscluster.
  - **PCAP-Player** – Eine PCAP-Datei mit aufgezeichneter Netzwerkaktivität hochladen und auf OT Security „abspielen“, wobei die Daten in Ihr System geladen werden. Siehe Umgebungs.
- **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 Benutzerverwaltung.
- **Benutzergruppen** – Ein Administratorbenutzer kann Benutzergruppen anzeigen, bearbeiten, hinzufügen und löschen. Siehe Benutzerverwaltung.
- **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 Benutzerverwaltung.

- **Integrationen** – Integration mit anderen Plattformen einrichten. OT Security unterstützt derzeit die Integration in Palo Alto Networks Next Generation Firewall (NGFW) und Aruba ClearPass sowie in andere Tenable-Produkte (Tenable Security Center und Tenable Vulnerability Management). Siehe Integrationen.
- **Server** – In Ihrem System konfigurierte Server anzeigen, erstellen und bearbeiten. Es sind separate Bildschirme für Folgendes verfügbar:
  - **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 OT Security-FortiGate-Integration können Sie auf der Grundlage der OT Security-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 OT Security Appliance zu sichern (mit Ausnahme von Paketerfassungsdaten). Informationen zum Wiederherstellen des Systems aus einer Sicherungsdatei finden Sie unter Manual Restore of a OT Security Backup. Während des Sicherungsvorgangs ist OT Security für Benutzer nicht verfügbar.
  - **Einstellungen exportieren** – Exportiert die Konfigurationseinstellungen der OT Security-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

OT Security-Plattform.

- **Einstellungen importieren** – Importiert die Konfigurationseinstellungen der OT Security-Plattform, die als `NDG`-Datei auf dem lokalen Computer gespeichert wurden.
- **Diagnosedaten herunterladen** – Erstellt eine Datei mit Diagnosedaten auf der OT Security-Plattform und speichert sie auf dem lokalen Computer.
- **Neu starten** – Startet die OT Security-Plattform neu. Dies ist für die Aktivierung bestimmter Konfigurationsänderungen erforderlich.
- **Deaktivieren** – Deaktiviert alle Überwachungsaktivitäten. Sie können die Überwachungsaktivitäten jederzeit wieder aktivieren.
- **Herunterfahren** – Fährt die OT Security-Plattform herunter. Drücken Sie zum Einschalten die Power-Taste auf der OT Security Appliance.
- **Auf Werkseinstellungen zurücksetzen** – Setzt alle Einstellungen auf die standardmäßigen Werkseinstellungen zurück.

  Achtung: Dieser Vorgang kann nicht rückgängig gemacht werden und alle Daten im System gehen verloren.

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

Sensoren

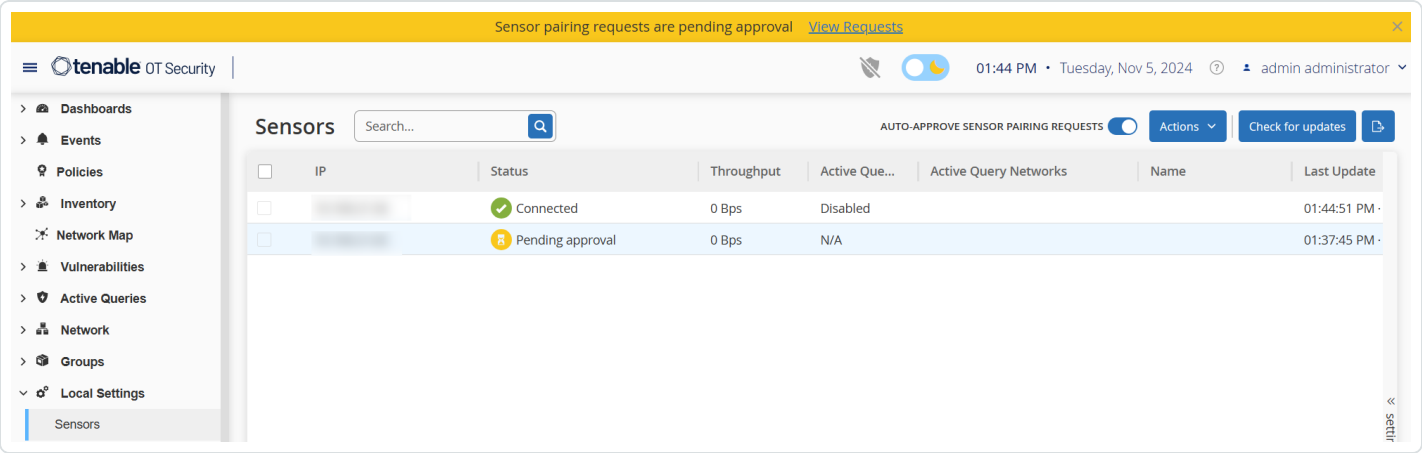
Nachdem Sensoren über die Tenable Core-Benutzeroberfläche gekoppelt wurden, können Sie neue Kopplungen genehmigen und Sensoren anzeigen und mit den Funktionen **Bearbeiten**, **Anhalten** und **Löschen** im Menü **Aktionen** verwalten. Sie können auch die automatische Genehmigung von Sensorkopplungsanforderungen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

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

Hinweis: Sie können eine unbegrenzte Anzahl von Sensoren mit ICP koppeln, aber das kombinierte SPAN-Traffic-Gesamtvolumen (Switched Port Analyzer) pro Appliance ist begrenzt. Sie können beispielsweise 10 Sensoren verwenden, von denen jeder zwischen 10 Mbit/s und 20 Mbit/s überträgt, aber der Gesamt-Traffic darf den ICP-Grenzwert nicht überschreiten. Weitere Informationen finden Sie im Abschnitt zu System- und Lizenzanforderungen im Benutzerhandbuch für Tenable Core und OT Security.

Sensoren anzeigen

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



Die Sensortabelle enthält die folgenden Details:

Parameter	Beschreibung
IP	Die IPv4-Adresse des Sensors.
Status	Der Status des Sensors: **Verbunden**, **Verbunden (nicht authentifiziert)**, **Genehmigung ausstehend**, **Getrennt** oder **Angehalten**. **Wichtig**: Nach der Kopplung wird für alle Sensoren der Status **Angehalten**angezeigt. • So ändern Sie den Status für authentifizierte Sensoren: Klicken Sie in OT Security mit der rechten Maustaste auf die Sensoren und aktivieren Sie diese, indem Sie den Status von **Angehalten** in **Verbunden** ändern. • So ändern Sie den Status für nicht authentifizierte

	Sensoren: Navigieren Sie in Tenable Core und OT Security Sensor zum Abschnitt **OT Security Sensor** > **Kopplungsinfo** und klicken Sie dann auf **Resume Data Transfer** (Datenübertragung wiederaufnehmen), um den **Verbindungsstatus** zu ändern.
Aktive Abfragen	Die Fähigkeit des Sensors, aktive Abfragen zu senden: **Aktiviert**, **Deaktiviert** oder **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).

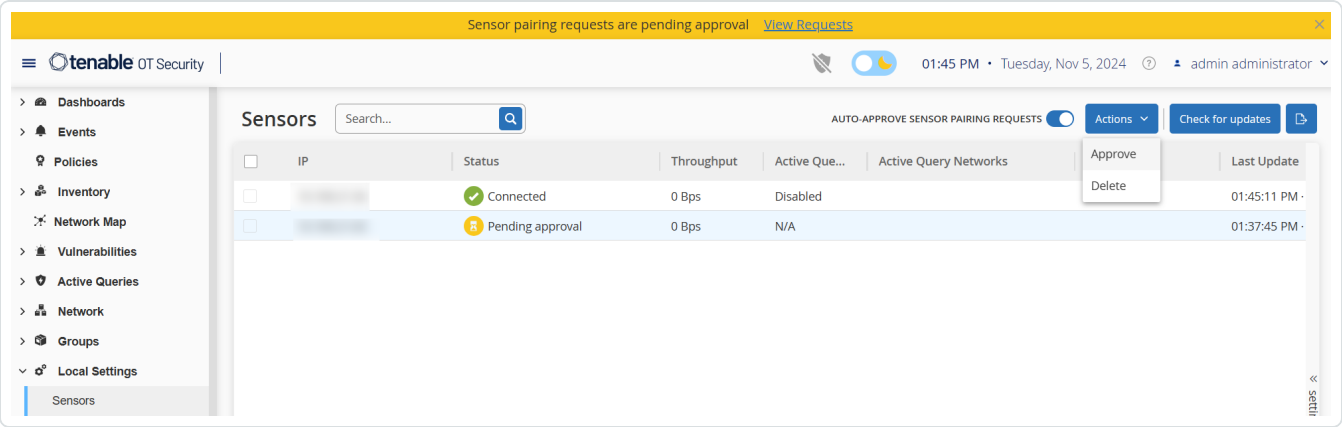
Eingehende Sensorkopplungsanforderung manuell genehmigen

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 zu **Lokale Einstellungen** > **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** aus.



> **Hinweis**: Um einen Sensor zu löschen, klicken Sie auf **Aktionen** > **Löschen** oder klicken Sie mit der rechten Maustaste und wählen Sie **Löschen** aus.

Aktive Abfragen konfigurieren

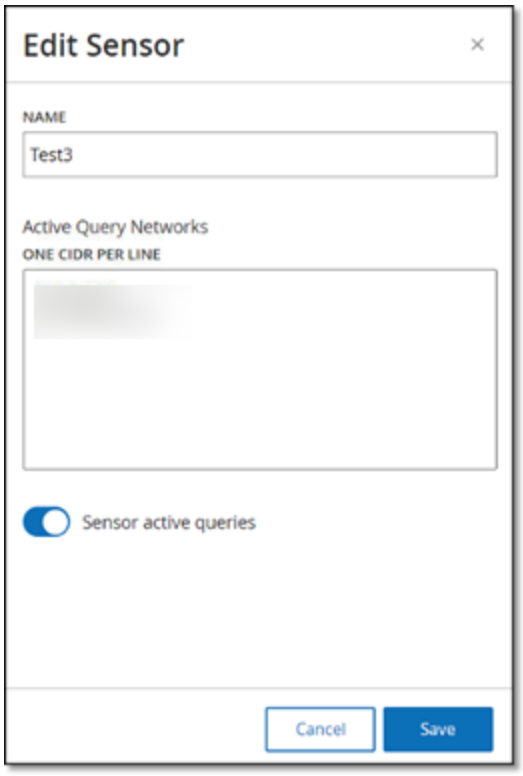
Sobald ein Sensor im authentifizierten Modus verbunden ist, kann er so konfiguriert werden, dass er aktive Abfragen in den Netzwerksegmenten durchführt, denen er zugewiesen ist. Sie müssen angeben, welche Netzwerksegmente abgefragt werden.

> **Hinweis**: Sensoren führen unabhängig von dieser Konfiguration eine passive Netzwerkerkennung in allen verfügbaren Segmenten durch.

So konfigurieren Sie aktive Abfragen:

1. Klicken Sie in der Tabelle auf eine Zeile mit dem Status **Verbunden**.
2. Klicken Sie auf **Aktionen** > **Bearbeiten** oder klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten** aus.

   Das Fenster **Sensor bearbeiten** wird angezeigt.



3. Um den Sensor umzubenennen, bearbeiten Sie den Text im Feld **Name**.
4. 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.

   Hinweis: Abfragen können nur für CIDRs durchgeführt werden, die in den überwachten Netzwerkbereichen enthalten sind. Stellen Sie sicher, dass Sie nur CIDRs hinzufügen, auf die über diesen Sensor zugegriffen werden kann. Das Hinzufügen nicht zugänglicher CIDRs kann sich auf die Abfragemöglichkeiten der ICP über andere Mittel auswirken.
5. Klicken Sie auf den Umschalter **Aktive Sensorabfragen**, um aktive Abfragen zu aktivieren.
6. Klicken Sie auf **Speichern**.

   Das Fenster wird geschlossen. In der Tabelle **Sensoren** wird in der Spalte **Aktive Abfragen** für die aktivierten Sensoren jetzt **Aktiviert** angezeigt.

Sensoren aktualisieren

Ab Version 3.16 erhält OT Security Sensor Software- und Sicherheitsupdates von der ICP, die für die Verwaltung zuständig ist. Sobald ein Sensor mit Authentifizierung gekoppelt ist, ist er darauf angewiesen, dass ihm alle erforderlichen Betriebssystem- und Softwareupdates von der Site bereitgestellt werden. Der Sensor muss nur OT Security erreichen, um Softwareupdates zu empfangen. In OT Security können Sie alle Ihre Sensoren über die zentrale Seite **Sensoren** aktualisieren.

Hinweis: OT Security verwendet die Offline-ISO für die zentralisierten Updates. Um alle authentifizierten Sensoren, die an eine ICP angeschlossen sind, zentral zu aktualisieren, platzieren Sie die Offline-ISO für die ICP/den Sensor unter `/srv/tenablecore/offlineiso/tenable-offline-updates.iso` auf der ICP.

Wenn der Sensor aktualisiert werden muss, erhalten Sie in folgenden Situationen eine Warnung:

- Beim Start.
- Beim Abschluss der Kopplung zwischen Sensor und ICP.
- Bei einer periodischen Prüfung.
- Bei Verwendung der Option **Nach Aktualisierungen suchen**.

Hinweis: Die Kopplung des Sensors mit OT Security muss mit Authentifizierung erfolgen, um Remote-Sensoren aktualisieren zu können. Weitere Informationen zum Koppeln finden Sie unter Koppeln von Sensoren mit der ICP.

So aktualisieren Sie einen authentifizierten Sensor der Version 3.16 oder höher mit der ICP:

1. Überprüfen Sie die Spalte **Version**, um festzustellen, ob die Version auf dem neuesten Stand ist oder ob ein Update erforderlich ist.
2. Wenn die Version aktualisiert werden muss, gehen Sie wie folgt vor:

   So aktualisieren Sie einen einzelnen Sensor:

   - Klicken Sie mit der rechten Maustaste auf den gewünschten Sensor und wählen Sie **Aktualisieren** aus.
   - Aktivieren Sie das Kontrollkästchen neben dem gewünschten Sensor und wählen Sie dann im Menü **Aktionen** die Option **Aktualisieren** aus.

   So aktualisieren Sie mehrere Sensoren:

- Wählen Sie einen oder mehrere Sensoren aus, für die ein Update erforderlich ist, und wählen Sie dann im Menü **Aktionen** die Option **Aktualisieren** aus.

OT Security aktualisiert die ausgewählten Sensoren.

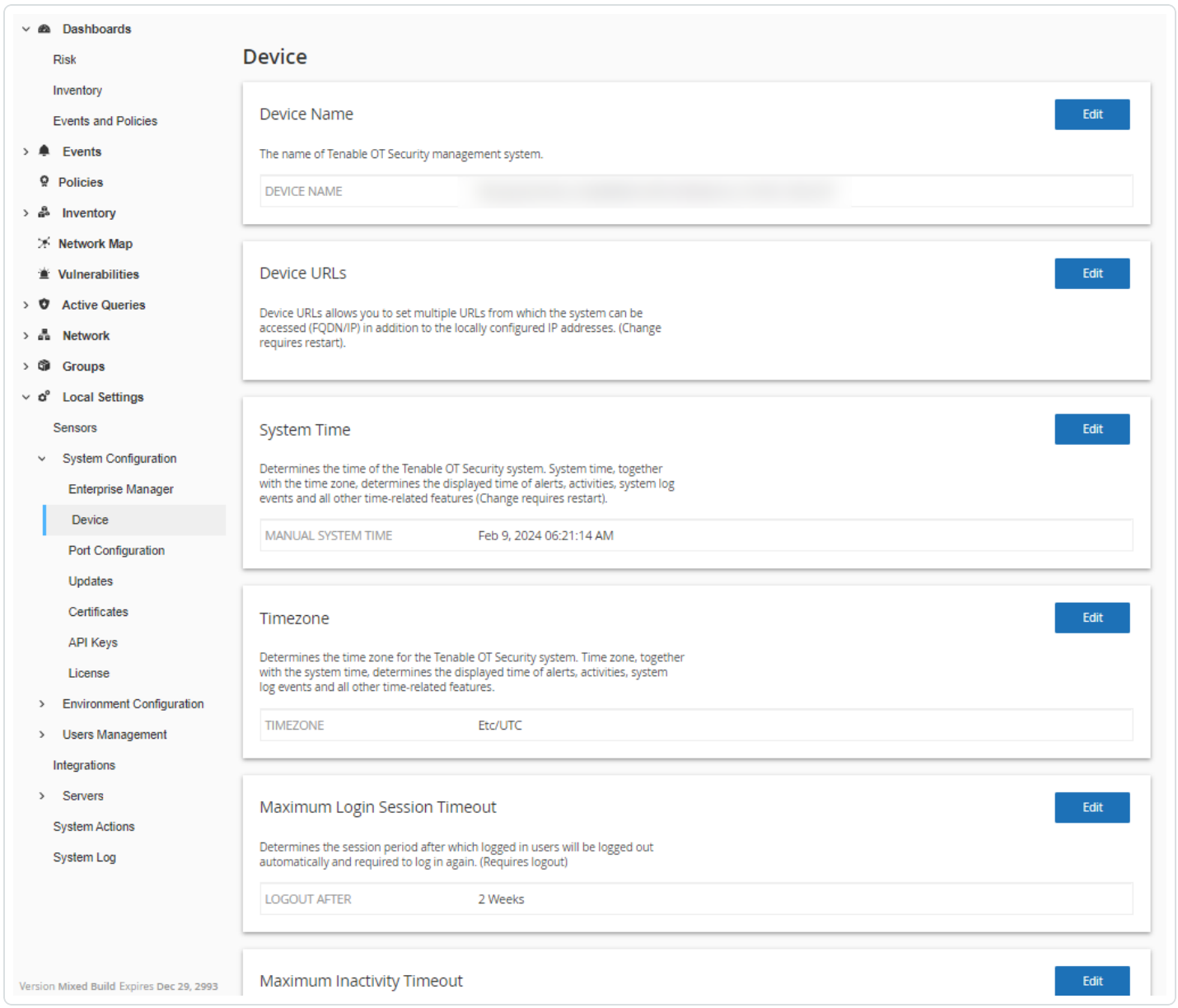
Hinweis: Während des Updates ist der Sensor möglicherweise nicht verfügbar.

Systemkonfiguration

Die Seiten zur **Systemkonfiguration** von OT Security 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

Die Seite **Gerät** enthält detaillierte Informationen zu Ihrer OT Security-Konfiguration. Sie können auf dieser Seite die Konfiguration anzeigen und bearbeiten.



Gerätename

Ein eindeutiger Bezeichner für die OT Security Appliance.

Geräte-URLs

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

Wichtig: 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 automatisch eingestellt, können jedoch bearbeitet werden.

Hinweis: 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 Standorts aus der Dropdown-Liste aus. Um die Zeitzone zu ändern, klicken Sie auf **Bearbeiten**.

Maximales Timeout von Login-Sitzung

Der Sitzungszeitraum, nach dem Benutzer automatisch ausgeloggt werden und sich erneut einloggen müssen. Um den Timeout-Zeitraum für die Login-Sitzung zu ändern, klicken Sie auf **Bearbeiten**. Verfügbare Optionen für den Zeitraum: 2 Wochen, 30 Minuten, 1Stunde, 4 Stunden, 12 Stunden, 1Tag, 1Woche und 2 Wochen.

Maximales Timeout bei Inaktivität

Der Inaktivitätszeitraum, nach dem eingeloggte Benutzer automatisch ausgeloggt werden und sich erneut einloggen müssen. Um den Inaktivitätszeitraum zu ändern, klicken Sie auf **Bearbeiten**.

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 Inventar.

Ping-Anfragen

Durch Aktivieren von Ping-Anfragen wird die automatische Antwort der OT Security-Plattform auf Ping-Anfragen aktiviert.

Klicken Sie auf den Umschalter **Ping-Anfragen**, um Ping-Anfragen zu aktivieren.

Paketerfassung

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 überschreitet, löscht das System ältere Dateien. Sie können verfügbare Dateien auf der Seite **Netzwerk** > **Paketerfassungen** anzeigen und herunterladen, siehe Abschnitt Netzwerk.

Klicken Sie auf den Umschalter **Paketerfassung**, um Paketerfassungen zu aktivieren.

> **Hinweis**: Sie können die Paketerfassungsfunktion jederzeit beenden, 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.

Klicken Sie auf den Umschalter **Sensorkopplungsanforderungen automatisch genehmigen**, um die automatische Genehmigung für eingehende Sensorkopplungsanforderungen zu aktivieren.

Nutzungsstatistiken aktivieren

Mit der Option **Nutzungsstatistiken aktivieren** wird festgelegt, ob Tenable anonyme Telemetriedaten über Ihre OT Security-Bereitstellung erfasst. 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 OT Security-Versionen zu verbessern sowie für andere angemessene Geschäftszwecke in Übereinstimmung mit dem Tenable-Rahmenvertrag. Diese Einstellung ist standardmäßig aktiviert.

Klicken Sie auf den Umschalter **Nutzungsstatistiken aktivieren**, um die Erfassung von Telemetriedaten zu aktivieren.

> **Hinweis**: Sie können das Teilen von Nutzungsstatistiken jederzeit deaktivieren, indem Sie auf den Umschalter klicken.

GraphQL Playground

Eine browserinterne GraphQL-IDE. Mit diesem Umschalter können Sie die Verwendung des Playgrounds in der Produktion aktivieren oder deaktivieren, um Ihre API-Abfragen zu testen.

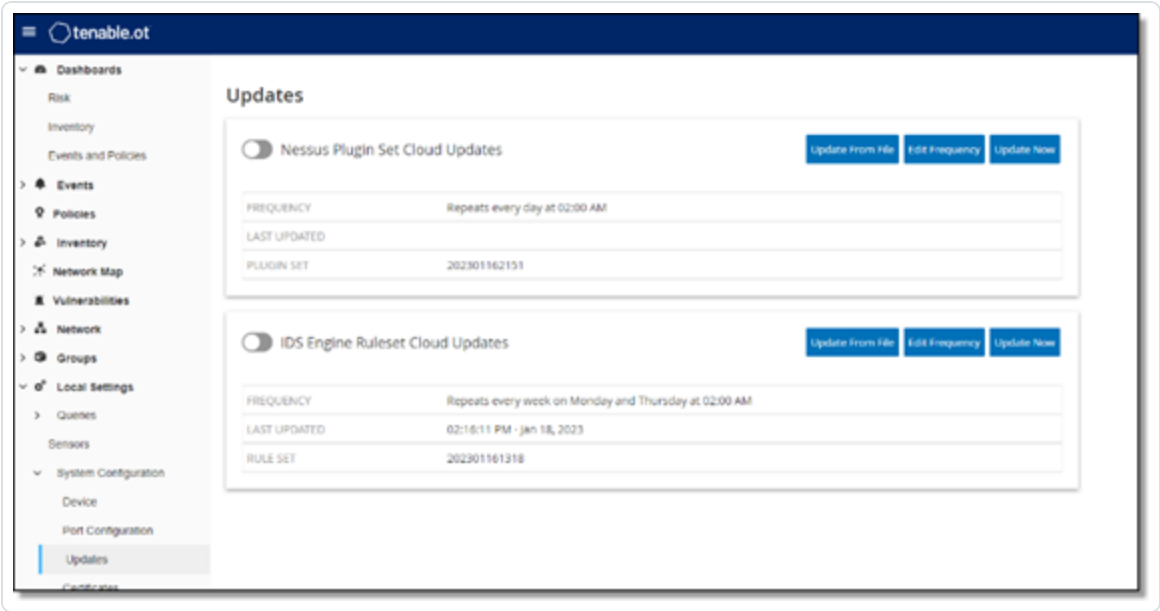
Portkonfiguration

Auf der Seite **Portkonfiguration** wird die Konfiguration der Ports des Geräts angezeigt. Weitere Informationen zur Portkonfiguration finden Sie unter Gerät.

Updates

Durch die Aktualisierung von Tenable Nessus-Plugins und des Regelsatzes der IDS-Engine (Intrusion Detection System) auf die neuesten Versionen wird sichergestellt, dass OT Security Ihre Assets auf die neuesten bekannten Schwachstellen überwacht. Sie können Updates über die Cloud – sowohl automatisch als auch manuell – und auch offline durchführen.

Hinweis: Informationen zum Aktualisieren von Tenable Core finden Sie unter Updates verwalten im Benutzerhandbuch für Tenable Core und OT Security.



Hinweis: Sie können Updates auch unter **Schwachstellen** > **Plugins aktualisieren** vornehmen.

Hinweis: Wenn die Benutzerlizenz abläuft, wird die Option zum Herunterladen neuer Updates blockiert und Plugins können nicht aktualisiert werden.

Updates des Tenable Nessus-Plugin-Satzes

Automatische Cloud-Updates von Plugins festlegen

Wenn Sie über eine Internetverbindung verfügen, können Sie Plugins über die Cloud aktualisieren. Wenn Sie automatische Updates aktivieren, werden Plugins zu der von Ihnen festgelegten Zeit und in der festgelegten Frequenz aktualisiert (Standard: täglich um 02:00 Uhr).

So aktivieren Sie automatische Updates von Plugins:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Das Fenster **Updates** wird angezeigt. Im Bereich **Cloud-Updates für Nessus-Plugin-Satz** werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf den Umschalter **Cloud-Updates für Nessus-Plugin-Satz**, um automatische Updates zu aktivieren.

Frequenz von Plugin-Updates bearbeiten

So bearbeiten Sie den Zeitplan für automatische Updates von Plugins:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Das Fenster **Updates** wird angezeigt. Im Bereich **Cloud-Updates für Nessus-Plugin-Satz** werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf **Frequenz bearbeiten**.

   Der Seitenbereich **Frequenz bearbeiten** wird angezeigt.

3. Legen Sie im Abschnitt **Wiederholung alle** das Zeitintervall fest, in dem Sie die Plugins aktualisieren möchten, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) im Dropdown-Feld auswählen.

   Bei Auswahl von **Wochen** wählen Sie die Wochentage aus, an denen Sie ein wöchentliches Update der Plugins durchführen möchten.

4. Legen Sie im Abschnitt **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.

5. Klicken Sie auf **Speichern**.

   Es wird eine Meldung mit der Bestätigung angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Manuelle Cloud-Updates von Plugins durchführen

So aktualisieren Sie Plugins manuell:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Die Seite **Updates** wird angezeigt. Im Bereich **Cloud-Updates für Nessus-Plugin-Satz** werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf **Jetzt aktualisieren**.

   In einer Meldung wird bestätigt, dass die Aktualisierung ausgeführt wird. Wenn das Update abgeschlossen ist, wird im Feld **Plugin-Satz** die Nummer des aktuellen Plugin-Satzes angezeigt.

   > **Tipp**: Lassen Sie das Browserfenster geöffnet und aktualisieren Sie die Seite nicht, während das Update des **Plugin-Satzes** durchgeführt wird.

Offline-Updates

Sollten Sie auf Ihrem OT Security-Gerät nicht über eine Internetverbindung verfügen, können Sie die Plugins manuell aktualisieren, indem Sie den neuesten Plugin-Satz aus dem Tenable Community-Portal herunterladen und die Datei hochladen.

So aktualisieren Sie Plugins offline:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Die Seite **Updates** wird angezeigt. Im Bereich **Cloud-Updates für Nessus-Plugin-Satz** werden die Nummer Ihres Plugin-Satzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf **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.

   Hinweis: 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 OT Security-Kundenportal heruntergeladen haben.

5. Klicken Sie auf **Aktualisieren**.

Updates des IDS-Engine-Regelsatzes

Automatische Cloud-Updates des IDS-Engine-Regelsatzes festlegen

Wenn Sie über eine Internetverbindung verfügen, können Sie den IDS-Engine-Regelsatz über die Cloud aktualisieren. Wenn Sie automatische Updates aktivieren, kann der IDS-Engine-Regelsatz zu der von Ihnen festgelegten Zeit und mit der festgelegten Frequenz aktualisiert werden (Standard: Wiederholung jede Woche am Montag und Donnerstag um 02:00 Uhr).

So aktivieren Sie automatische Updates des IDS-Engine-Regelsatzes:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Die Seite **Updates** wird angezeigt. Im Bereich **Cloud-Updates für IDS-Engine-Regelsatz** werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf den Umschalter **Cloud-Updates für IDS-Engine-Regelsatz**, um automatische Updates zu aktivieren.

Frequenz von Updates des IDS-Engine-Regelsatzes bearbeiten

So bearbeiten Sie den Zeitplan für automatische Updates des IDS-Engine-Regelsatzes:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Die Seite **Updates** wird angezeigt. Im Bereich **Cloud-Updates für IDS-Engine-Regelsatz** werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf **Frequenz bearbeiten**.

   Der Seitenbereich **Frequenz bearbeiten** wird angezeigt.

3. Legen Sie im Abschnitt **Wiederholung alle** das Zeitintervall fest, in dem Sie den Regelsatz aktualisieren möchten, indem Sie eine Zahl eingeben und eine Zeiteinheit (Tage oder Wochen) im Dropdown-Feld auswählen.

   Bei Auswahl von **Wochen** wählen Sie die Wochentage aus, an denen Sie ein wöchentliches Update des Regelsatzes durchführen möchten.

4. Legen Sie im Abschnitt **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.

5. Klicken Sie auf **Speichern**.

   Es wird eine Meldung mit der Bestätigung angezeigt, dass die Frequenz erfolgreich aktualisiert wurde.

Manuelle Cloud-Updates des IDS-Engine-Regelsatzes durchführen

So aktualisieren Sie den IDS-Engine-Regelsatz manuell:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Die Seite **Updates** wird angezeigt. Im Bereich **Cloud-Updates für IDS-Engine-Regelsatz** werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf **Jetzt aktualisieren**.

   In einer Meldung wird bestätigt, dass die Aktualisierung ausgeführt wird. Wenn das Update abgeschlossen ist, wird im Feld **Regelsatz** die Nummer des aktuellen IDS-Engine-Regelsatzes angezeigt.

Offline-Updates

Sollten Sie auf Ihrem OT Security-Gerät nicht über eine Internetverbindung verfügen, können Sie Ihren IDS-Engine-Regelsatz manuell aktualisieren, indem Sie den neuesten Regelsatz aus dem Tenable-Kundenportal herunterladen und die Datei hochladen.

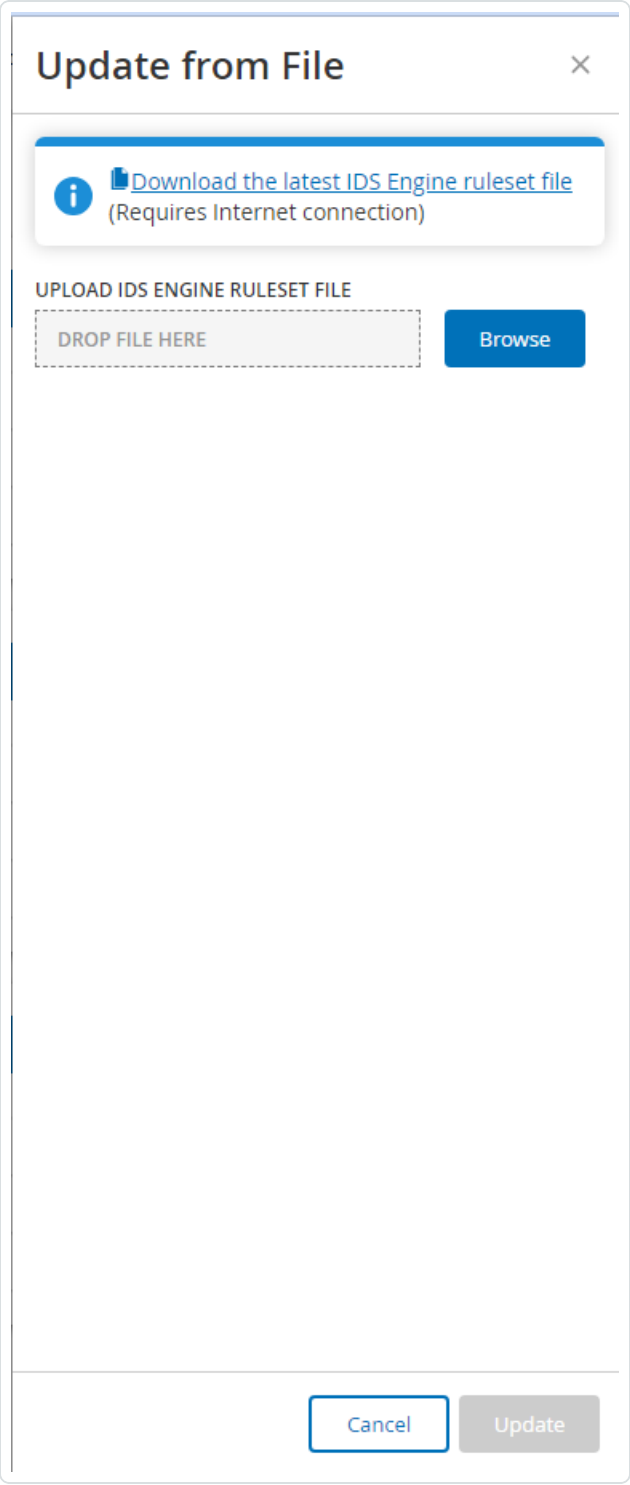
So aktualisieren Sie den IDS-Engine-Regelsatz offline:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Updates**.

   Das Fenster **Updates** wird angezeigt. Im Bereich **Cloud-Updates für IDS-Engine-Regelsatz** werden die Nummer Ihres Regelsatzes, das Datum der letzten Aktualisierung und der Update-Zeitplan angezeigt.

2. Klicken Sie auf **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.

Hinweis: 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 OT Security-Kundenportal heruntergeladen haben.
5. Klicken Sie auf **Aktualisieren**.

Zertifikate

HTTPS-Zertifikat generieren

Das HTTPS-Zertifikat stellt sicher, dass das System eine sichere Verbindung zur OT Security 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.

Hinweis: Wenn Sie ein neues Zertifikat generieren, wird das aktuelle Zertifikat überschrieben.

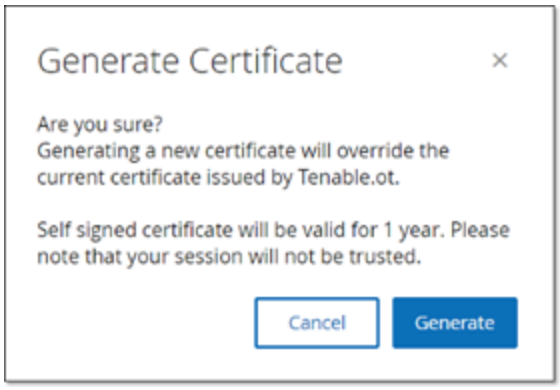
So generieren Sie ein selbstsigniertes Zertifikat:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Zertifikate**.

   Das Fenster **Zertifikate** wird angezeigt.

2. Wählen Sie im Menü **Aktionen** die Option **Selbstsigniertes Zertifikat generieren** aus.

   Das Bestätigungsfenster zum Generieren eines Zertifikats wird angezeigt.



3. Klicken Sie auf **Generieren**.

   OT Security generiert das selbstsignierte Zertifikat. Sie können es unter **Lokale Einstellungen** > **Systemkonfiguration** > **Zertifikat** einsehen.

HTTPS-Zertifikat hochladen

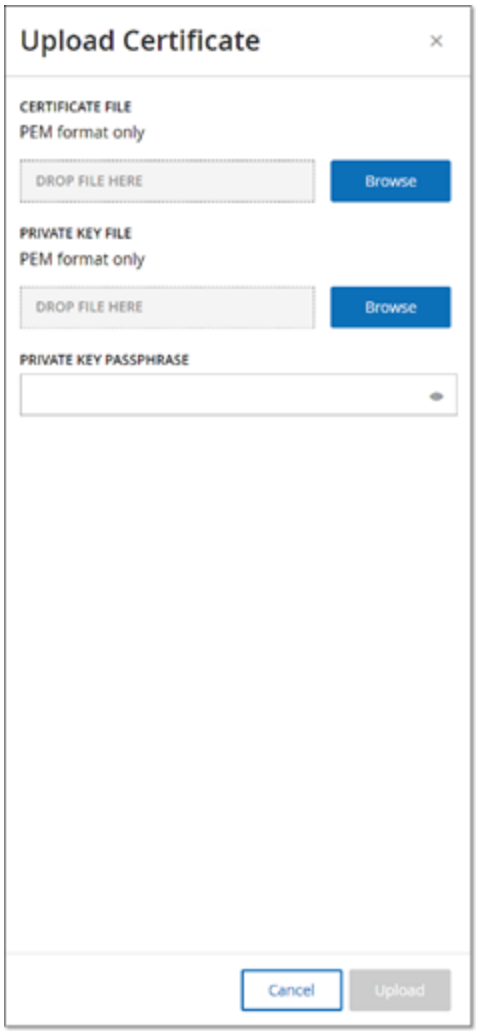
So laden Sie ein HTTPS-Zertifikat hoch:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **Zertifikate**.

   Das Fenster **Zertifikate** wird angezeigt.

2. Wählen Sie im Menü **Aktionen** die Option **Zertifikat hochladen** aus.

   Der Seitenbereich **Zertifikat hochladen** wird angezeigt.



3. Klicken Sie im Abschnitt **Zertifikatdatei** auf **Durchsuchen** und navigieren Sie zu der Zertifikatdatei, die Sie hochladen möchten.
4. Klicken Sie im Abschnitt **Datei mit privatem Schlüssel** auf **Durchsuchen** und navigieren Sie zu der Datei des privaten Schlüssels, die Sie hochladen möchten.
5. Geben Sie im Feld **Passphrase für privaten Schlüssel** die Passphrase des privaten Schlüssels ein.
6. Klicken Sie auf **Hochladen**, um die Dateien hochzuladen.

   Der Seitenbereich wird geschlossen.

   Hinweis: Nachdem Sie das Zertifikat ersetzt haben, empfiehlt Tenable, die Registerkarte des Browsers neu zu laden, um sich zu vergewissern, dass die Aktualisierung des HTTP-Zertifikats erfolgreich war. Wenn der Upload nicht erfolgreich ist, zeigt OT Security eine Warnmeldung an.

API-Schlüssel generieren

Die Generierung eines API-Schlüssels kann für die Integration von OT Security mit anderen Sicherheitstools und -systemen in Ihrer Organisation hilfreich sein.

So generieren Sie API-Schlüssel in OT Security:

1. Gehen Sie zu **Lokale Einstellungen** > **Systemkonfiguration** > **API-Schlüssel**.

   Die Seite **API-Schlüssel** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf **Schlüssel generieren**.

   Der Bereich **Schlüssel generieren** wird angezeigt.

3. Wählen Sie im Feld **Ablauffrist** die Anzahl Tage aus, nach denen der API-Schlüssel als veraltet gelten soll.

4. Geben Sie im Feld **Beschreibung** eine Beschreibung für den API-Schlüssel ein.

5. Klicken Sie auf **Generieren**.

   Der Bereich **Schlüssel generieren** wird zusammen mit der **ID** und dem **API-Schlüssel** angezeigt.

6. Klicken Sie auf die Schaltfläche , um den API-Schlüssel zu kopieren.

7. Klicken Sie auf **Fertig**.

   Die Seite **API-Schlüssel** mit der ID des neu hinzugefügten API-Schlüssels wird angezeigt.

Lizenz

Wenn Sie Ihre OT Security-Lizenz aktualisieren oder neu initialisieren müssen, wenden Sie sich an Ihren Tenable Account Manager. Sobald Ihr Tenable Account Manager Ihre Lizenz aktualisiert hat, können Sie Ihre Lizenz aktualisieren oder neu initialisieren. Weitere Informationen finden Sie im Lizenzaktivierung für OT Security.

Umgebungs

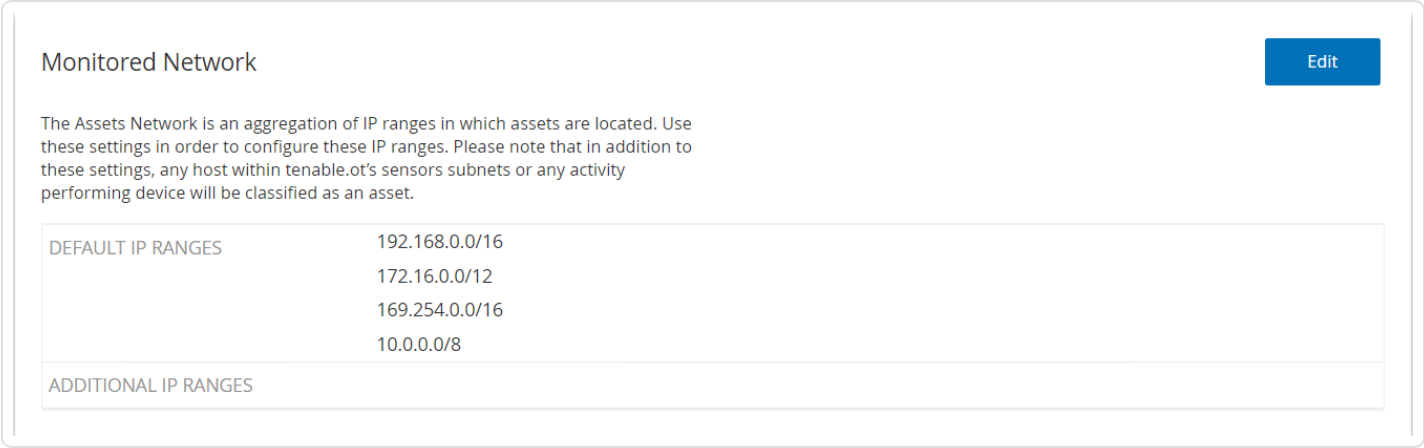
Die Seite umfasst die folgenden Abschnitte:

- Überwachte Netzwerke
- IP-Adresse für IoT-Assets abrufen

Überwachte Netzwerke

Die Konfiguration des überwachten Netzwerks enthält eine Reihe von IP-Bereichen (CIDRs/Subnetze), die die Überwachungsgrenzen für OT Security definieren. OT Security ignoriert Assets außerhalb der konfigurierten Bereiche.

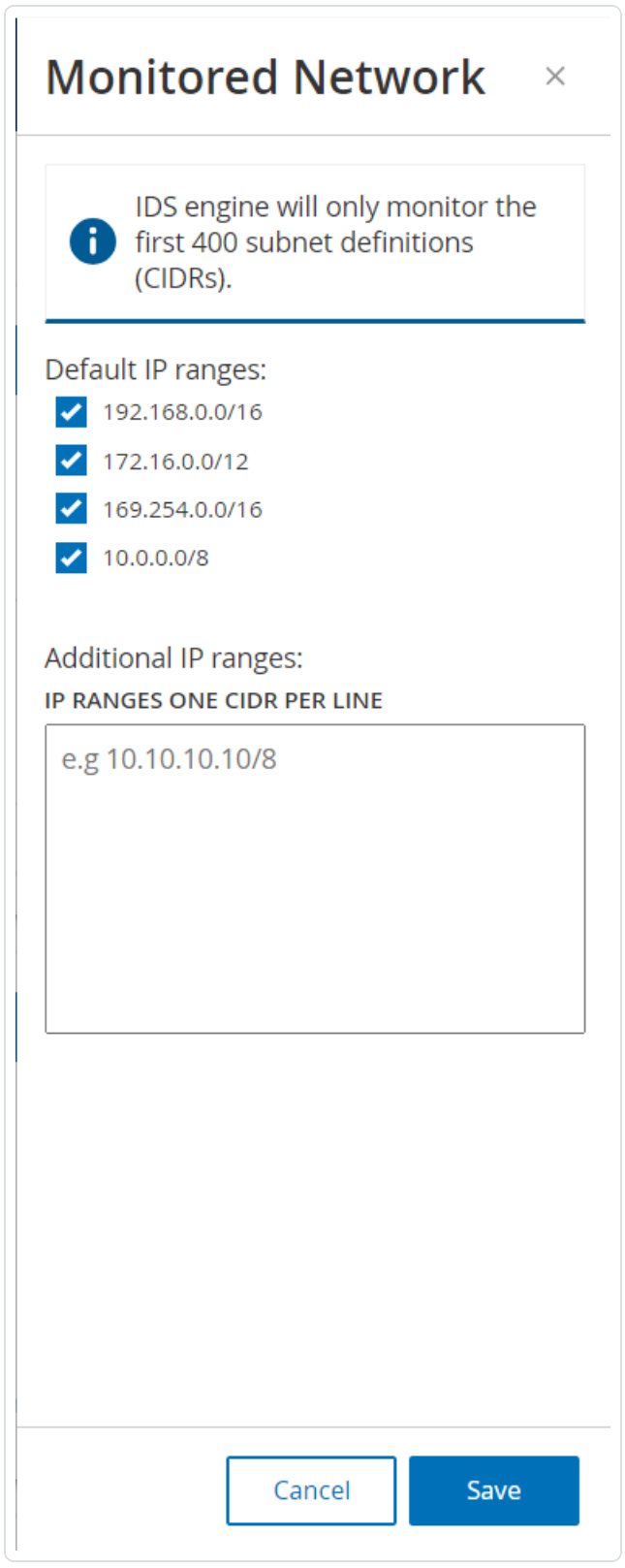
Standardmäßig konfiguriert OT Security drei öffentliche Standardbereiche: 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16 sowie den Link-Local-Bereich 169.254.0.0/16 (APIPA).



So deaktivieren Sie einen der Standardbereiche oder fügen für Ihr Netzwerk geeignete Bereiche hinzu:

1. Klicken Sie im Abschnitt **Überwachtes Netzwerk** auf **Bearbeiten**.

   Der Bereich **Überwachtes Netzwerk** wird angezeigt.


Monitored Network
IDS engine will only monitor the first 400 subnet definitions (CIDRs).
Default IP ranges:
192.168.0.0/16
172.16.0.0/12
169.254.0.0/16
10.0.0.0/8
Additional IP ranges:
IP RANGES ONE CIDR PER LINE
e.g 10.10.10.10/8
Cancel
Save

2. Wählen Sie die erforderlichen **Standard-IP-Bereiche** aus und/oder fügen Sie im Textfeld **Zusätzliche IP-Bereiche** entsprechende Einträge (ein IP-Bereich pro Zeile) hinzu.
3. Klicken Sie auf **Speichern**.

   OT Security speichert die Konfiguration des überwachten Netzwerks.

Ereigniscluster

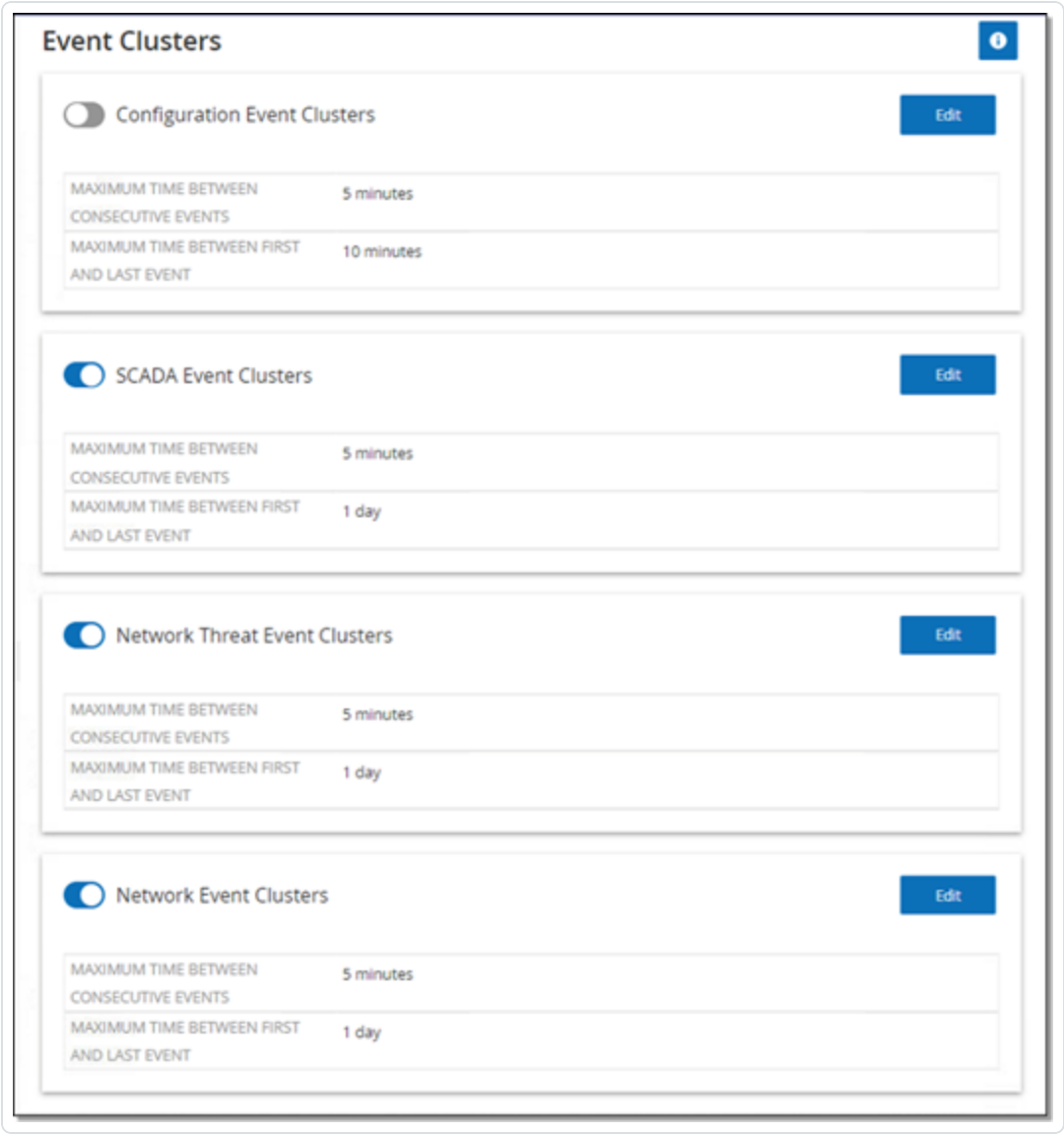
Um die Überwachung von Ereignissen zu vereinfachen, werden mehrere Ereignisse mit denselben Merkmalen in einem einzigen Cluster zusammengefasst. Das Clustering basiert auf dem Ereignistyp (d. h. Ereignisse, die dieselbe Richtlinie nutzen), Quell- und Ziel-Assets usw.

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 aufeinanderfolgende 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. Die Seite **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 **Bearbeiten**.

   Das Fenster **Konfiguration bearbeiten** wird angezeigt.
4. Geben Sie den gewünschten Zahlenwert in das Zahlenfeld ein und wählen Sie die Zeiteinheit über das Dropdown-Feld aus.

Hinweis: Weitere Informationen zu Clustering und Zeitintervallen können Sie über das Symbol aufrufen.

5. Klicken Sie auf **Speichern**.

Benutzerverwaltung

Der Zugriff auf die OT Security-Konsole wird über Benutzerkonten gesteuert, in denen die für den jeweiligen Benutzer verfügbaren Berechtigungen festgelegt sind. Die Berechtigungen des Benutzers werden durch die Benutzergruppen bestimmt, denen er zugewiesen 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 OT Security-Rollen auf der Grundlage Ihrer vorhandenen Gruppen in Active Directory zuweisen.
- **SAML** – Richten Sie eine Integration mit Ihrem Identitätsanbieter (z. B. Microsoft Entra ID) ein und weisen Sie Ihrer OT Security-Anwendung Benutzer zu.

Lokale Benutzer

Benutzergruppen

Benutzerrollen

Authentifizierungsserver

SAML

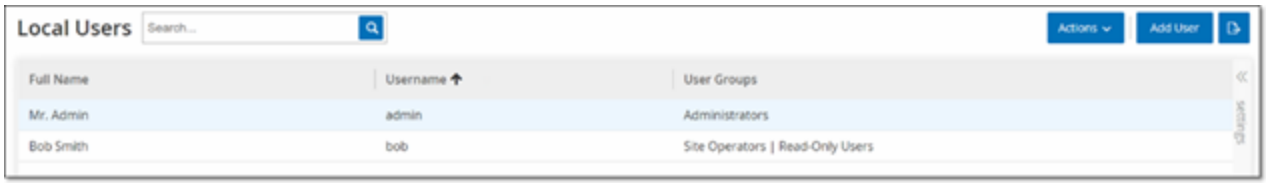
Lokale Benutzer

Ein Administratorbenutzer kann neue Benutzerkonten erstellen und vorhandene Konten bearbeiten. Jeder Benutzer wird einer oder mehreren Benutzergruppen zugewiesen, die die dem Benutzer zugewiesenen Rollen bestimmen.

Hinweis: Benutzer können Benutzergruppen entweder während der Erstellung oder der Bearbeitung des Benutzerkontos oder der Benutzergruppe hinzugefügt werden.

Lokale Benutzer anzeigen

Im Fenster **Lokale Benutzer** wird eine Liste aller lokalen Benutzer im System angezeigt.



Das Fenster **Lokale Benutzer** enthält die folgenden Details:

Parameter	Beschreibung
Vollständiger Name	Der vollständige Name des Benutzers.
Benutzername	Der Benutzername des Benutzers, der zum Einloggen verwendet wird.
Benutzergruppen	Die Benutzergruppen, denen der Benutzer zugewiesen ist.

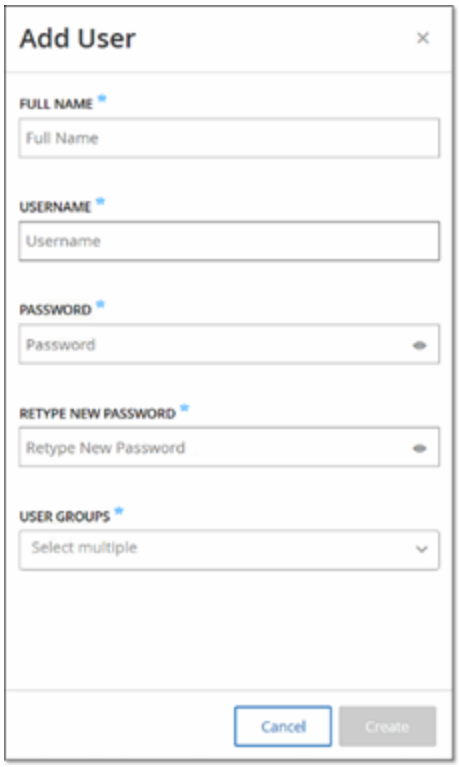
Lokale Benutzer hinzufügen

Sie können Benutzerkonten erstellen, um den Zugriff einzelner Benutzer auf das System zu autorisieren. Jeder Benutzer muss einer oder mehreren Benutzergruppen zugewiesen werden.

So erstellen Sie ein Benutzerkonto:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Lokale Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**.

   Daraufhin wird der Bereich **Benutzer hinzufügen** angezeigt.



3. Geben Sie im Feld **Vollständiger Name** den Vor- und Nachnamen ein.

   Hinweis: 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.

   Hinweis: Dies ist das Passwort, das der Benutzer beim ersten Login verwendet. Der Benutzer kann das Passwort im Fenster **Einstellungen** ändern, nachdem er sich beim System eingeloggt hat.

7. Aktivieren Sie im Dropdown-Feld **Benutzergruppen** das Kontrollkästchen für jede Benutzergruppe, der Sie diesen Benutzer zuweisen möchten.

   Hinweis: 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 Lokale Benutzer.

8. Klicken Sie auf **Erstellen**.

   OT Security erstellt das neue Benutzerkonto im System erstellt und fügt es der Liste der Benutzer unter **Lokale Benutzer** hinzu.

Zusätzliche Aktionen für Benutzerkonten

Benutzerkonto bearbeiten

Sie können einen Benutzer weiteren Benutzergruppen zuweisen oder den Benutzer aus einer Gruppe entfernen.

So ändern Sie die Benutzergruppen eines Benutzers:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Lokaler Benutzer**.

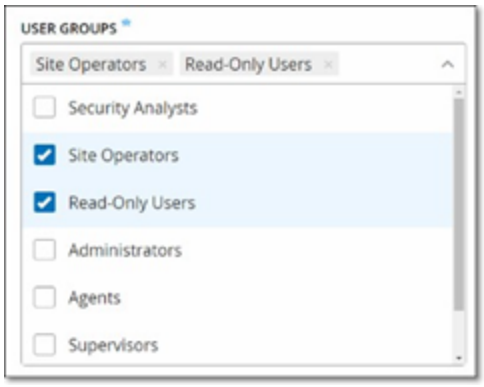
   Die Seite **Lokale Benutzer** wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer, und wählen Sie **Benutzer bearbeiten** aus.

   Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü **Aktionen** die Option **Benutzer bearbeiten** auswählen.

3. Der Bereich **Benutzer bearbeiten** wird angezeigt. Er zeigt die Benutzergruppen, denen der Benutzer zugewiesen ist.

4. Aktivieren bzw. deaktivieren Sie im Dropdown-Feld **Benutzergruppen** die gewünschten Benutzergruppen.



5. Klicken Sie auf **Speichern**.

Benutzerpasswort ändern

Hinweis: Mit diesem 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 zu **Einstellungen** > **Benutzerverwaltung** > **Lokaler Benutzer**.

   Die Seite **Lokale Benutzer** wird angezeigt.

2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer, und wählen Sie **Passwort zurücksetzen** aus.

   Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü **Aktionen** die Option **Passwort zurücksetzen** auswählen.

   Das Fenster **Passwort zurücksetzen** wird angezeigt.

3. Geben Sie im Feld **Neues Passwort** ein neues Passwort ein.
4. Geben Sie im Feld **Passwort erneut eingeben** das neue Passwort erneut ein.
5. Klicken Sie auf **Zurücksetzen**.

   OT Security wendet das neue Passwort auf das angegebene Benutzerkonto an.

Lokale Benutzer löschen

So löschen Sie ein Benutzerkonto:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Lokaler Benutzer**.

   Die Seite **Lokale Benutzer** wird angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Benutzer, und wählen Sie **Benutzer löschen** aus.

   > **Hinweis**: Alternativ können Sie einen Benutzer auswählen und dann im Menü **Aktionen** die Option **Benutzer löschen** auswählen.

   Daraufhin wird ein Bestätigungsfenster angezeigt.
3. Klicken Sie auf **Löschen**.

   OT Security löscht das Benutzerkonto aus dem System.

Benutzergruppen

Ein Administratorbenutzer kann neue Benutzergruppen erstellen und vorhandene Gruppen bearbeiten. Jeder Benutzer wird einer oder mehreren Benutzergruppen zugewiesen, die die dem Benutzer zugewiesenen Rollen 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

Auf der Seite „Benutzergruppen“ wird eine Liste aller Benutzergruppen im System angezeigt.

Die folgenden Details sind auf der Seite „Benutzergruppen“ verfügbar:

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 unter Tabelle der Benutzerrollen.

Benutzergruppen hinzufügen

Sie können neue Benutzergruppen erstellen und dieser Gruppe Benutzer zuweisen.

So erstellen Sie eine Benutzergruppe:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Benutzergruppen**.

   Der Bildschirm **Benutzergruppen** wird angezeigt.

2. Klicken Sie auf **Benutzergruppe erstellen**.

   Der Bereich **Benutzergruppe erstellen** wird angezeigt.

3. Geben Sie im Feld **Name** einen Namen für die Gruppe ein.
4. Wählen Sie im Dropdown-Feld **Rolle** in der Dropdown-Liste die Rolle aus, die Sie dieser Gruppe zuweisen möchten. Verfügbare Rollen sind:

   - Schreibgeschützt
   - Sicherheitsanalyst
   - Sicherheitsmanager

- Site-Operator
- Supervisor

5. Wählen Sie im Dropdown-Feld **Benutzer** einen oder mehrere Benutzer aus, die Sie dieser Gruppe zuweisen möchten.
6. Klicken Sie auf **Erstellen**.

   OT Security erstellt die neue Benutzergruppe und fügt sie der Liste der Gruppen hinzu, die im Bildschirm **Benutzergruppen** angezeigt werden.

Zusätzliche Aktionen für Benutzergruppen

Benutzergruppen bearbeiten

Sie können die Einstellungen bearbeiten und Mitglieder zu einer vorhandenen Benutzergruppe hinzufügen oder daraus entfernen, indem Sie die Gruppe bearbeiten.

Hinweis: Alternativ können Sie einen Benutzer auswählen und dann im Menü **Aktionen** die Option **Benutzer löschen** auswählen.

So bearbeiten Sie eine Benutzergruppe:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Benutzergruppen**.

   Der Bildschirm **Benutzergruppen** wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie mit der rechten Maustaste auf die gewünschte Benutzergruppe, und wählen Sie **Bearbeiten** aus.
   - Wählen Sie die Benutzergruppe aus, die Sie bearbeiten möchten. Das Menü **Aktionen** wird angezeigt. Wählen Sie **Aktionen** > **Bearbeiten** aus.

   Der Fensterbereich **Benutzergruppe bearbeiten** mit den Einstellungen der Gruppe wird angezeigt.
3. Ändern Sie den **Namen** und die **Rolle**. Sie können auch Benutzer aktivieren oder deaktivieren,

um Benutzer zur Gruppe hinzuzufügen oder daraus zu entfernen.

4. Klicken Sie auf **Speichern**.

Benutzergruppen löschen

Hinweis: 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 zu **Einstellungen** > **Benutzerverwaltung** > **Benutzergruppen**.

   Der Bildschirm **Benutzergruppen** wird angezeigt.

2. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie mit der rechten Maustaste auf die gewünschte Benutzergruppe, und wählen Sie **Löschen** aus.
   - Wählen Sie die Benutzergruppe aus, die Sie löschen möchten. Das Menü **Aktionen** wird angezeigt. Wählen Sie **Aktionen** > **Löschen** aus.

   Daraufhin wird ein Bestätigungsfenster angezeigt.

3. Klicken Sie auf **Löschen**.

   OT Security löscht die **Benutzergruppe**

Benutzerrollen

Die folgenden Rollen sind verfügbar:

- **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 und 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)
Ereignisse		
Ereignisse anzeigen	✓	✓
Auflösen	✓	✓
Erfassungsdatei herunterladen	✓	✓
Aus Richtlinie ausschließen	✓	✓
Alle auflösen	✓	✓
Exportieren	✓	✓
Richtlinie auf FortiGate erstellen	✓	✓

Aktualisieren	✓	✓
Richtlinien		
Richtlinien anzeigen	✓	✓
Aktivieren/ Deaktivieren	✓	✓
Aktion anzeigen	✓	✓
Bearbeiten	✓	✓
Duplizieren	✓	✓
Löschen	✓	✓
Richtlinie erstellen	✓	✓
Exportieren	✓	✓
Assets		
Assets anzeigen	✓	✓
Aktion anzeigen	✓	✓
Bearbeiten	✓	✓
Löschen	✓	✓
Importieren (neue Assets über CSV-Datei hochladen)	✓	✓
Ausblenden	✓	✓
Exportieren	✓	✓
Erneut synchronisieren	✓	✓
Nessus-Scan	✓	✓
Snapshot erstellen (einzelnes Asset)	✓	✓

Offene Ports aktualisieren (einzelnes Asset)	✓	✓
Port-Status aktualisieren (einzelnes Asset)	✓	✓
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	✓	✓
Plugin-Satz aktualisieren	✓	✓
Exportieren	✓	✓
Netzwerk		
Paketerfassung aktivieren	✓	✓
Fortlaufende Erfassungen schließen	✓	✓
PCAP-Datei herunterladen	✓	✓
Konversationstabelle exportieren	✓	✓
Als Baseline festlegen	✓	✓
Übersicht generieren	✓	✓
Übersicht aktualisieren	✓	✓

Gruppen		
Gruppen anzeigen	✓	✓
Aktion anzeigen	✓	✓
Bearbeiten	✓	✓
Duplizieren	✓	✓
Löschen	✓	✓
Gruppe erstellen	✓	✓
Exportieren	✓	✓
Bericht		
Berichte anzeigen	✓	✓
Generieren	✓	✓
Herunterladen	✓	✓
Exportieren	✓	✓
Netzwerksegmente		
Netzwerksegmente anzeigen	✓	✓
Bearbeiten	✓	✓
Löschen	✓	✓
Erstellen	✓	✓
Exportieren	✓	✓
Mehr erfahren	✓	✓
Lokale Einstellungen		
Abfragen	✓	✓

Systemkonfiguration – Gerätedetails	✓	✓
Systemkonfiguration – Sensoren	✓	✓
Systemkonfiguration – Portkonfiguration	✓	✓
Systemkonfiguration – Updates	✓	✓
Systemkonfiguration – Zertifikat (HTTPS)	✓	✓
Systemkonfiguration – API-Schlüssel	✓	✗
Systemkonfiguration – Lizenz	✓	✓
Umgebungskonfiguration – Asset-Einstellungen	✓	✓
Umgebungskonfiguration – Ausgeblendete Assets	✓	✓
Umgebungskonfiguration – Benutzerdefinierte Felder	✓	✓
Umgebungskonfiguration – Ereigniscluster	✓	✓
Umgebungskonfiguration – PCAP-Player	✓	✓
Benutzer und Rollen – Benutzereinstellungen	✓	✓
Benutzer und Rollen – Lokale Benutzer	✓	✗
Benutzer und Rollen – Benutzergruppen	✓	✗
Benutzer und Rollen – Active Directory	✓	✗

Integrationen	✓	✓
Server	✓	✓
Systemaktionen	✓	✓ ohne Zurücksetzung auf Werkseinstellungen
Systemprotokoll	✓	✓
Aktivieren (beim Setup und nach Deaktivierung)	✓	✓
Assets löschen	✓	✓

Berechtigung	Supervisor	Sicherheitsmanager	Sicherheitsanalyst	Site-Operator	Schreibgeschützt
Ereignisse					
Ereignisse anzeigen	✓	✓	✓	✓	✓
Auflösen	✓	✓	✓	✗	✗
Erfassungsdatei herunterladen	✓	✓	✓	✓	✓
Aus Richtlinie ausschließen	✓	✓	✗	✗	✗
Alle auflösen	✓	✓	✓	✗	✗
Exportieren	✓	✓	✓	✓	✓
Richtlinie auf FortiGate erstellen	✓	✓	✗	✗	✗
Aktualisieren	✓	✓	✓	✓	✓
Richtlinien					

Richtlinien anzeigen	✓	✓	✓	✓	✓
Aktivieren/ Deaktivieren	✓	✓	✗	✗	✗
Aktion anzeigen	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✗	✗	✗
Duplizieren	✓	✓	✗	✗	✗
Löschen	✓	✓	✗	✗	✗
Richtlinie erstellen	✓	✓	✗	✗	✗
Exportieren	✓	✓	✓	✓	✓
Assets					
Assets anzeigen	✓	✓	✓	✓	✓
Aktion anzeigen	✓	✓	✓	✓	✓
Bearbeiten	✓	✗	✗	✓	✗
Löschen	✓	✗	✗	✓	✗
Importieren (neue Assets über CSV-Datei hochladen)	✓	✗	✗	✓	✗
Ausblenden	✓	✗	✗	✓	✗
Exportieren	✓	✓	✓	✓	✓
Erneut synchronisieren	✓	✓	✓	✓	✗
Nessus-Scan	✓	✓	✓	✓	✗
Snapshot erstellen	✓	✓	✓	✓	✗

(einzelnes Asset)					
Offene Ports aktualisieren (einzelnes Asset)	✓	✓	✓	✗	✗
Port-Status aktualisieren (einzelnes Asset)	✓	✓	✓	✗	✗
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	✓	✓	✓	✗	✗
Plugin-Satz aktualisieren	✓	✓	✗	✗	✗
Exportieren	✓	✓	✓	✓	✓
Netzwerk					
Paketerfassung	✓	✗	✗	✗	✗

aktivieren					
Fortlaufende Erfassungen schließen	✓	✓	✓	✓	✗
PCAP-Datei herunterladen	✓	✓	✓	✓	✓
Konversationstabelle exportieren	✓	✓	✓	✓	✓
Als Baseline festlegen	✓	✓	✗	✗	✗
Übersicht generieren	✓	✓	✓	✓	✓
Übersicht aktualisieren	✓	✓	✓	✓	✓
Gruppen					
Gruppen anzeigen	✓	✓	✓	✓	✓
Aktion anzeigen	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✗	✗	✗
Duplizieren	✓	✓	✗	✗	✗
Löschen	✓	✓	✗	✗	✗
Gruppe erstellen	✓	✓	✗	✗	✗
Exportieren	✓	✓	✓	✓	✓
Bericht					
Berichte anzeigen	✓	✓	✓	✓	✓
Generieren	✓	✓	✓	✓	✓

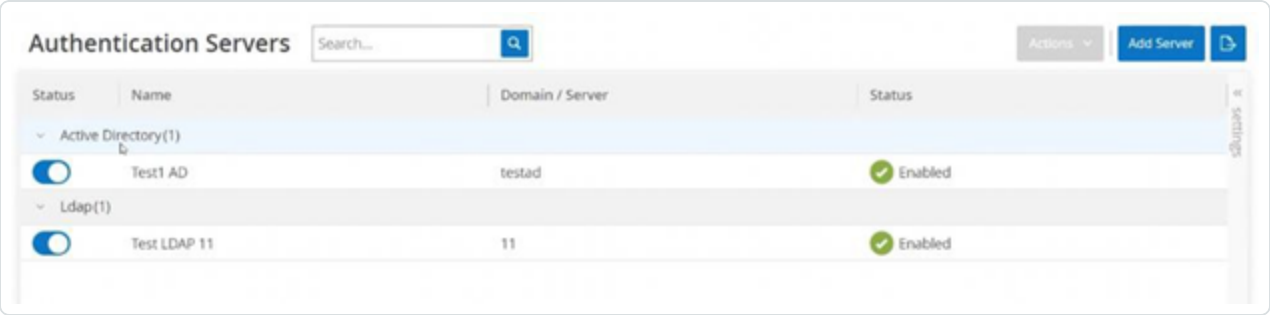
Herunterladen	✓	✓	✓	✓	✓
Exportieren	✓	✓	✓	✓	✓
Netzwerksegmente					
Netzwerksegmente anzeigen	✓	✓	✓	✓	✓
Bearbeiten	✓	✓	✗	✗	✗
Löschen	✓	✓	✗	✗	✗
Erstellen	✓	✓	✗	✗	✗
Exportieren	✓	✓	✓	✓	✓
Mehr erfahren	✓	✓	✓	✓	✓
Lokale Einstellungen					
Abfragen	✓	✗	✗	✗	✗
Systemkonfiguration – Gerätedetails	✓	✗	✗	✗	✗
Systemkonfiguration – Sensoren	✓	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)
Systemkonfiguration – Portkonfiguration	✓	✗	✗	✗	✗
Systemkonfiguration – Updates	✓	✗	✗	✗	✗
Systemkonfiguration – Zertifikat (HTTPS)	✗	✗	✗	✗	✗

Systemkonfiguration – API-Schlüssel	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)	✓ (Nur lokale Benutzer)
Systemkonfiguration – Lizenz	✗	✗	✗	✗	✗
Umgebungskonfiguration – Asset-Einstellungen	✓	✗	✗	✗	✗
Umgebungskonfiguration – Ausgeblendete Assets	✓	✓ – keine Wiederherstellung	✓ – keine Wiederherstellung	✓	✓ – keine Wiederherstellung
Umgebungskonfiguration – Benutzerdefinierte Felder	✓	✗	✗	✗	✗
Umgebungskonfiguration – Ereigniscluster	✓	✗	✗	✗	✗
Umgebungskonfiguration – PCAP-Player	✓	✗	✗	✗	✗
Benutzer und Rollen – Benutzereinstellungen	✓	✗	✗	✗	✗
Benutzer und Rollen – Lokale	✗	✗	✗	✗	✗

Benutzer					
Benutzer und Rollen – Benutzergruppen	✗	✗	✗	✗	✗
Benutzer und Rollen – Active Directory	✗	✗	✗	✗	✗
Integrationen	✗	✗	✗	✗	✗
Server	✓	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)	✓ (Keine Aktionen)
Systemaktionen	✓ nur Sicherung und Diagnose	✓ nur Diagnose	✗	✗	✗
Systemprotokoll	✓	✓	✓	✓	✓ kein Syslog
Aktivieren (beim Setup und nach Deaktivierung)	✗	✗	✗	✗	✗
Assets löschen	✓	✗	✗	✗	✗

Authentifizierungsserver

Auf der Seite **Authentifizierungsserver** werden Ihre vorhandenen Integrationen mit Authentifizierungsservern angezeigt. Sie können einen Server hinzufügen, indem Sie auf die Schaltfläche **Server hinzufügen** klicken.



Active Directory

Sie können OT Security mit dem Active Directory (AD) Ihrer Organisation integrieren. Dies ermöglicht es Benutzern, sich mit ihren Active Directory-Zugangsdaten bei OT Security einzuloggen. Im Rahmen der Konfiguration richten Sie die Integration ein und ordnen dann Gruppen in Ihrem AD zu Benutzergruppen in OT Security zu.

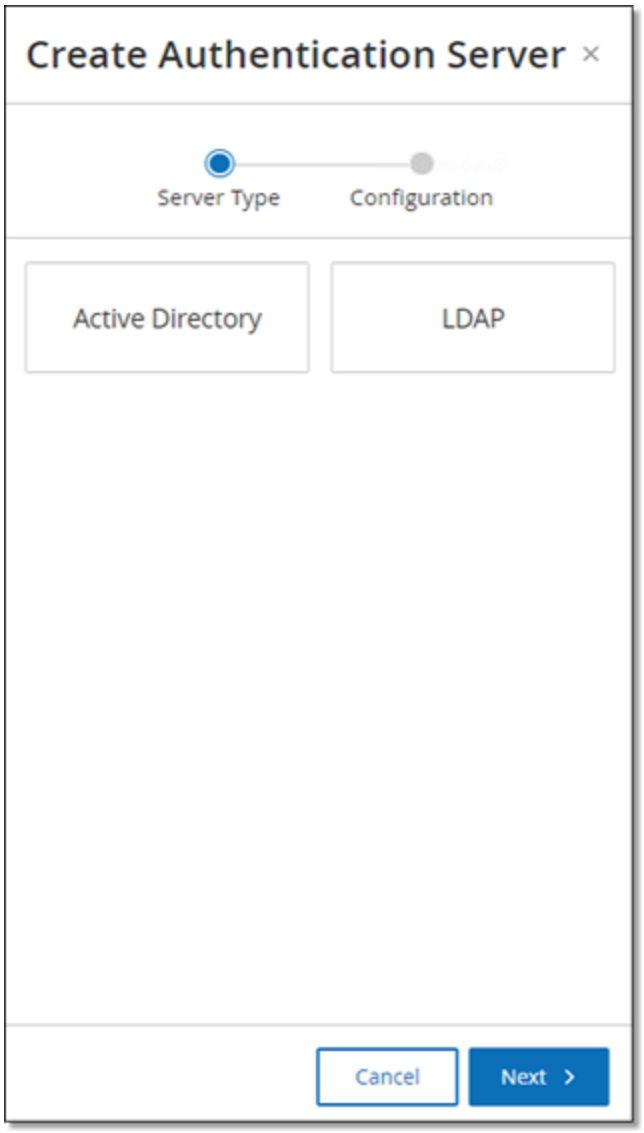
Hinweis: Das System wird mit einer Reihe vordefinierter Benutzergruppen geliefert, die den einzelnen verfügbaren Rollen entsprechen: **Benutzergruppe „Administratoren“** > **Rolle „Administrator“**, **Benutzergruppe „Site-Operatoren“** > **Rolle „Site-Operator“** usw. Eine Erläuterung der verfügbaren Rollen finden Sie unter Authentifizierungsserver.

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.
2. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Authentifizierungsserver**.

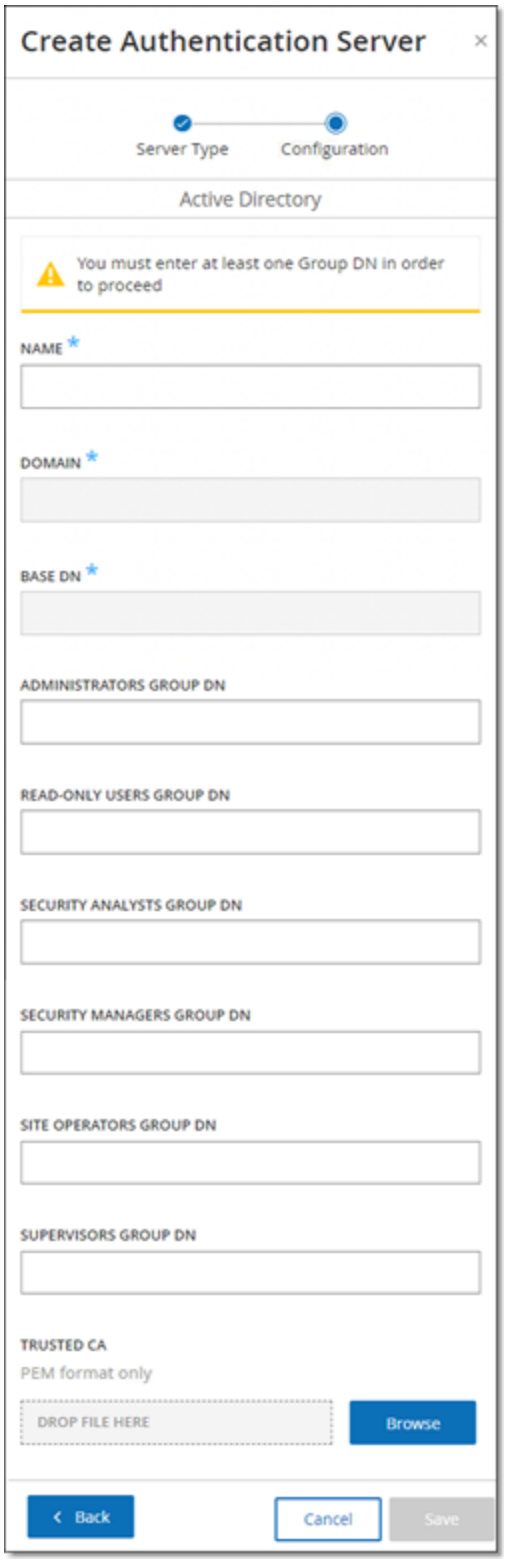
   Das Fenster **Authentifizierungsserver** wird angezeigt.
3. Klicken Sie auf **Server hinzufügen**.

   Der Bereich **Authentifizierungsserver erstellen** mit dem **Servertyp** wird geöffnet.



4. Klicken Sie auf **Active Directory** und dann auf **Weiter**.

   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 **Domäne** den FQDN der Organisationsdomäne ein (z. B. firma.com).

Hinweis: Wenn Sie Ihren Domänennamen nicht kennen, können Sie nach ihm suchen, indem Sie den Befehl „set“ in die Windows-Eingabeaufforderung oder -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 OT Security-Benutzergruppe zuordnen möchten, den DN der AD-Gruppe in das entsprechende Feld ein.

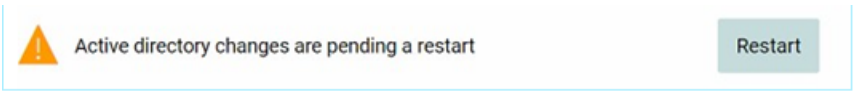
   Um beispielsweise eine Gruppe von Benutzern der Benutzergruppe „Administratoren“ zuzuweisen, geben Sie den DN der Active Directory-Gruppe, der Sie Administratorrechte zuweisen möchten, in das Feld **Administratorgruppen-DN** ein.

   Hinweis: Wenn Sie den DN der Gruppe, der Sie OT Security-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 oder -Befehlszeile eingeben. Geben Sie den Namen der Gruppe, die Sie zuweisen möchten, im gleichen Format ein, 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.

   Hinweis: Diese Felder sind optional. Wenn ein Feld leer 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. (Optional) 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).
10. Aktivieren Sie das Kontrollkästchen **Active Directory aktivieren**.
11. Klicken Sie auf **Speichern**.

    In einer Meldung werden Sie zum Neustart des Geräts aufgefordert, um Active Directory zu aktivieren.



12. Klicken Sie auf **Neu starten**.

    Das Gerät startet neu. Beim Neustart aktiviert OT Security die Active Directory-Einstellungen. Jeder Benutzer, der den festgelegten Gruppen zugewiesen ist, kann mit den Zugangsdaten der Organisation auf die OT Security-Plattform zugreifen.

    Hinweis: Um sich über Active Directory einzuloggen, muss 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.

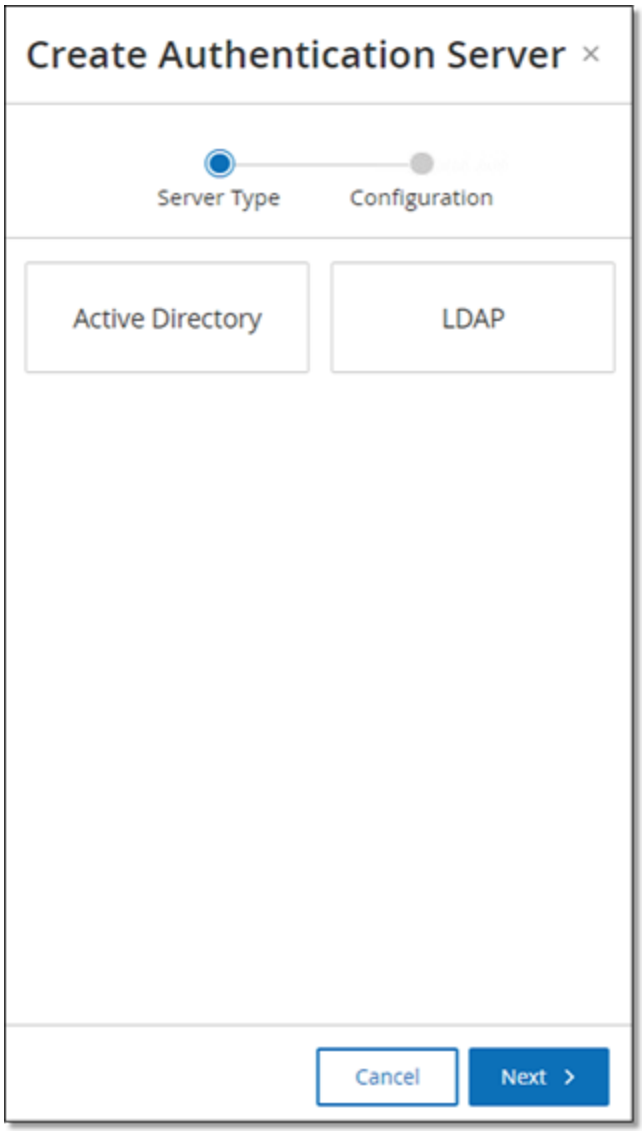
LDAP

Sie können OT Security mit dem LDAP Ihrer Organisation integrieren. Dies ermöglicht es Benutzern, sich mit ihren LDAP-Zugangsdaten bei OT Security einzuloggen. Im Rahmen der Konfiguration richten Sie die Integration ein und ordnen dann Gruppen in Ihrem AD zu Benutzergruppen in OT Security zu.

So konfigurieren Sie LDAP:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **Authentifizierungsserver**.
2. Klicken Sie auf **Server hinzufügen**.

   Der Bereich **Authentifizierungsserver hinzufügen** mit dem **Servertyp** wird geöffnet.



3. Wählen Sie **LDAP** aus und klicken Sie dann auf **Weiter**.

   Der Bereich **LDAP-Konfiguration** wird angezeigt.

4. Geben Sie im Feld **Name** den Namen ein, der im Login-Bildschirm verwendet werden soll.

   > **Hinweis**: Der Login-Name muss eindeutig sein und 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.

Hinweis: Wenn Sie eine sichere Verbindung nutzen, empfiehlt Tenable, den FQDN anstelle einer IP-Adresse zu verwenden, um sicherzustellen, dass das bereitgestellte sichere Zertifikat verifiziert wird.

Hinweis: Wenn ein Hostname verwendet wird, muss er in der Liste der DNS-Server im OT Security-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.

   Hinweis: 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 „adsrv1tenable.com“ kann der Benutzer-DN `CN=Administrator,CN=Benutzer,DC=adsrv1,DC=tenable,DC=com` lauten.

8. Geben Sie im Feld **Passwort** das Passwort des Benutzer-DN ein.

   Hinweis: Die OT Security-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 daher auch die OT Security-Konfiguration aktualisiert werden.

9. Geben Sie im Feld **Basis-DN des Benutzers** den Basis-Domänennamen im DN-Format ein. Beispiel: Für den Servernamen „adsrv1tenable.com“ kann der Basis-DN des Benutzers `OU=Benutzer,DC=adsrv1,DC=tenable,DC=com` lauten.

10. Geben Sie im Feld **Basis-DN der Gruppe** den Basis-Domänennamen der Gruppe im DN-Format ein. Beispiel: Für den Servernamen „adsrv1tenable.com“ kann der Basis-DN der Gruppe `OU=Gruppe,DC=adsrv1,DC=tenable,DC=com` lauten.

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**.

    OT Security startet den Server im Modus **Deaktiviert**.
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.

    > **Hinweis**: 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.

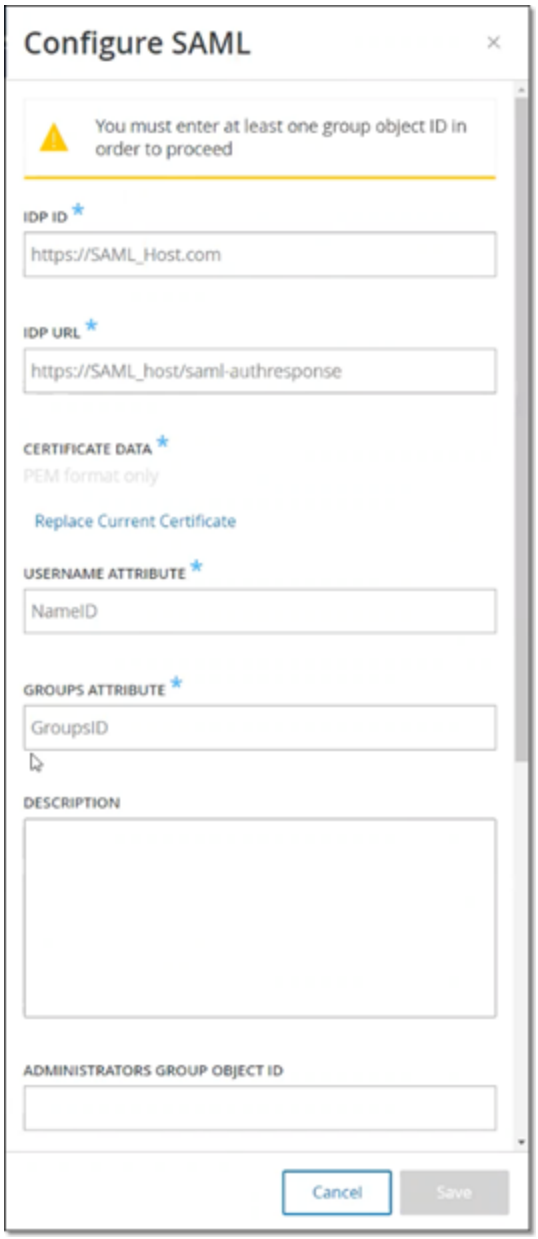
SAML

Sie können OT Security 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 OT Security-Anwendung innerhalb Ihres Identitätsanbieters erstellen, Informationen über Ihre erstellte OT Security-Anwendung eingeben, das Zertifikat Ihres Identitätsanbieters auf die OT Security-Seite **SAML** hochladen und dann Gruppen von Ihrem Identitätsanbieter zu Benutzergruppen in OT Security zuordnen. Eine ausführliche Anleitung zur Integration von OT Security mit Microsoft Azure finden Sie unter Anhang – SAML-Integration für Microsoft Azure.

So konfigurieren Sie SAML:

1. Gehen Sie zu **Einstellungen** > **Benutzerverwaltung** > **SAML**.
2. Klicken Sie auf **Konfigurieren**.

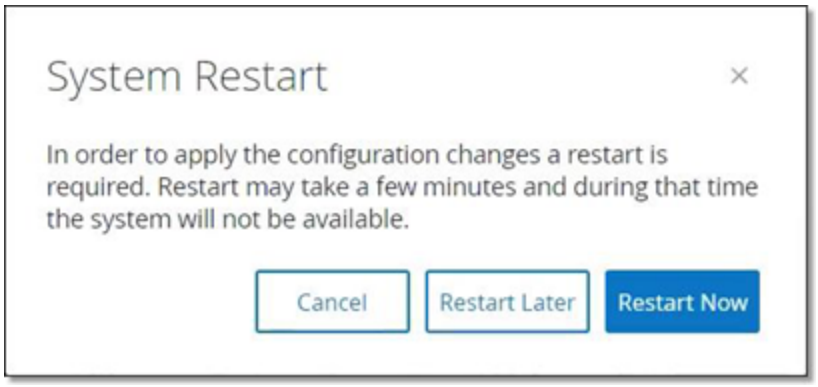
   Daraufhin wird der Bereich **SAML konfigurieren** angezeigt.



3. Geben Sie im Feld **IDP-ID** die ID des Identitätsanbieters für die OT Security-Anwendung ein.
4. Geben Sie im Feld **IDP-URL** die URL des Identitätsanbieters für die OT Security-Anwendung ein.
5. Klicken Sie unter **Zertifikatdaten** auf **Datei hier ablegen**, navigieren Sie zur Zertifikatdatei des Identitätsanbieters, die Sie zur Verwendung mit der OT Security-Anwendung heruntergeladen haben, und öffnen Sie sie.

6. Geben Sie im Feld **Username-Attribut** das Username-Attribut vom Identitätsanbieter für die OT Security-Anwendung ein.
7. Geben Sie im Feld **Groups-Attribut** das Groups-Attribut vom Identitätsanbieter für die OT Security-Anwendung ein.
8. (Optional) Geben Sie im Feld **Beschreibung** eine Beschreibung ein.
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 im Feld der gewünschten **Gruppenobjekt-ID** ein, um sie der gewünschten OT Security-Benutzergruppe zuzuordnen.
10. Klicken Sie auf **Speichern**, um die Informationen im Seitenbereich zu speichern und diesen zu schließen.
11. Klicken Sie im Fenster **SAML** auf den Umschalter **SAML Single Sign-On-Login**, um das Single Sign-On-Login zu aktivieren.

    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 in OT Security 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 OT Security-Plattform zugreifen.

Integrationen

Sie können Integrationen mit weiteren unterstützten Plattformen einrichten, damit OT Security mit Ihren anderen Cybersecurity-Plattformen synchronisiert werden kann.

Tenable-Produkte

Sie können OT Security mit Tenable Security Center und Tenable Vulnerability Management integrieren. OT Security tauscht über diese Integrationen Daten mit den anderen Plattformen aus. Die synchronisierten Daten umfassen sowohl OT-Schwachstellen als auch Daten, die durch IT-bezogene Tenable Nessus-Scans erfasst wurden, die über OT Security initiiert wurden.

Hinweis: OT Security sendet über die Integration keine Daten für **ausgeblendete** Assets an Tenable Security Center und Tenable Vulnerability Management.

Hinweis: Um die Plattformen zu integrieren, muss OT Security Tenable Security Center und/oder Tenable Vulnerability Management über Port 443 erreichen können. Tenable empfiehlt, einen bestimmten Benutzer in Tenable Security Center und/oder Tenable Vulnerability Management zu erstellen, der als Integrationsbenutzer für OT Security verwendet werden soll.

Tenable Security Center

Um Tenable Security Center zu integrieren, erstellen Sie in Tenable Security Center ein **universelles Repository** zur Speicherung von OT Security-Daten, und notieren Sie sich die Repository-ID. Weitere Informationen finden Sie unter Universal Repositories.

Hinweis: Tenable empfiehlt, in Tenable Security Center einen spezifischen Benutzer zu erstellen, der für die Integration mit OT Security verwendet wird. Der Benutzer sollte über die Rolle „Sicherheitsmanager/Sicherheitsanalyst“ oder „Schwachstellenanalyst“ verfügen und der Gruppe „Vollzugriff“ zugewiesen sein.

So integrieren Sie Tenable Security Center:

1. Gehen Sie zu **Einstellungen** > **Integrationen**.

   Die Seite **Integrationen** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf **Integrationsmodul hinzufügen**.

   Der Bereich **Integrationsmodul hinzufügen** wird angezeigt.

3. Wählen Sie im Abschnitt **Modultyp** die Option Tenable Security Center aus.

4. Klicken Sie auf **Weiter**.

   Der Bereich **Moduldefinition** wird mit den relevanten Feldern angezeigt.

5. Geben Sie im Feld **Hostname/ IP** den Hostnamen oder die IP-Adresse Ihres Tenable Security Center ein.

6. Geben Sie im Feld **Benutzername** die Benutzer-ID des Kontos ein.

7. Geben Sie im Feld **Passwort** das Passwort Ihres Kontos ein.

8. Geben Sie im Feld **Repository-ID** die ID des universellen Repository an.

9. Legen Sie im Dropdown-Feld **Synchronisierungsfrequenz** die Frequenz fest, mit der die Daten synchronisiert werden sollen.

10. Klicken Sie auf **Speichern**.

    OT Security erstellt die Integration und zeigt die neue Integration auf der Seite „Integrationen“ an.

11. Klicken Sie mit der rechten Maustaste auf die neue Integration und klicken Sie auf **Synchronisieren**.

Tenable Vulnerability Management

Hinweis: Sie müssen zuerst einen API-Schlüssel in der Tenable Vulnerability Management-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 OT Security-Konsole eingeben können.

So integrieren Sie Tenable Vulnerability Management:

1. Gehen Sie zu **Einstellungen** > **Integrationen**.

   Die Seite **Integrationen** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf **Integrationsmodul hinzufügen**.

   Der Bereich **Integrationsmodul hinzufügen** wird angezeigt.

3. Wählen Sie im Abschnitt **Modultyp** die Option Tenable Vulnerability Management aus.

4. Klicken Sie auf **Weiter**.

   Der Bereich **Moduldefinition** wird mit den relevanten Feldern angezeigt.

5. Geben Sie im Feld **Zugriffsschlüssel** den Zugriffsschlüssel an.

6. Geben Sie im Feld **Geheimer Schlüssel** den geheimen Schlüssel an.

7. Wählen Sie im Dropdown-Feld **Synchronisierungsfrequenz** die Frequenz aus, mit der die Daten synchronisiert werden sollen.

Tenable One

Befolgen Sie zur Integration mit Tenable One die unter Mit Tenable One integrieren beschriebenen Schritte.

Palo Alto Networks – Next Generation Firewall

Sie können von OT Security erfasste Asset-Inventarisierungsdaten an Ihr Palo Alto-System übertragen.

So integrieren Sie OT Security mit Ihren Palo Alto Networks Next Generation Firewalls (NGFW):

1. Gehen Sie zu **Einstellungen** > **Integrationen**.

   Die Seite **Integrationen** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf **Integrationsmodul hinzufügen**.

   Der Bereich **Integrationsmodul hinzufügen** wird angezeigt.

3. Wählen Sie im Abschnitt **Modultyp** die Option „Palo Alto Networks NGFW“ aus.

4. Klicken Sie auf **Weiter**.

5. Geben Sie im Feld **Hostname/ IP** den Hostnamen oder die IP-Adresse Ihres Palo Alto Networks NGFW-Kontos ein.
6. Geben Sie im Feld **Benutzername** den Benutzernamen Ihres NGFW-Kontos ein.
7. Geben Sie im Feld **Passwort** das Passwort für Ihr NGFW-Konto ein.
8. Klicken Sie auf **Speichern**.

   OT Security speichert die Integration.

Aruba – ClearPass-Richtlinienmanager

Sie können von OT Security erfasste Asset-Inventarisierungsdaten an Ihr Aruba-System übertragen.

So integrieren Sie OT Security mit Ihrem Aruba ClearPass-Konto:

1. Gehen Sie zu **Einstellungen** > **Integrationen**.

   Die Seite **Integrationen** wird angezeigt.
2. Klicken Sie in der oberen rechten Ecke auf **Integrationsmodul hinzufügen**.

   Der Bereich **Integrationsmodul hinzufügen** wird angezeigt.
3. Wählen Sie im Abschnitt **Modultyp** die Option „Aruba Networks ClearPass“ aus.
4. Klicken Sie auf **Weiter**.
5. Geben Sie im Feld **Hostname/ IP** den Hostnamen oder die IP-Adresse Ihres Aruba Networks ClearPass-Kontos ein.
6. Geben Sie im Feld **Benutzername** den Benutzernamen Ihres Aruba Networks ClearPass-Kontos ein.
7. Geben Sie im Feld **Passwort** das Passwort für Ihr Aruba Networks ClearPass-Kontos ein.
8. Geben Sie im Feld **Client-ID** die Client-ID Ihres Aruba Networks ClearPass-Kontos ein.
9. Geben Sie im Feld **API-Client-Geheimnis** das API-Client-Geheimnis Ihres Aruba Networks ClearPass-Kontos ein.
10. Klicken Sie auf **Speichern**.

    OT Security speichert die Integration.

Mit Tenable One integrieren

Sie können OT Security mit Tenable One integrieren, um Daten zu Assets und Risikowerten an Tenable Vulnerability Management zu senden. Für die Integration mit Tenable One müssen Sie zuerst einen Linking Key in Tenable Vulnerability Management generieren und diesen in OT Security angeben. Tenable One wird regelmäßig mit allen Asset-Änderungen aktualisiert, die seit der letzten Synchronisierung erfolgt sind.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über den in Tenable Vulnerability Management generierten Linking Key verfügen. Weitere Informationen finden Sie unter OT Connectors im Benutzerhandbuch zu Tenable Vulnerability Management.

  Hinweis: Ein in Tenable Vulnerability Management generierter Linking Key kann nur für eine einzelne OT Security-Site verwendet werden.

So führen Sie die Integration mit Tenable One durch:

1. Gehen Sie zu **Einstellungen** > **Integrationen**.

   Die Seite **Integrationen** wird angezeigt.

2. Klicken Sie in der oberen rechten Ecke auf **Integrationsmodul hinzufügen**.

   Der Bereich **Integrationsmodul hinzufügen** wird angezeigt.

3. Klicken Sie im Abschnitt **Modultyp** auf **Tenable One**.

4. Klicken Sie auf **Weiter**.

   Der Abschnitt **Moduldefinition** wird angezeigt.

5. Geben Sie im Feld **Cloud-Site** den Namen der Cloud-Site ein.

   Hinweis: Der Name der Cloud-Site wird im Fenster **Add OT Connector** von Tenable Vulnerability Management angezeigt, nachdem Sie den Linking Key generiert haben.

6. Geben Sie im Feld **Linking Key** den Linking Key ein, den Sie in Tenable Vulnerability Management generiert haben.

7. Klicken Sie auf **Speichern**.

In OT Security wird die Meldung angezeigt, dass die Integration durchgeführt wurde. Sobald die Integration abgeschlossen ist, wird die verknüpfte Site auf der Seite **Integrationen** angezeigt. In Tenable One wird auf der Seite **Sensors** > **OT Connectors** der Gerätename angezeigt, der für diese Site in OT Security konfiguriert ist.

Den Gerätenamen für eine Site finden Sie im Abschnitt **Gerätename** auf der Seite **Systemkonfiguration** > **Gerät**.

> **Hinweis**: Wenn Sie den Namen Ihrer Site in OT Security ändern, nachdem die Kopplung bereits erfolgt hat, können Sie den Sensornamen in Tenable Vulnerability Management manuell so ändern, dass er dem neuen Site-Namen entspricht. Alternativ können Sie die Integration sowohl in OT Security als auch in Tenable Vulnerability Management löschen und die Kopplung erneut durchführen, um die Änderung des Site-Namens automatisch zu übernehmen.

Informationen zum vollständigen Verfahren für die Bereitstellung und Lizenzierung von Tenable OT Security für Tenable One finden Sie im Tenable One Deployment Guide.

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 OT Security-Netzwerkereignissen Vorschläge zu Firewall-Richtlinien zu senden.

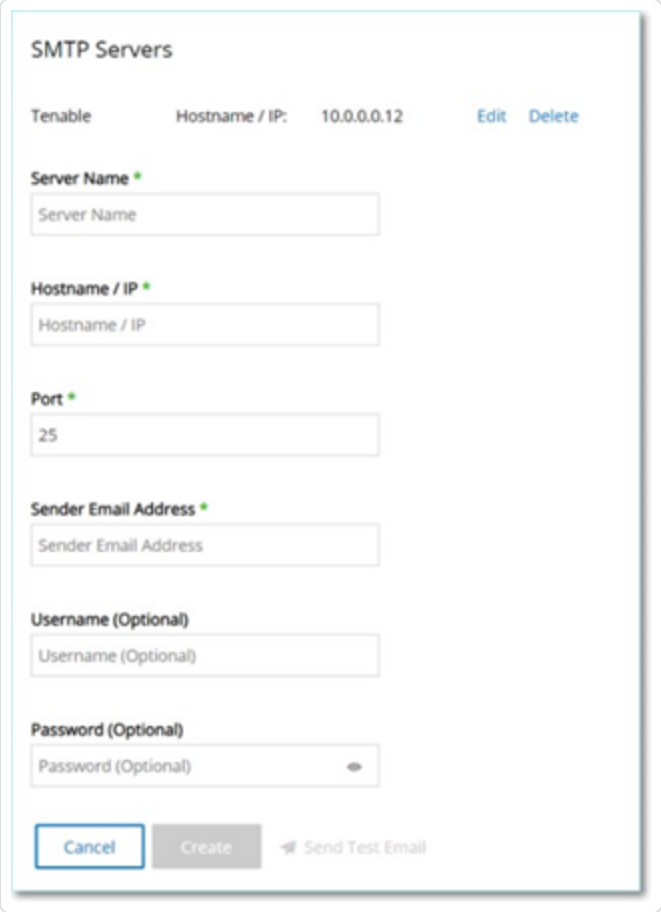
SMTP-Server

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, kann das System keine E-Mail-Benachrichtigungen senden, wenn Ereignisse generiert werden. In jedem Fall können alle Ereignisse in der Verwaltungskonsole (Benutzeroberfläche) im Bildschirm **Ereignisse** eingesehen werden.

So richten Sie einen SMTP-Server ein:

1. Gehen Sie zu **Einstellungen** > **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 auf Ereignisse lauscht (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. (Optional) Geben Sie in die Felder **Benutzername** und **Passwort** einen Benutzernamen und ein Passwort für den Zugriff auf den SMTP-Server ein.

8. Um eine Test-E-Mail zu senden und damit 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**.

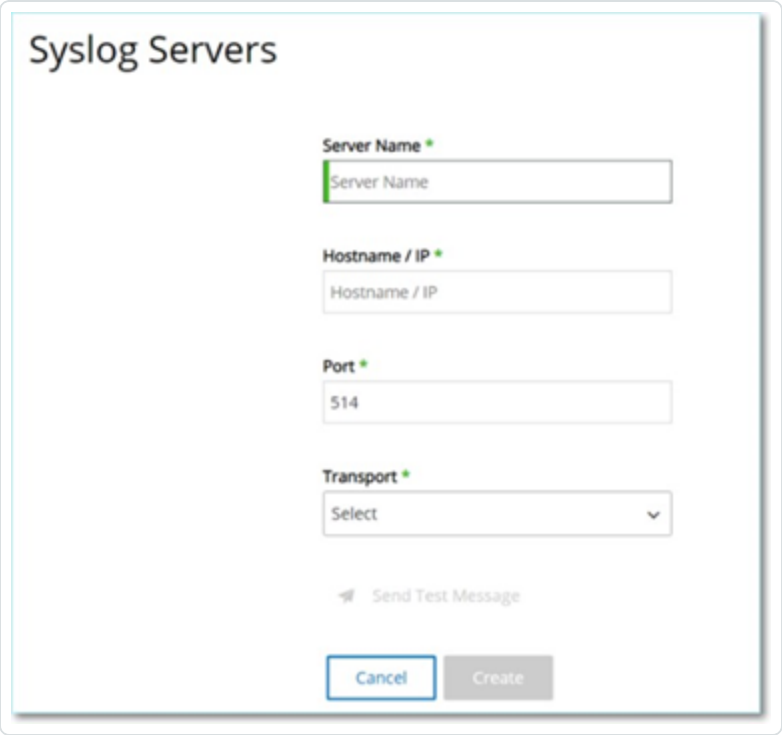
   Sie können weitere SMTP-Server einrichten, indem Sie den Vorgang wiederholen.

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 OT Security-Plattform gespeichert.

So richten Sie einen Syslog-Server ein:

1. Gehen Sie zu **Einstellungen** > **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 Dropdown-Feld **Transport** das gewünschte Transportprotokoll aus. Verfügbare Optionen: TCP oder UDP.
7. Um eine Testnachricht zu senden und damit 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 Vorgang wiederholen.

FortiGate-Firewalls

So richten Sie einen FortiGate-Server ein:

1. Gehen Sie zu **Einstellungen** > **Server** > **FortiGate-Firewalls**.
2. Klicken Sie auf **Firewall hinzufügen**.

   Das Konfigurationsfenster **FortiGate-Firewall hinzufügen** wird angezeigt.

3. Geben Sie im Feld **Servername** den Namen eines FortiGate-Servers ein, den Sie verwenden möchten.
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.

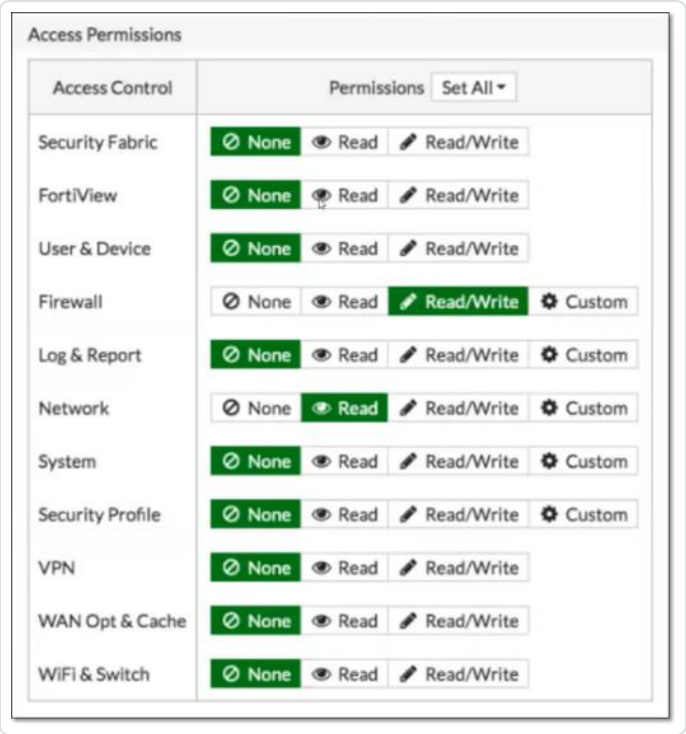
   Hinweis: Anweisungen zum Generieren eines FortiGate-API-Tokens finden Sie auf folgender Seite: https://registry.terraform.io/providers/fortinetdev/fortios/latest/docs/guides/fgt_token

6. Klicken Sie auf **Hinzufügen**.

   OT Security erstellt den FortiGate-Firewall-Server.

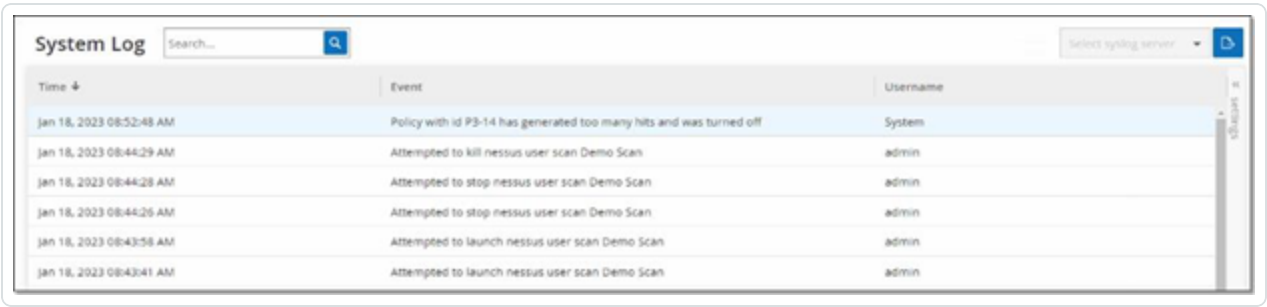
   Hinweis: Verwenden Sie als Quelladresse (die erforderlich ist, um sicherzustellen, dass das API-Token nur von vertrauenswürdigen Hosts verwendet werden kann) die IP-Adresse Ihres OT Security-Geräts.

Stellen Sie beim Erstellen eines Administratorprofils für OT Security sicher, dass Sie Zugriffsberechtigungen gemäß den folgenden Einstellungen anwenden:



Systemprotokoll

Die Seite **Systemprotokoll** enthält eine Liste aller Systemereignisse (z. B. Richtlinie aktiviert, Richtlinie bearbeitet, Ereignis aufgelöst usw.), die im System aufgetreten sind. Dieses Protokoll umfasst 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. Sie können die Protokolle als CSV-Datei exportieren. Sie können das System auch so konfigurieren, dass die Systemprotokollereignisse an einen Syslog-Server gesendet werden.



Jedes protokollierte Ereignis enthält die folgenden Details:

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 zu **Einstellungen** > **Systemprotokoll**.
2. Klicken Sie in der oberen rechten Ecke auf das Dropdown-Feld, um die Liste der Server anzuzeigen.

   Hinweis: Informationen zum Hinzufügen eines Syslog-Servers finden Sie unter Syslog-Server.
3. Wählen Sie den gewünschten Server aus.

   OT Security sendet die Systemprotokollereignisse an den angegebenen Syslog-Server.

Anhang – SAML-Integration für Microsoft Azure

OT Security unterstützt die Integration mit Azure über das SAML-Protokoll. Dies ermöglicht es Azure-Benutzern, die OT Security zugewiesen wurden, sich über Single Sign-On (SSO) bei OT Security einzuloggen. Mithilfe der Gruppenzuordnung können Sie Rollen in OT Security entsprechend den Gruppen zuzuweisen, denen Benutzer in Azure zugewiesen sind.

In diesem Abschnitt wird der vollständige Ablauf für die Einrichtung einer SSO-Integration für OT Security mit Azure erläutert. Im Rahmen der Konfiguration wird eine OT Security-Anwendung in Azure erstellt, um die Integration einzurichten. Anschließend können Sie Informationen zu dieser neu erstellten OT Security-Anwendung angeben und das Zertifikat Ihres Identitätsanbieters auf die

SAML-Seite in OT Security hochladen. Die Konfiguration ist abgeschlossen, wenn Sie Gruppen von Ihrem Identitätsanbieter zu Benutzergruppen in OT Security zuordnen.

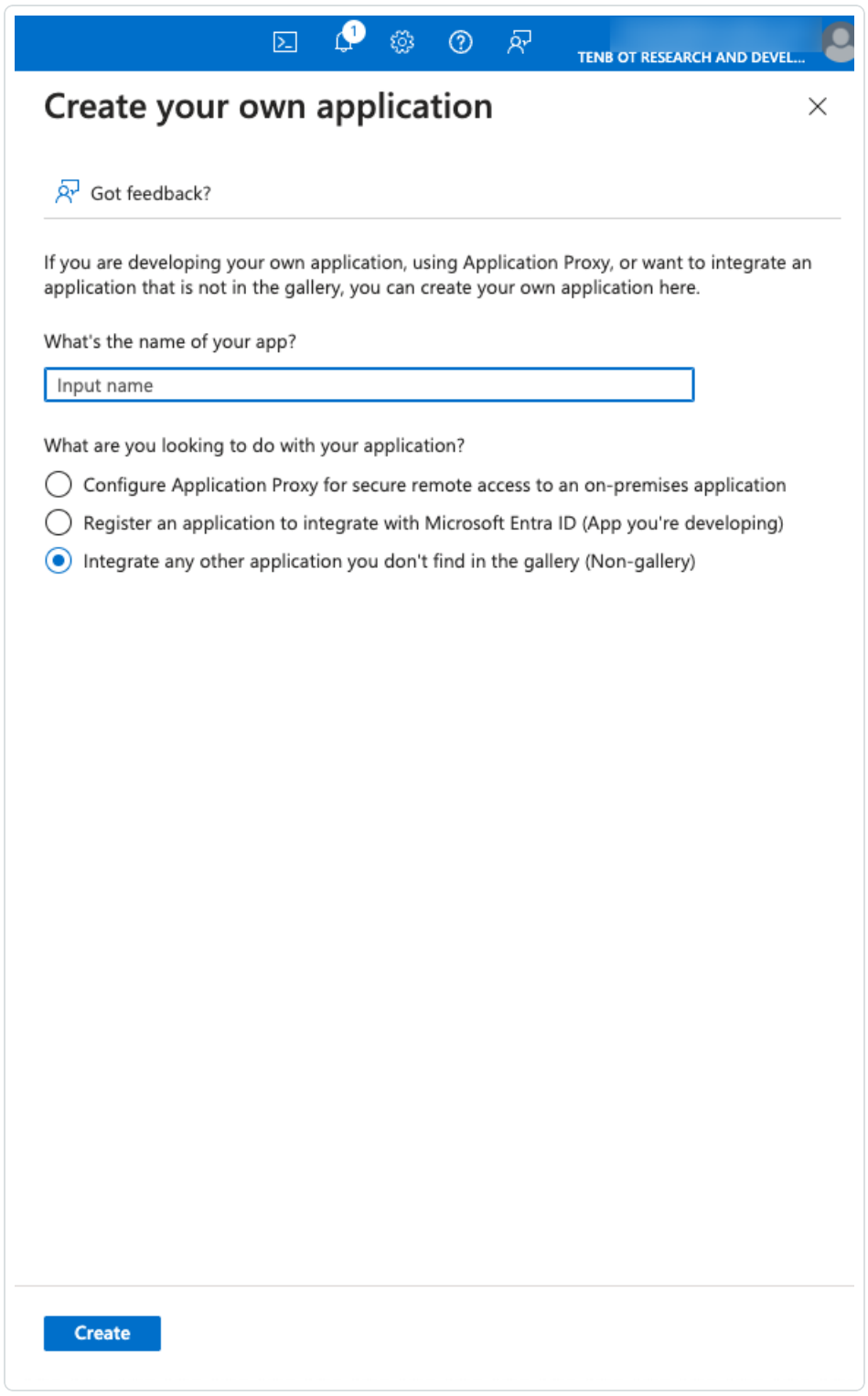
Um die Konfiguration einzurichten, müssen Sie sowohl bei Microsoft Azure als auch bei OT Security als Administrator eingeloggt sein.

Schritt 1– Erstellen der Tenable-Anwendung in Azure

So erstellen Sie die Tenable-Anwendung in Azure:

1. Gehen Sie in Azure zu Microsoft Entra ID > **Unternehmensanwendungen** und klicken Sie auf **+ Neue Anwendung.**

   Die Seite **Microsoft Entra ID-Katalog durchsuchen** wird angezeigt.



2. Klicken Sie auf **+ Eigene Anwendung erstellen**.

   Der Seitenbereich **Eigene Anwendung erstellen** wird angezeigt.

3. Geben Sie im Feld **Wie lautet der Name der App?** einen Namen für die Anwendung ein (z. B. Tenable_OT) und wählen Sie **Beliebige andere, nicht im Katalog gefundene Anwendung integrieren** aus (Standardeinstellung). Klicken Sie dann auf **Erstellen**, um die Anwendung hinzuzufügen.

Schritt 2 – Erstkonfiguration

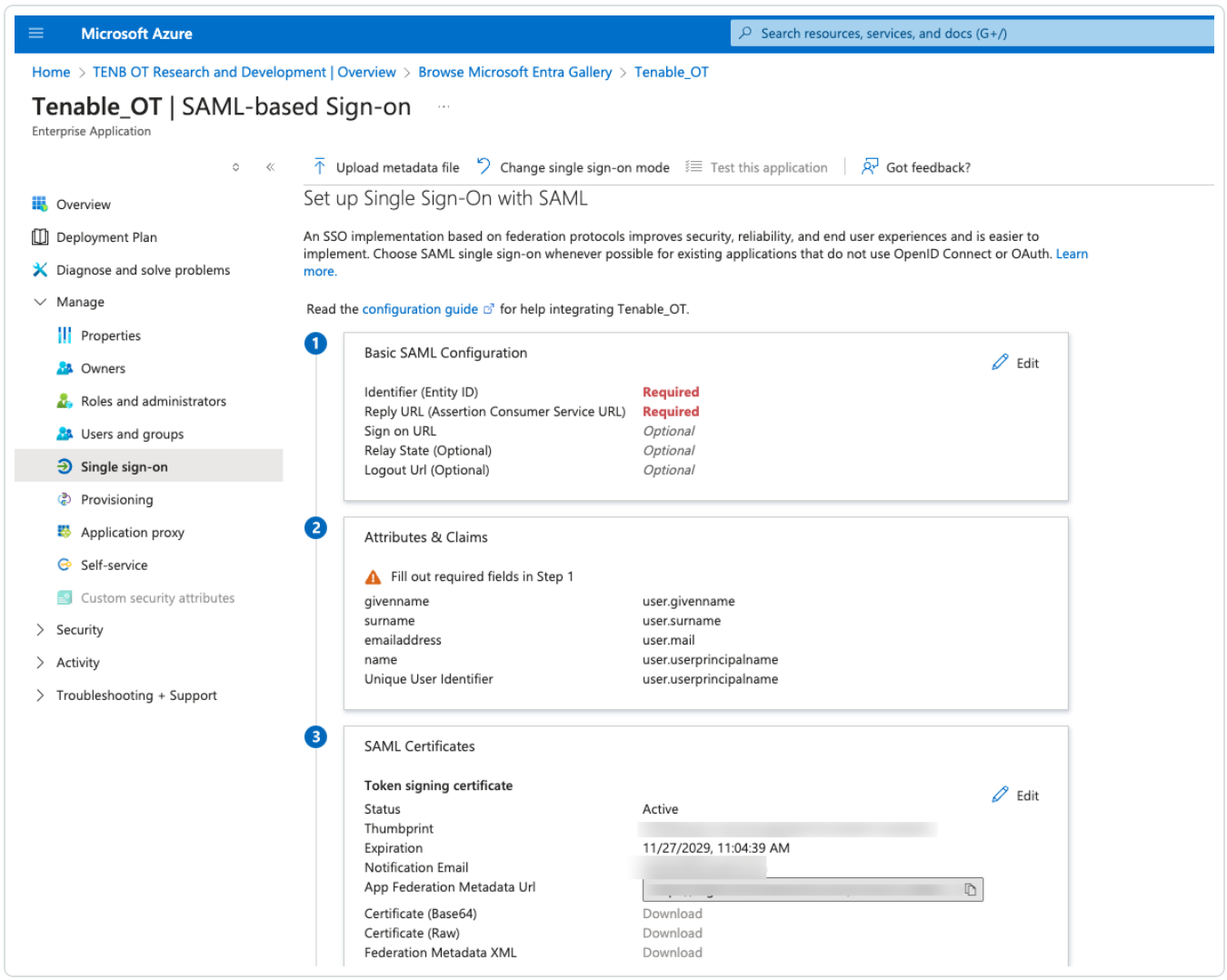
In diesem Schritt erfolgt die Erstkonfiguration der OT Security-Anwendung in Azure. Dies umfasst das Erstellen temporärer Werte für die grundlegenden SAML-Konfigurationswerte **Bezeichner** und **Antwort-URL**, um das erforderliche Zertifikat herunterzuladen.

> **Hinweis**: Konfigurieren Sie nur die in diesem Verfahren genannten Parameter. Behalten Sie für die anderen Parameter die Standardwerte bei.

So führen Sie die Erstkonfiguration durch:

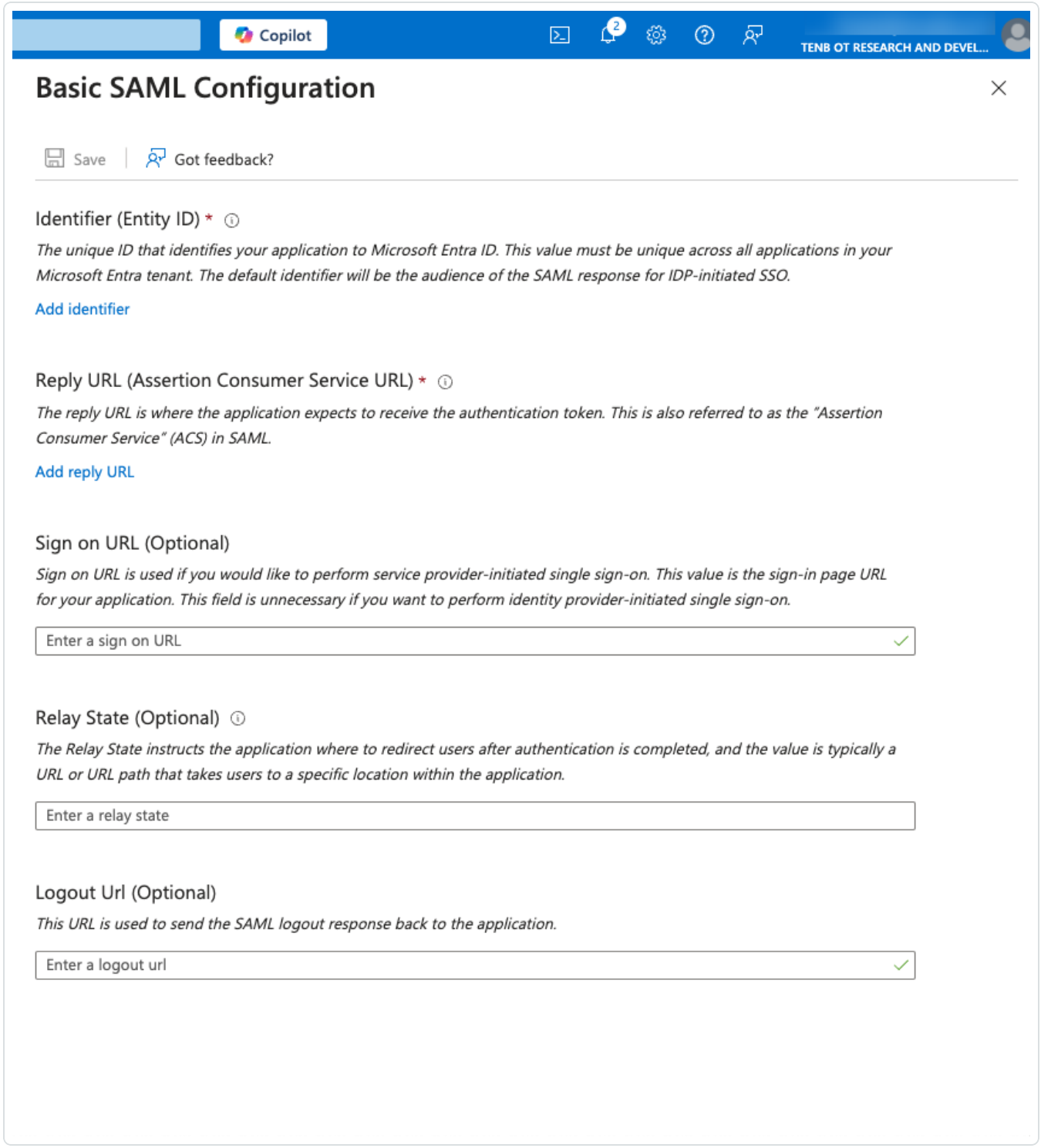
1. Klicken Sie im Navigationsmenü von Azure auf **Einmaliges Anmelden** und wählen Sie dann SAML als Methode für einmaliges Anmelden (Single Sign-On, SSO) aus.

   Die Seite **SAML-basierte Anmeldung** wird angezeigt.



2. Klicken Sie in Abschnitt 1, **Grundlegende SAML-Konfiguration**, auf  **Bearbeiten**.

   Der Seitenbereich **Grundlegende SAML-Konfiguration** wird angezeigt.



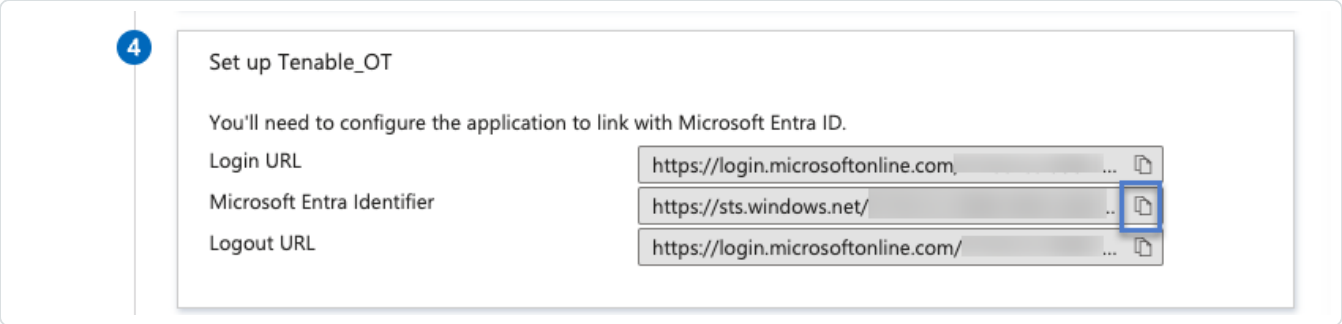
3. Geben Sie im Feld **Bezeichner (Entitäts-ID)** eine temporäre ID für die Tenable-Anwendung ein, z. B. `tenable_ot`.

4. Geben Sie im Feld **Antwort-URL (Assertion Consumer Service-URL)** eine gültige URL ein, z. B. `https://OT Security`.

   Hinweis: Die Werte für **Bezeichner** und **Antwort-URL** sind temporäre Werte, die Sie später im Konfigurationsprozess ändern können.

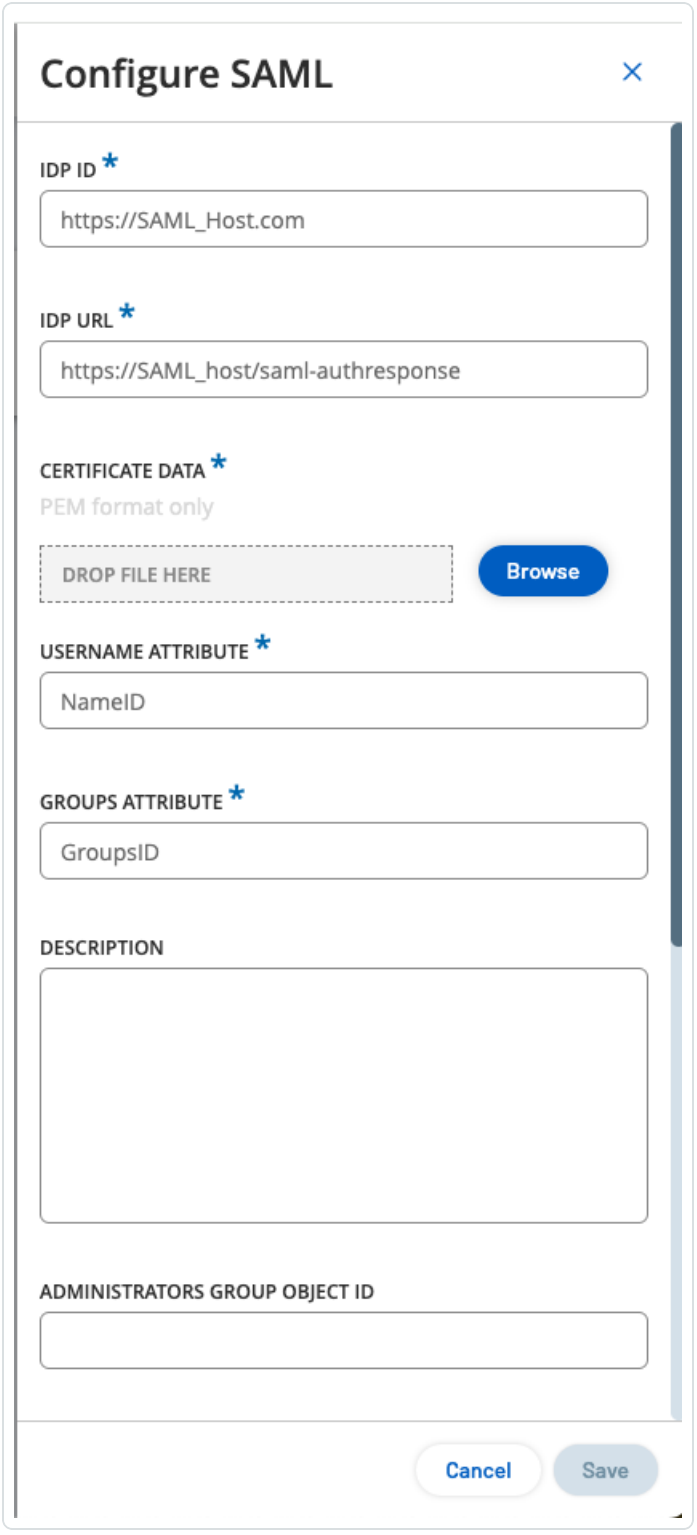
5. Klicken Sie auf **Speichern**, um die temporären Werte zu speichern und den Seitenbereich **Grundlegende SAML-Konfiguration** zu schließen.

6. Klicken Sie in Abschnitt 4, **Einrichten**, auf die Schaltfläche, um den **Microsoft Entra ID-Bezeichner** zu kopieren.



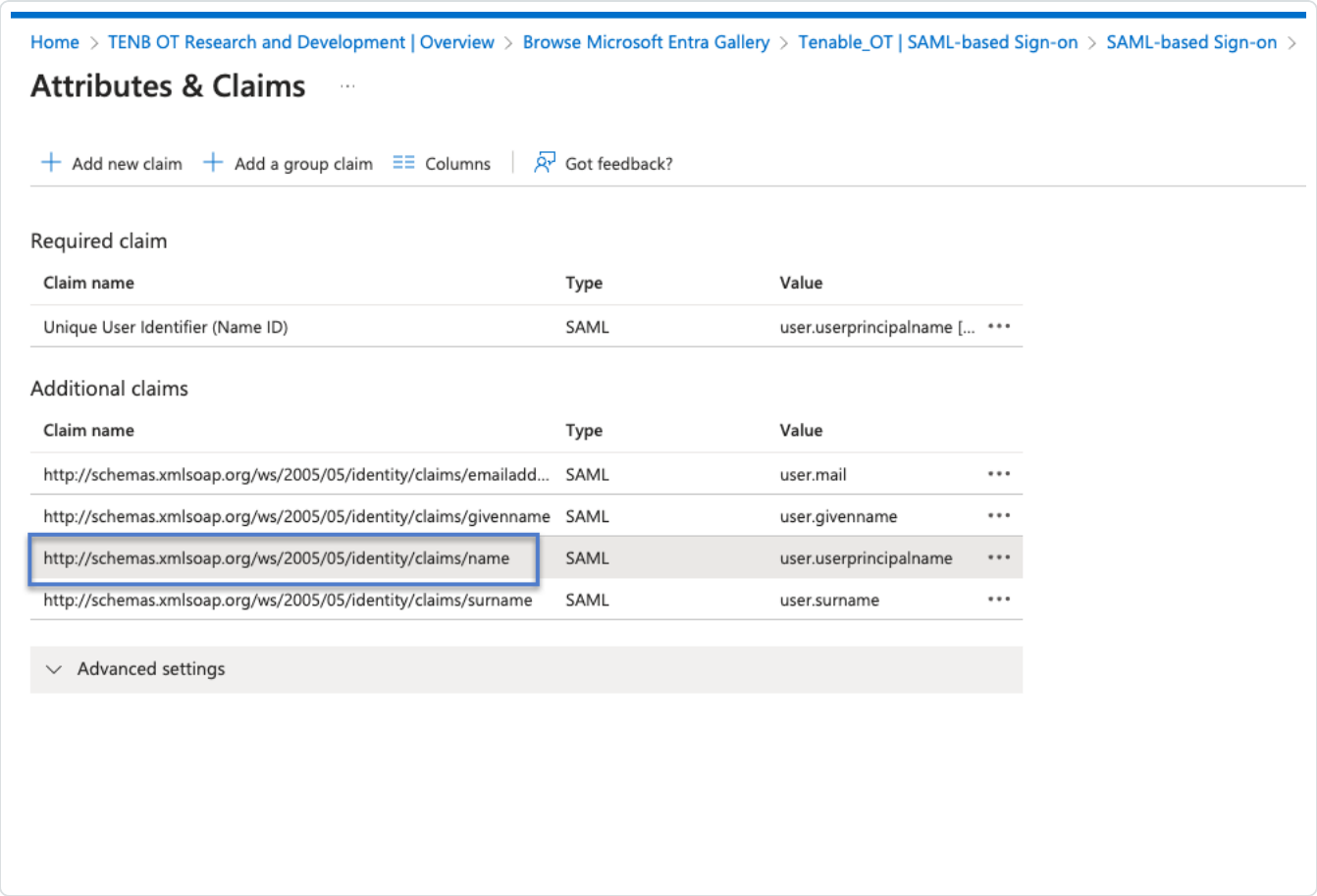
7. Wechseln Sie zur OT Security-Konsole und gehen Sie zu **Benutzerverwaltung** > **SAML**.

8. Klicken Sie auf **Konfigurieren**, um den Seitenbereich **SAML konfigurieren** anzuzeigen, und fügen Sie den kopierten Wert in das Feld **IDP-ID** ein.



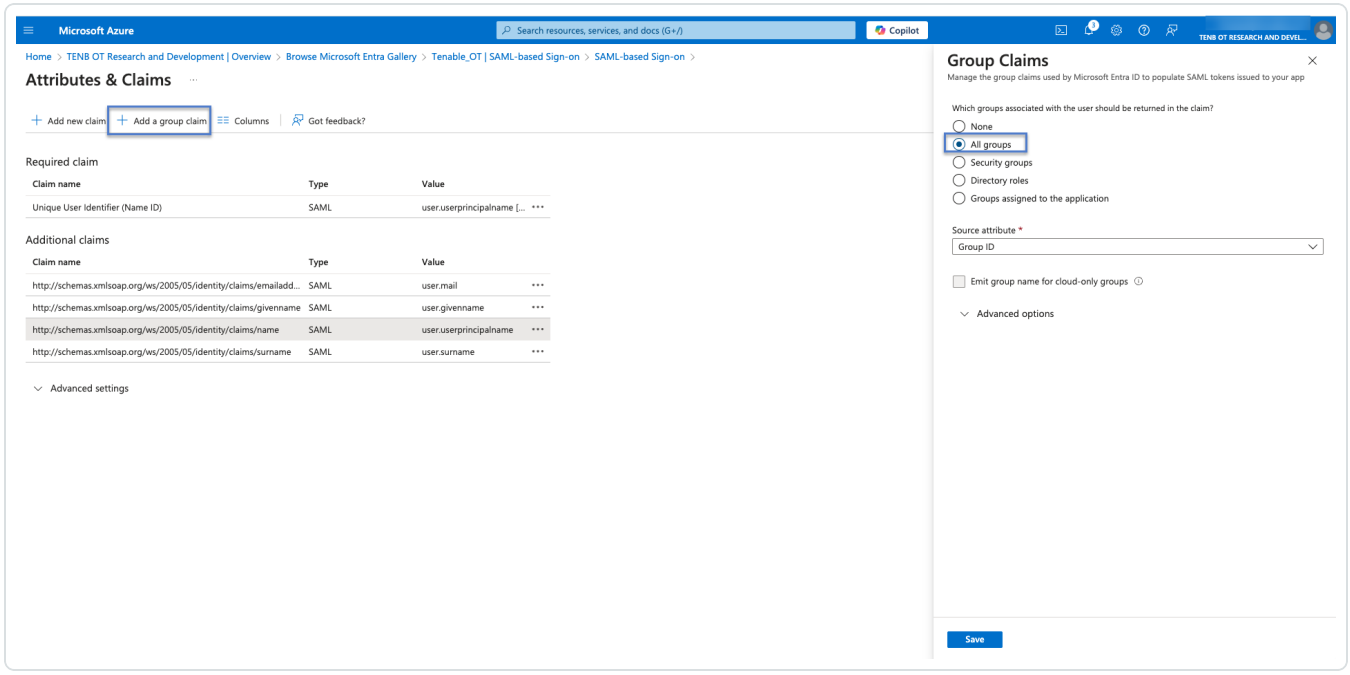
9. Klicken Sie in der Microsoft Azure-Konsole auf die Schaltfläche, um die **Anmelde-URL** zu kopieren.

10. Kehren Sie zur OT Security-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 OT Security-Konsole zurück und klicken Sie im Abschnitt **Zertifikatdaten** auf **Durchsuchen**. Navigieren Sie dann zur Sicherheitszertifikatdatei und wählen Sie sie aus.
13. Klicken Sie in der Azure-Konsole in Abschnitt 2, **Attribute & Ansprüche**, auf **Bearbeiten**.
14. Wählen Sie im Abschnitt **Zusätzliche Ansprüche** die URL unter **Anspruchsname** aus, die dem **Wert user.userprincipalname** entspricht, und kopieren Sie sie.



15. Kehren Sie zur OT Security-Konsole zurück und fügen Sie diese URL in das Feld **Username-Attribut** ein.
16. Klicken Sie in der Azure-Konsole auf **+ Gruppenanspruch hinzufügen**.

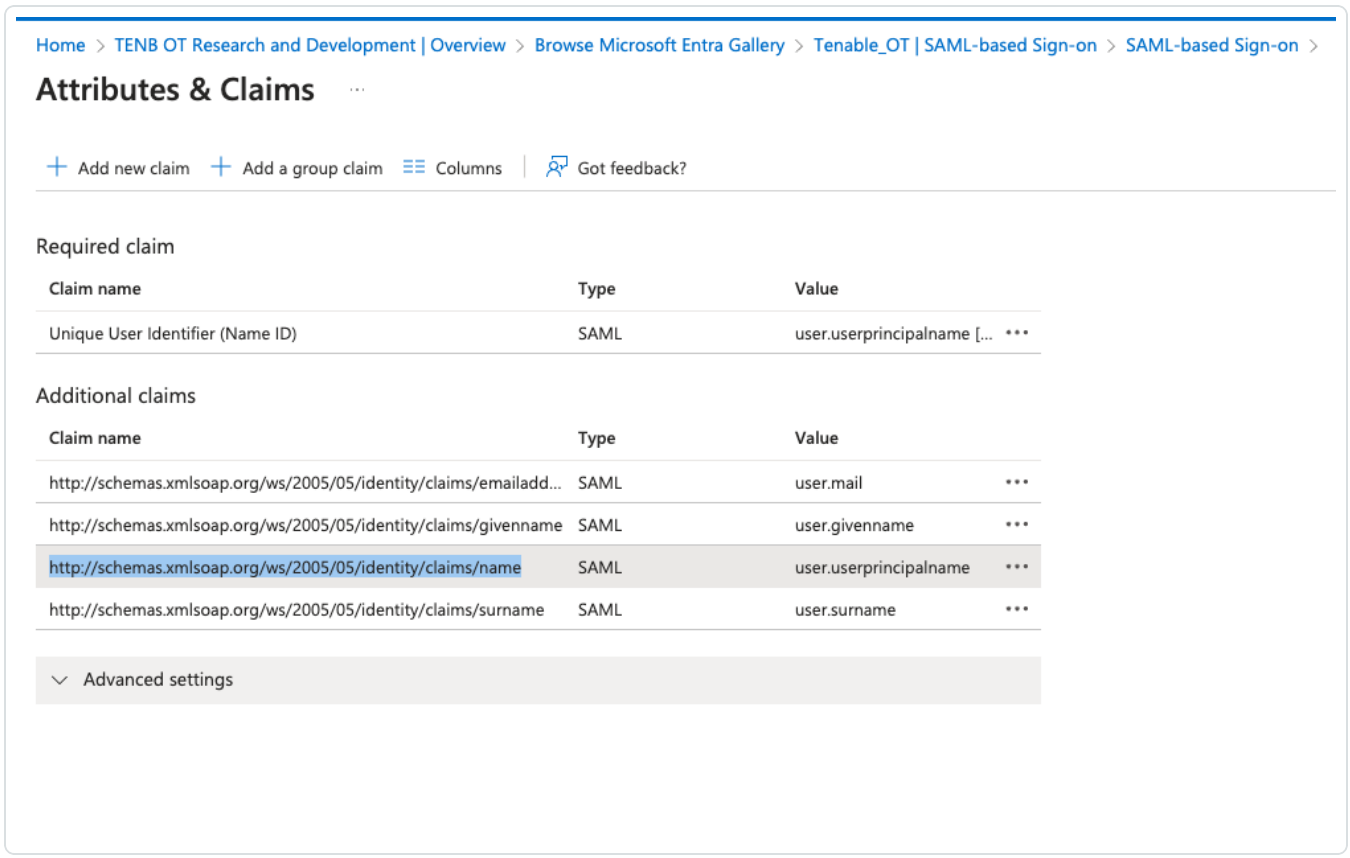
Der Seitenbereich **Gruppenansprüche** wird angezeigt.



17. Wählen Sie im Abschnitt **Welche dem Benutzer zugeordneten Gruppen sollen im Anspruch zurückgegeben werden?** die Option **Alle Gruppen** aus und klicken Sie auf **Speichern**.

> **Hinweis**: Wenn Sie die Gruppeneinstellung in Azure aktivieren, können Sie **Der Anwendung zugewiesene Gruppen** anstelle von **Alle Gruppen** auswählen. Azure stellt dann nur die Benutzergruppen bereit, die der Anwendung zugewiesen sind.

18. Markieren und kopieren Sie im Abschnitt **Zusätzliche Ansprüche** die URL unter **Anspruchsname**, die dem **Wert user.groups [All]** zugeordnet ist.



19. Kehren Sie zur OT Security-Konsole zurück und fügen Sie die kopierte URL in das Feld **Groups-Attribut** ein.
20. (Optional) Geben Sie im Feld **Beschreibung** eine Beschreibung der SAML-Konfiguration ein.

Schritt 3 – Zuordnen von Azure-Benutzern zu Tenable-Gruppen

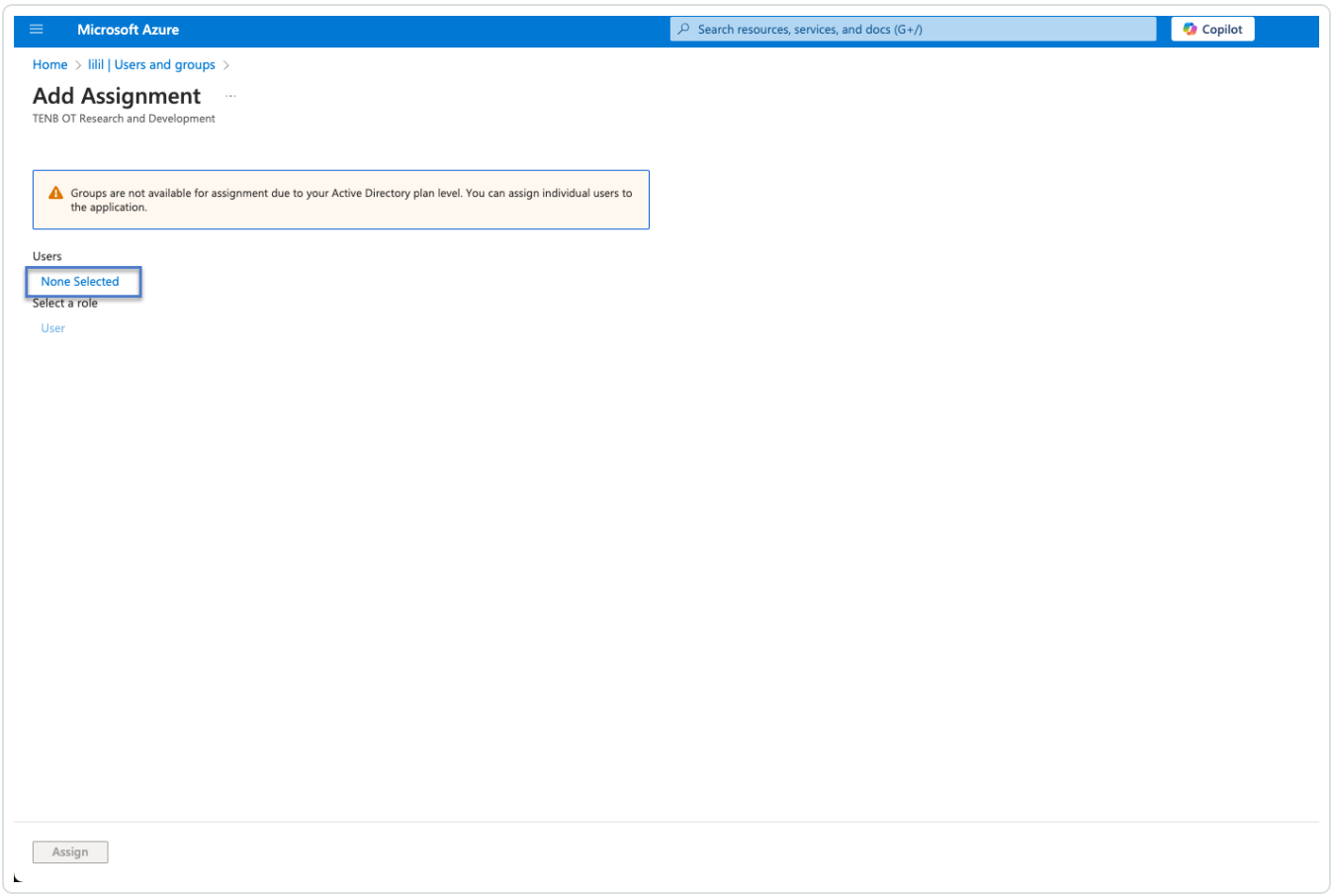
In diesem Schritt weisen sie Azure-Benutzer der OT Security-Anwendung zu. Die jedem Benutzer gewährten Berechtigungen werden festgelegt, indem die Azure-Gruppen, denen die Benutzer zugewiesen sind, einer vordefinierten OT Security-Benutzergruppe zugeordnet werden, die eine zugeordnete Rolle und einen Satz von Berechtigungen hat. Die vordefinierten Benutzergruppen von OT Security sind folgende: „Administratoren“, „Schreibgeschützt“ (Benutzer mit reinen Leseberechtigungen), „Sicherheitsanalysten“, „Sicherheitsmanager“, „Site-Operatoren“ und „Supervisoren“. Weitere Informationen finden Sie unter Benutzerverwaltung. Jeder Azure-Benutzer muss mindestens einer Gruppe zugewiesen werden, die einer OT Security-Benutzergruppe zugeordnet ist.

Hinweis: 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 OT Security zu:

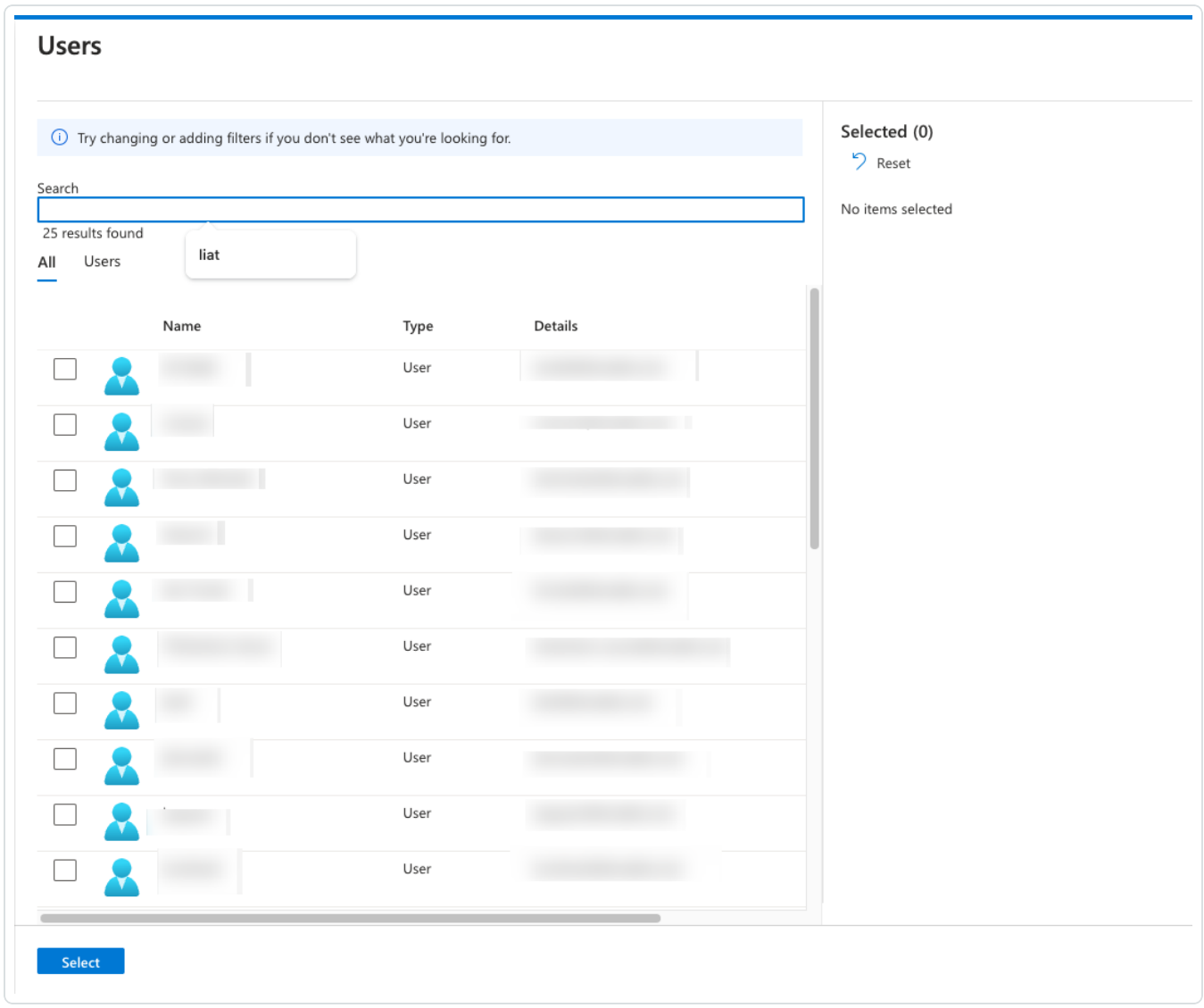
1. Navigieren Sie in Azure zur Seite **Benutzer und Gruppen** und klicken Sie auf **+ Benutzer/ Gruppe hinzufügen**.
2. Klicken Sie auf der Seite **Zuweisung hinzufügen** unter **Benutzer** auf **Keine ausgewählt**.

   Die Seite **Benutzer** wird angezeigt.



Hinweis: Wenn Sie die Gruppeneinstellung in Azure aktivieren und **Der Anwendung zugewiesene Gruppen** anstelle von **Alle Gruppen** auswählen, können Sie Gruppen anstelle von einzelnen Benutzern zuweisen.

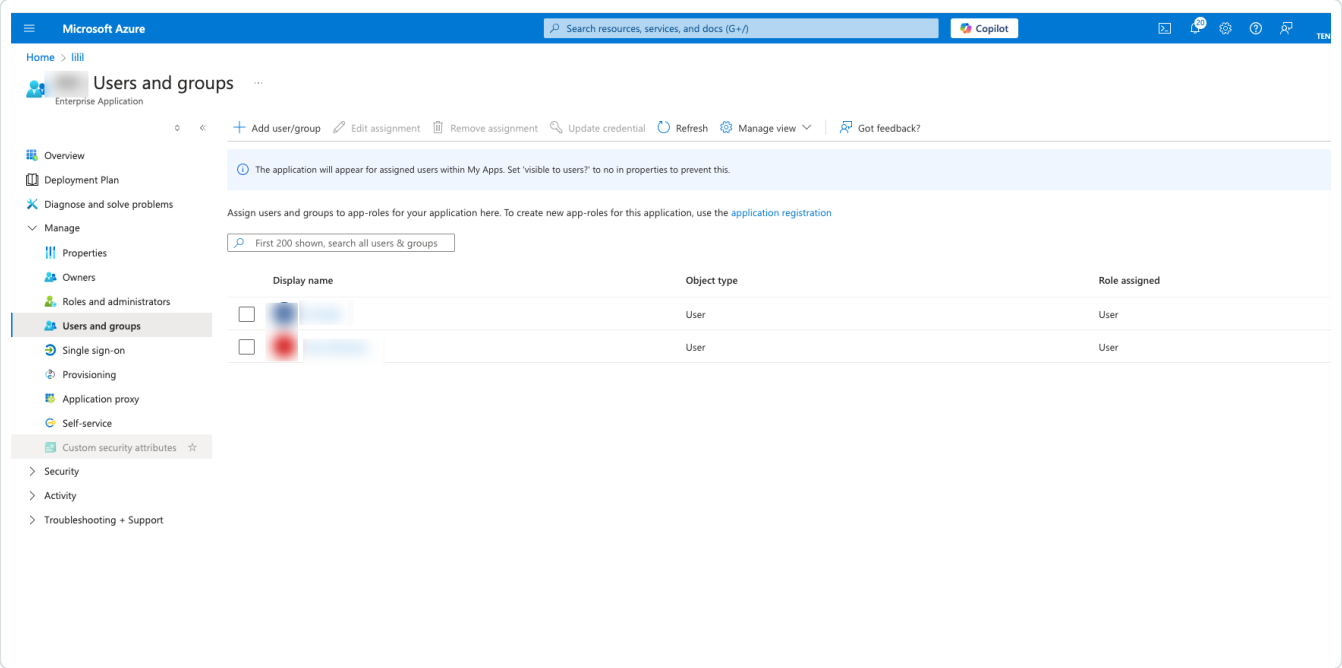
3. Suchen und markieren Sie alle erforderlichen Benutzer und klicken Sie dann auf **Auswählen**.



4. Klicken Sie auf **Zuweisen**, um sie der Anwendung zuzuweisen.

   Die Seite **Benutzer und Gruppen** wird angezeigt.

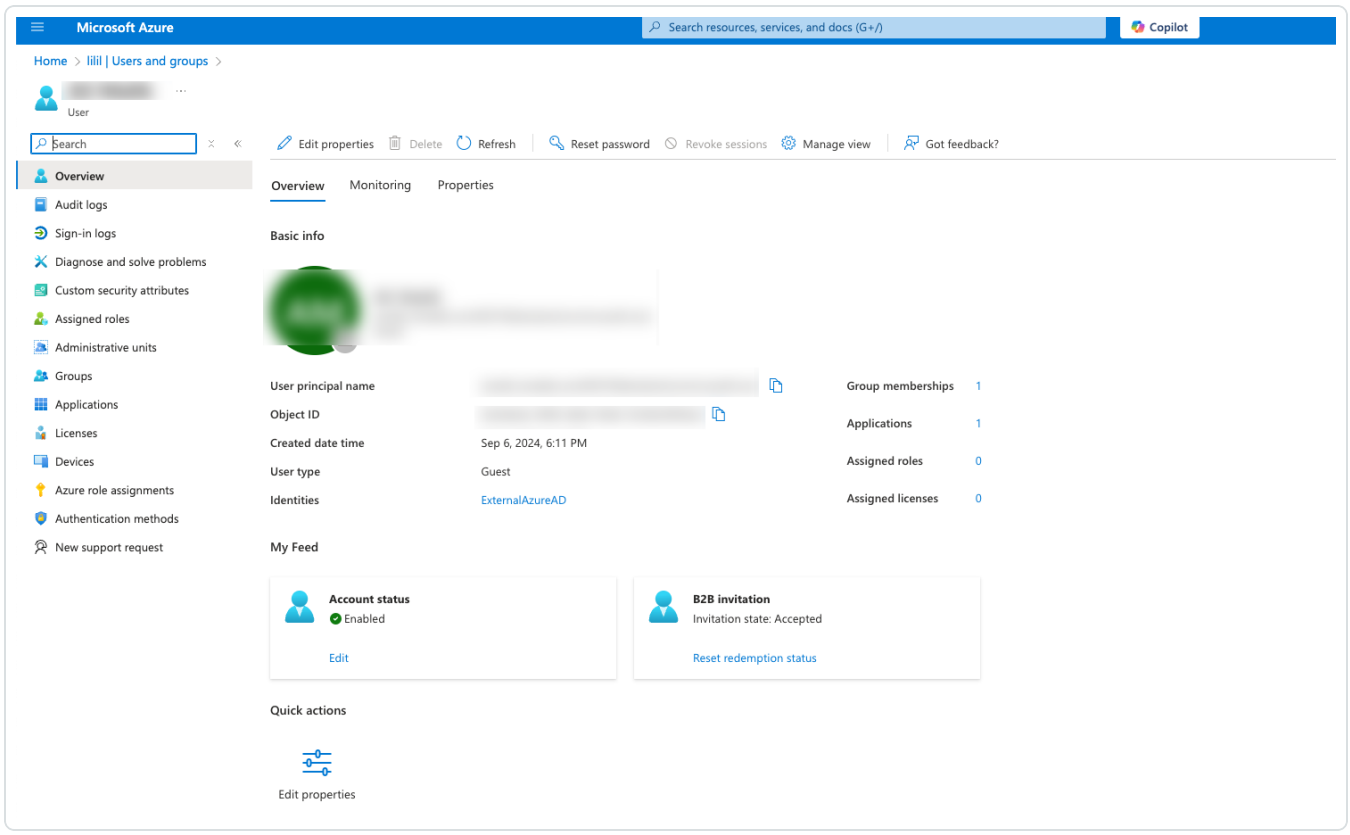
5. Klicken Sie auf den **Anzeigenamen** eines Benutzers (oder einer Gruppe), um das Profil dieses Benutzers (oder dieser Gruppe) anzuzeigen.



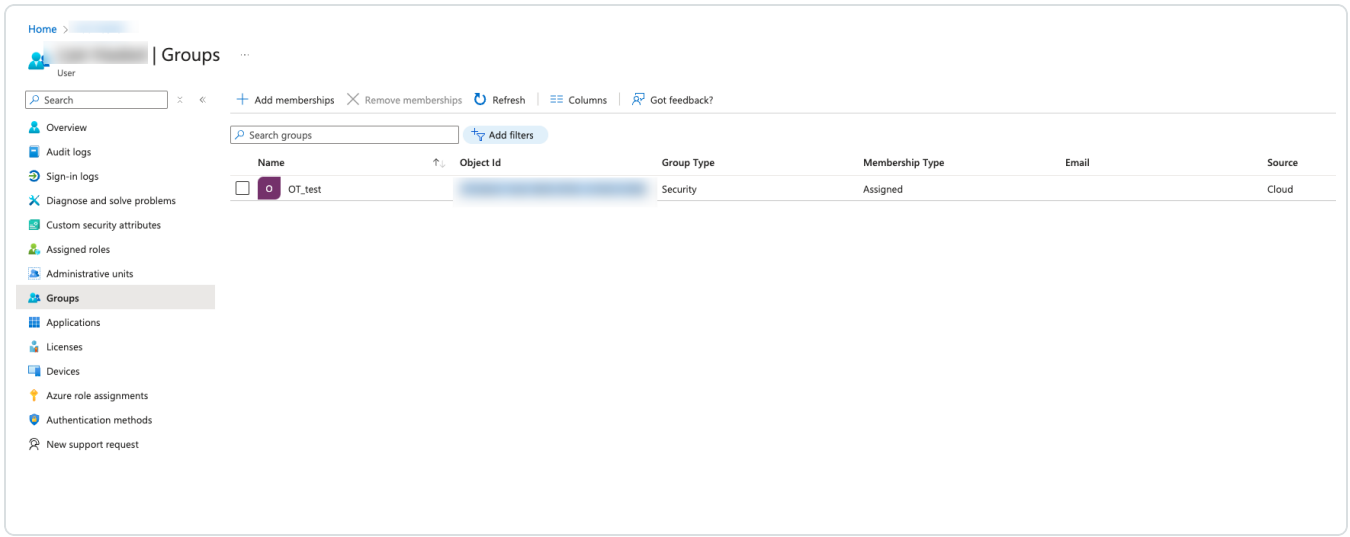
Die Seite **Profil** wird angezeigt.

6. Wählen Sie in der linken Navigationsleiste die Option **Gruppen** aus.

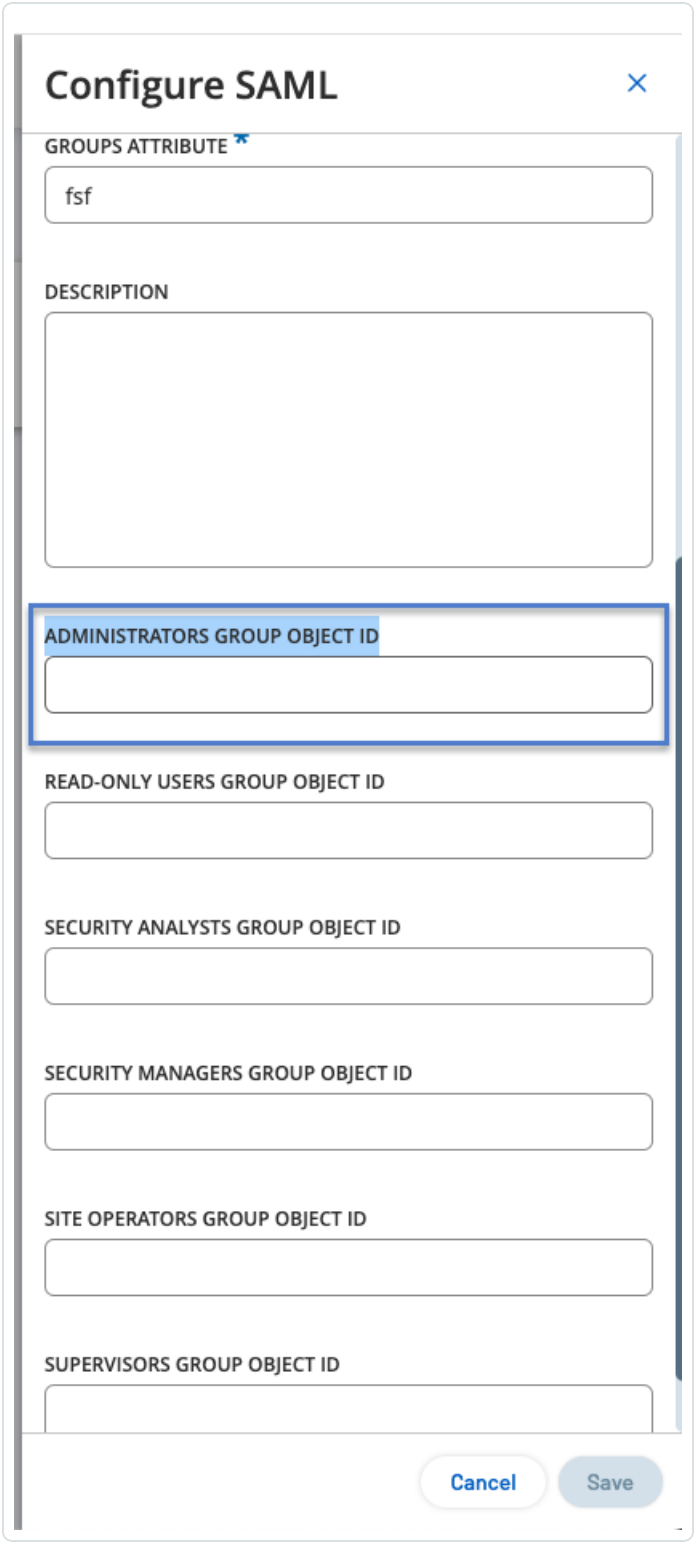
   Die Seite **Gruppen** wird angezeigt.



7. Wählen Sie in der Spalte **Objekt-ID** den Wert für die Gruppe aus, die Tenable zugeordnet werden soll, und kopieren Sie ihn.



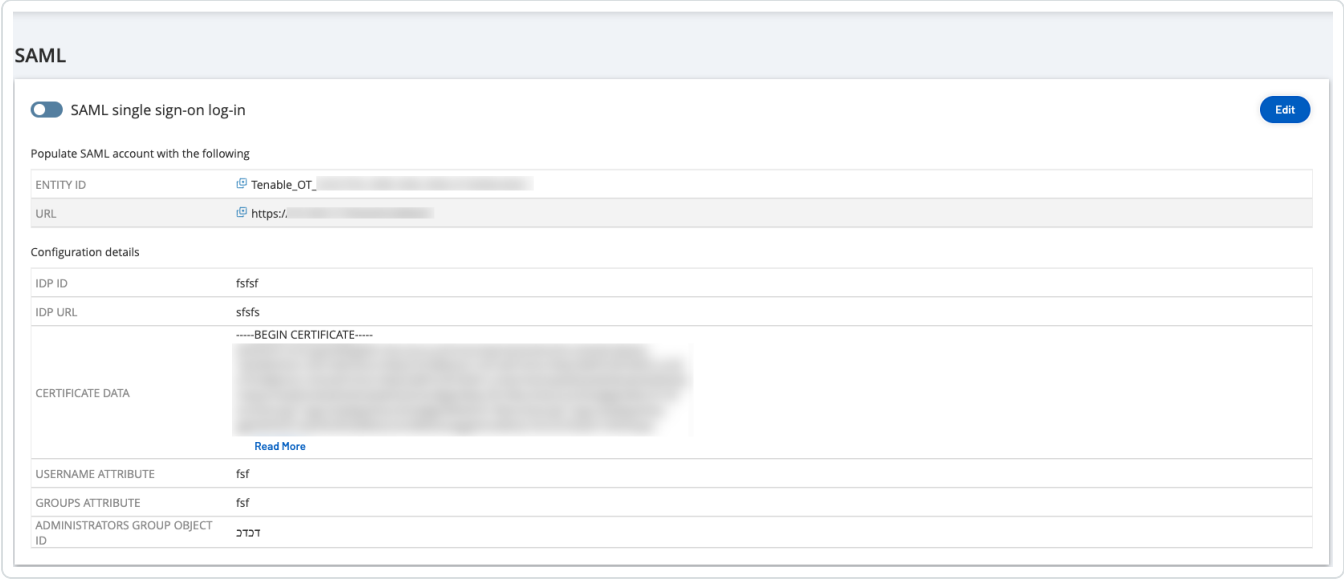
8. Kehren Sie zur OT Security-Konsole zurück und fügen Sie den kopierten Wert in das Feld der gewünschten **Gruppenobjekt-ID** ein. Zum Beispiel **Gruppenobjekt-ID für Administratoren**.



9. Wiederholen Sie die Schritte 1bis 7 für jede Gruppe, die Sie einer bestimmten Benutzergruppe in OT Security zuordnen möchten.

10. Klicken Sie auf **Speichern**, um die Informationen im Seitenbereich zu speichern und diesen zu schließen.

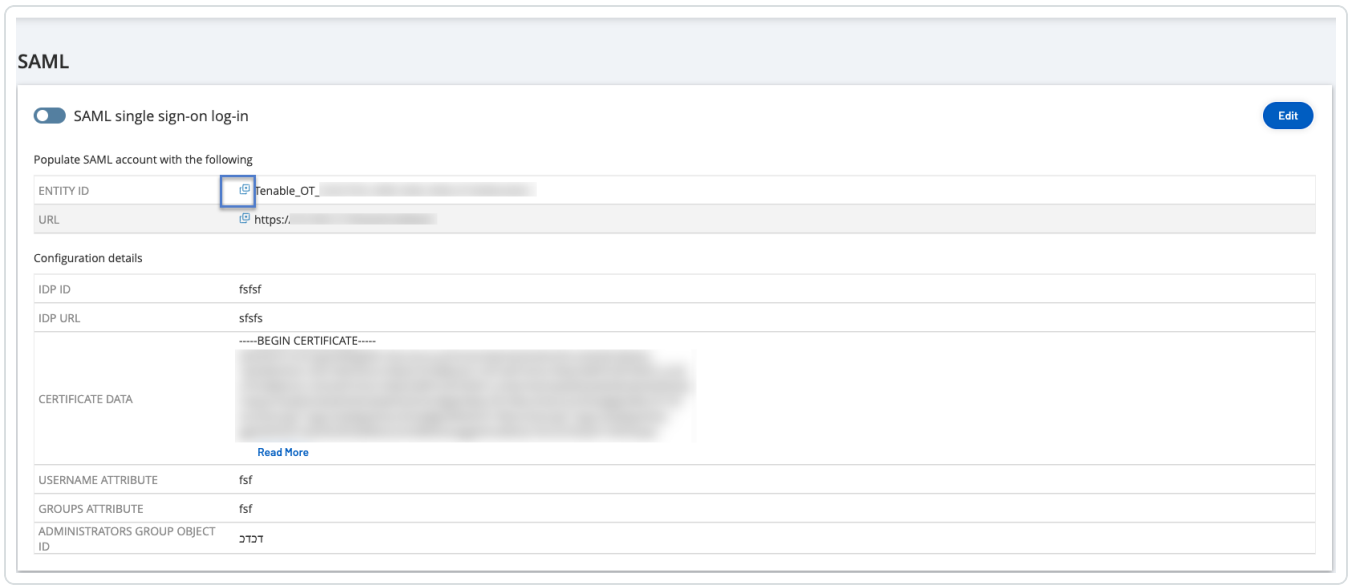
    Die SAML-Seite wird in der OT Security-Konsole mit den konfigurierten Informationen angezeigt.



Schritt 4 – Abschließen der Konfiguration in Azure

So schließen Sie die Konfiguration in AzurAzure ab:

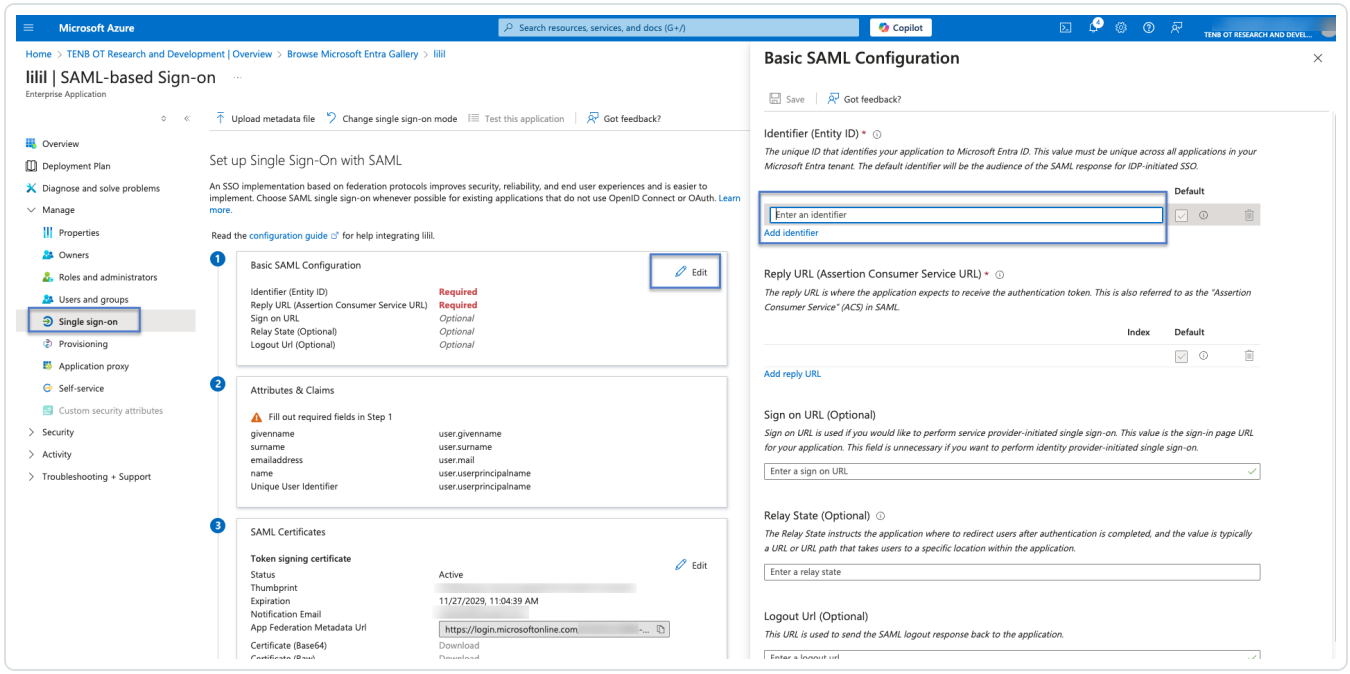
1. Klicken Sie auf der OT Security-Seite **SAML** auf die Schaltfläche , um die **Entitäts-ID** zu kopieren.



2. Klicken Sie in der Azure-Konsole im linken Navigationsmenü auf **Single Sign-On**.

   Die Seite **SAML-basierte Anmeldung** wird angezeigt.

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. Wechseln Sie zu OT Security und klicken Sie auf der Seite **SAML** auf die Schaltfläche , um die **URL** zu kopieren.
5. Wechseln Sie zur Azure-Konsole und fügen Sie im Abschnitt **Grundlegende SAML-Konfiguration** die kopierte URL in das Feld **Antwort-URL (Assertion Consumer Service-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 auf der Seite **Azure-Unternehmensanwendungen** angezeigt.

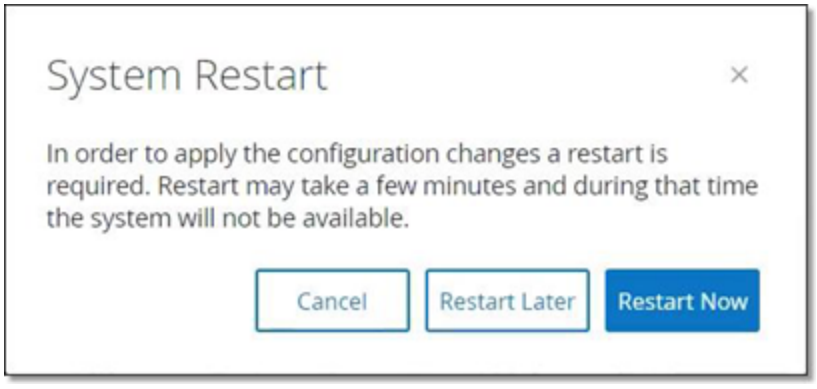
Schritt 5 – Aktivieren der Integration

Um die SAML-Integration zu aktivieren, müssen Sie OT Security neu starten. Sie können das System sofort oder später neu starten.

So aktivieren Sie die Integration:

1. Klicken Sie in der OT Security-Konsole auf der Seite **SAML** auf den Umschalter **SAML Single Sign-On-Login**, um SAML zu aktivieren.

   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

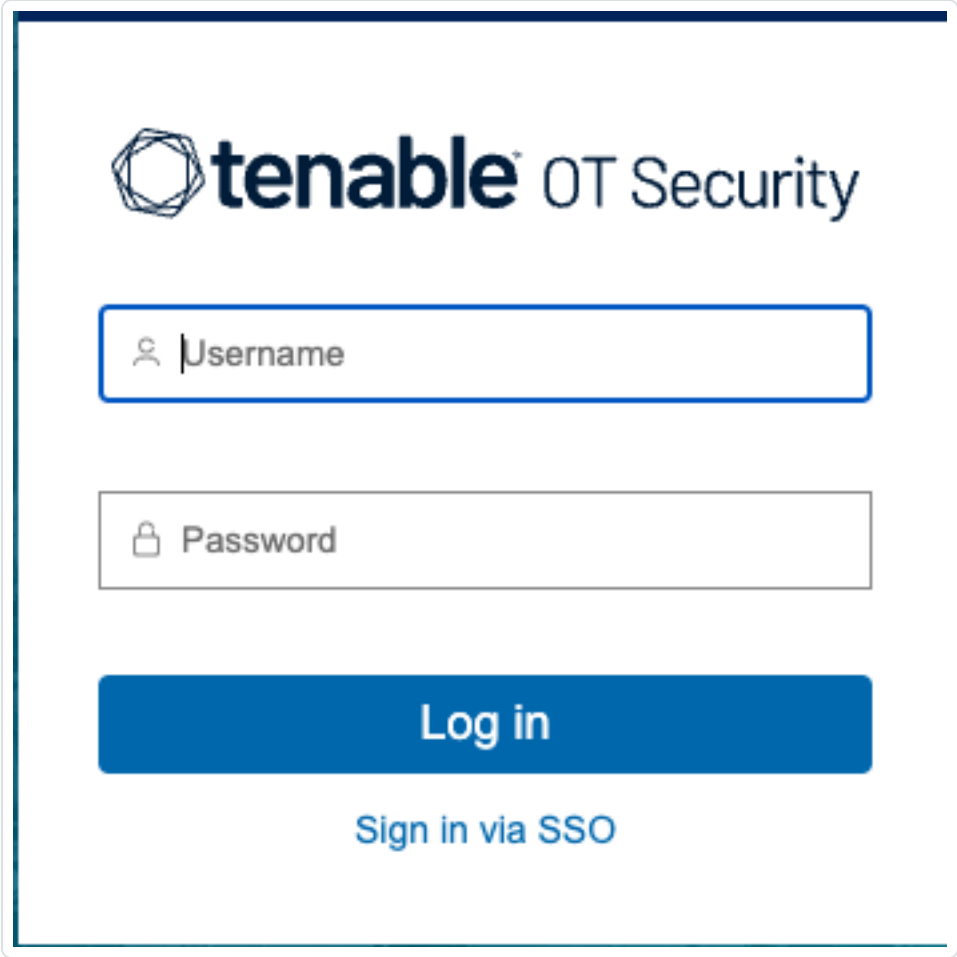
Neustart abgeschlossen ist:

Mit SSO einloggen

Nach dem Neustart enthält das OT Security-Login-Fenster unter der Schaltfläche **Einloggen** den neuen Link **Über SSO einloggen**. Azure-Benutzer, die OT Security zugewiesen sind, können sich mit ihrem Azure-Konto bei OT Security einloggen.

So loggen Sie sich mit SSO ein:

1. Klicken Sie im Login-Fenster von OT Security auf den Link **Über SSO einloggen**.



Wenn Sie bereits bei Azure eingeloggt sind, gelangen Sie direkt zur OT Security-Konsole, andernfalls werden Sie zur Login-Seite von Azure weitergeleitet.

Wenn Sie mehr als ein Konto haben, werden Sie von OT Security zur Microsoft-Seite **Konto auswählen** umgeleitet, auf der sie das gewünschte Konto für den Login auswählen können.